



Consiglio regionale della Calabria

DOSSIER

PL n. 202/12

di iniziativa del Consigliere P. STRAFACE recante:

"Modifiche ed integrazioni alla legge regionale 12 febbraio 2016, n. 2 (Istituzione del Registro tumori di popolazione della Regione Calabria)"

relatore: P. STRAFACE;

DATI DELL'ITER

NUMERO DEL REGISTRO DEI PROVVEDIMENTI	
DATA DI PRESENTAZIONE ALLA SEGRETERIA DELL'ASSEMBLEA	28/06/2023
DATA DI ASSEGNAZIONE ALLA COMMISSIONE	28/06/2023
COMUNICAZIONE IN CONSIGLIO	
SEDE	MERITO
PARERE PREVISTO	Il Comm.
NUMERO ARTICOLI	

Testo del Provvedimento

Proposta di legge 202/XII pag. 4
"Modifiche ed integrazioni alla Legge regionale 12 febbraio 2016, n. 2 (Istituzione del Registro tumori di popolazione della Regione Calabria)"

Normativa citata

Legge regionale 12 febbraio 2016, n. 2 pag. 10
"Istituzione del Registro tumori di popolazione della Regione Calabria"

Decreto legislativo 30 giugno 2003, n. 196 pag. 13
"Codice in materia di protezione dei dati personali ((, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE))."

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 pag. 202
"Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"

Normativa nazionale

Legge 22 marzo 2019, n. 29 pag. 290
"Istituzione e disciplina della Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza e del referto epidemiologico per il controllo sanitario della popolazione"

Normativa comparata

Regolamento regionale 18 gennaio 2023, n. 1 - Puglia pag. 295
"Regolamento di organizzazione e funzionamento del Registro Tumori della regione Puglia (RTP)"

Legge regionale 14 luglio 2022, n. 12 - Abruzzo pag. 309
"Istituzione del Registro Tumori della Regione Abruzzo"

Legge regionale 01 giugno 2017, n. 9 (agg. 2021) - Emilia Romagna pag. 311
"FUSIONE DELL'AZIENDA UNITÀ SANITARIA LOCALE DI REGGIO EMILIA E DELL'AZIENDA OSPEDALIERA 'ARCISPEDALE SANTA MARIA NUOVA'. ALTRE DISPOSIZIONI DI ADEGUAMENTO DEGLI ASSETTI ORGANIZZATIVI IN MATERIA SANITARIA"

Deliberazione della Giunta regionale n. 36 del 27 gennaio 2020 - Marche pag. 316
"Regolamento regionale di competenza della Giunta regionale concernente: "Disposizioni per il funzionamento del registro tumori di cui alla legge regionale 10 aprile 2012, n. 6 (Osservatorio 66 Epidemiologico Regionale. Registri regionali delle cause di morte e di patologia)"

Legge regionale 12 giugno 2015, n. 7 - Lazio pag. 332

"Istituzione del registro tumori di popolazione della Regione Lazio"

Regolamento regionale 15 Novembre 2017 n. 28 - Lazio

pag. 338

"Regolamento di attuazione e integrazione della Legge regionale 12 giugno 2015, n. 7 (Istituzione del Registro tumori di popolazione della Regione Lazio)."



Proposta di legge regionale, recante:

“Modifiche ed integrazioni alla Legge regionale 12 febbraio 2016, n. 2 (Istituzione del Registro tumori di popolazione della Regione Calabria)”

**di iniziativa del
Consigliere regionale
Pasqualina Straface**

Proposta di legge recante:

“Modifiche ed integrazioni alla Legge regionale 12 febbraio 2016, n. 2 (Istituzione del Registro tumori di popolazione della Regione Calabria)”

RELAZIONE ILLUSTRATIVA

La presente proposta di legge mira ad integrare la l.r. n. 2/2016 al fine di superare alcune criticità che ne limitano la piena attuazione nel perseguimento dei relativi principi e finalità. Richiamata anche la vigente normativa europea di riferimento in materia di protezione dei dati personali, si intende dunque apportare alcune modifiche di natura organizzativa con particolare riferimento all’attività del Centro di Coordinamento dei Registri Tumori regionale, che andrà innanzitutto eseguita in conformità al Regolamento regionale Privacy Registro tumori. Si conferiscono al Dirigente Generale del Dipartimento Tutela della Salute e Servizi Socio-Sanitari della Regione, o un suo delegato, le funzioni di Coordinatore del Centro, di cui si mira inoltre ad integrare le attività conferendo allo stesso anche una funzione di monitoraggio e di valutazione dell’operato dei registri territoriali nonché propositiva rispetto alla risoluzione di eventuali problematiche. Si integrano altresì i compiti del Dipartimento Tutela della Salute e Servizi Socio-Sanitari, che sarà nuova sede del Centro di Coordinamento e che avrà tra l’altro il compito di fissare e aggiornare i criteri e le procedure per il corretto funzionamento dei Registri Tumori provinciali.

La proposta di legge è strutturata in sette articoli e reca la clausola di invarianza finanziaria, giustificata dal fatto che le norme presenti hanno carattere squisitamente ordinamentale.

RELAZIONE TECNICO-FINANZIARIA

La presente legge introduce modifiche di carattere ordinamentale senza produrre alcun impatto finanziario sul bilancio regionale, in termini di nuove o maggiori spese e di minori entrate.

Relazione finanziaria**Quadro di riepilogo analisi economico finanziaria**

(allegato a margine della relazione tecnico finanziaria art. 39 Statuto Regione Calabria)

Titolo della legge: “Modifiche ed integrazioni alla Legge regionale 12 febbraio 2016, n. 2 (Istituzione del Registro tumori di popolazione della Regione Calabria)”

Tab. 1 - Oneri finanziari:

Articolo	Descrizione spese	Tipologia I o C	Carattere Temporale A o P	Importo
Art. 1	Norma a carattere ordinamentale che prevede l’istituzione	//	//	0,00 €

	del Registro tumori regionale al fine di assicurare la totale copertura della registrazione oncologica sull'intero territorio regionale, specificando la normativa europea di riferimento.			
Art. 2	Norma a carattere ordinamentale che, con riferimento al Centro di coordinamento regionale, ne stabilisce composizione, compiti, sede e strumenti per il raggiungimento delle finalità della legge.	//	//	0, 00 €
Art. 3	Norma a carattere ordinamentale che stabilisce l'allocazione dei registri tumori presso le AA.SS.PP. territorialmente competenti, prevedendo l'individuazione dei relativi responsabili nonché il coinvolgimento del Dipartimento competente al fine di fissare i criteri per il loro corretto funzionamento.	//	//	0, 00 €
Art. 4	Norma a carattere ordinamentale che prevede che il Regolamento regionale Privacy Registro tumori rappresenti il riferimento per le attività del Centro di coordinamento.	//	//	0, 00 €
Art. 5	Norma a carattere ordinamentale che prevede l'invarianza finanziaria.	//	//	0, 00 €
Art. 6	La clausola valutativa è volta a monitorare lo	//	//	0, 00 €

	stato attuativo della legge.			
Art. 7	Norma a carattere ordinamentale che dispone l'urgenza della legge, anticipandone l'entrata in vigore rispetto al termine ordinario di 15 giorni decorrenti dalla pubblicazione della stessa sul BURC telematico.	//	//	0, 00 €

Art. 1

(Modifiche all'articolo 1 della l.r. 2/2016)

1. Il comma 1 dell'articolo 1 della legge 2/2016 (Istituzione del Registro tumori di popolazione della Regione Calabria) è soppresso e sostituito dal seguente:
 “1. La Regione Calabria, nell'ambito delle proprie competenze e nel rispetto delle disposizioni del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e del Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, istituisce il Registro tumori della popolazione della Regione Calabria, alimentato dai registri tumori delle Aziende Sanitarie Provinciali (AA.SS.PP.) di Catanzaro, Cosenza, Crotona, Reggio Calabria e Vibo Valentia, al fine di assicurare la totale copertura della registrazione oncologica su tutto il territorio calabrese.”.
2. Al comma 1-*bis*, le parole “di cui agli articoli 85, comma 1, lettera b) e 98, comma 1, lettera c) del Codice in materia di protezione dei dati personali” sono sostituite dalle seguenti: “previste dal Codice in materia di protezione dei dati personali”.
3. Al comma 1-*bis*, lettera f), la parola “locali” è sostituita dalla seguente: “Provinciali”.

Art. 2

(Modifiche all'articolo 2 della l.r. 2/2016)

1. L'articolo 2 della legge 2/2016 (Istituzione del Registro tumori di popolazione della Regione Calabria) è soppresso e sostituito dal seguente:

“Art. 2

(Istituzione del Centro di Coordinamento dei Registri Tumori)

1. È istituito il Centro di Coordinamento regionale dei Registri Tumori composto da:
 - a) il Dirigente generale del Dipartimento Tutela della Salute e Servizi Socio-Sanitari, o un suo delegato, con funzioni di Coordinatore del Centro;
 - b) i responsabili dei registri tumori delle AA.SS.PP. di Catanzaro, Cosenza, Crotona, Reggio Calabria e Vibo Valentia;
 - c) il Direttore generale dell'Agenzia regionale per la protezione dell'ambiente della Calabria (ARPACAL), o da un suo delegato;

- d) un referente scientifico, nominato dal Dirigente Generale del Dipartimento Tutela della Salute e Servizi Socio-Sanitari.
2. Il Centro di Coordinamento regionale ha il compito di monitorare e valutare l'operato dei registri tumori delle AA.SS.PP., proponendo soluzioni idonee alla risoluzione di eventuali problematiche ed opportuni studi per le valutazioni di merito dell'impatto dell'ambiente sulla salute dei cittadini. Ha il compito, inoltre, di proporre ogni idonea azione finalizzata al miglioramento della prevenzione, della diagnosi e della terapia della patologia oncologica nel territorio della Regione Calabria, in sinergia con il Coordinamento regionale della Rete Oncologica. L'incarico di componente del Centro di coordinamento dei registri tumori è a titolo gratuito e senza compenso alcuno.
3. Il Centro di Coordinamento regionale ha sede presso il Dipartimento Tutela della Salute e Servizi Socio-Sanitari della Regione Calabria.
4. Il Centro di Coordinamento regionale si avvale di tutte le possibili e necessarie collaborazioni tecnico-scientifiche al fine di attuare gli scopi della presente legge, senza nuovi o maggiori oneri a carico del bilancio regionale.”.

Art. 3

(Modifiche all'articolo 3 della l.r. 2/2016)

1. I commi 1, 2 e 3 dell'articolo 3 della legge 2/2016 (Istituzione del Registro tumori di popolazione della Regione Calabria) sono soppressi e sostituiti dai seguenti:
- “1. I registri tumori sono allocati presso la Direzione strategica di ciascuna delle rispettive AA.SS.PP..
2. Le AA.SS.PP. provvedono a individuare entro novanta giorni dall'approvazione della presente legge, tra il personale in servizio con competenze in materia, i responsabili dei rispettivi registri tumori e l'ulteriore personale necessario agli adempimenti di legge e alla corretta operatività dei registri.
3. Il Dipartimento Tutela della Salute e Servizi Socio-Sanitari della Regione Calabria, con propri atti, fissa e aggiorna i criteri e le procedure per il corretto funzionamento dei Registri Tumori provinciali.”.

Art. 4

(Modifiche all'articolo 3-bis della l.r. 2/2016)

1. Dopo il comma 1 dell'articolo 3-bis si inserisce il seguente:
- “1-bis. Le attività del Centro di Coordinamento regionale e dei registri tumori delle AA.SS.PP. sono eseguite in conformità al vigente Regolamento regionale Privacy Registro Tumori.”.
2. Al comma 2 dell'articolo 3-bis della legge 2/2016 (Istituzione del Registro tumori di popolazione della Regione Calabria) la parola “statale” è sostituita dalla seguente: “vigente”, e sono, inoltre, soppresse le parole “in conformità al parere espresso dal Garante ai sensi degli articoli 20 e 154, comma 1, lettera g), del d.lgs. 196/2003,”.

Art. 5

(Clausola di invarianza degli oneri finanziari)

1. Dall'attuazione della presente legge non derivano nuovi o maggiori oneri finanziari a carico del bilancio regionale.

Art. 6

(Clausola valutativa)

1. La Giunta regionale, avvalendosi anche dei dati e delle informazioni prodotte dal Centro di Coordinamento regionale di cui al comma 2 dell'art. 2, presenta alla Commissione consiliare competente, entro sei mesi dalla data di entrata in vigore della presente legge e successivamente con cadenza annuale, una relazione sull'attività svolta. In particolare la relazione dovrà contenere dati e informazioni su:

- a) livello raggiunto relativo alla mappatura di tutte le patologie tumorali nel territorio regionale;
- b) interventi da parte della Giunta regionale nella programmazione sanitaria e nella rimodulazione dell'offerta sanitaria territoriale ed ospedaliera, anche in termini di campagne di prevenzione specifiche per aree geografiche o tipologia di screening, che tengano conto delle analisi e delle ricerche elaborate grazie ai dati raccolti dal Registro tumori della Regione Calabria;
- c) criticità riscontrate nella gestione del Registro tumori della Regione Calabria, in particolare le anomalie nella corretta e completa ricezione dei flussi di dati, e interventi posti in essere per ridurre al minimo le eventuali interruzioni;
- d) proposte idonee alla soluzione di eventuali problematiche e valutazioni di merito dell'impatto dell'ambiente sulla salute dei cittadini;
- e) criticità verificatesi nella applicazione della presente legge.

2. La relazione di cui al comma 1, è resa pubblica attraverso i portali istituzionali della Regione Calabria.

Art. 7

(Entrata in vigore)

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nel Bollettino ufficiale telematico della Regione Calabria (BURC).

Il Consigliere regionale

F.to Pasqualina Straface

Legge regionale 12 febbraio 2016, n. 2

Istituzione del Registro tumori di popolazione della Regione Calabria.

(BURC n. 14 del 15 febbraio 2016)

(Testo coordinato con le modifiche e le integrazioni di cui alla l.r. 20 aprile 2016, n. 12)

Art. 1

(Principi e finalità)

1. La Regione Calabria, nell'ambito delle proprie competenze e *nel rispetto delle disposizioni del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)*¹, riconosce la necessità dell'istituzione del Registro tumori della popolazione della Regione Calabria, attraverso la rete di registri tumori, per come individuati nella deliberazione di Giunta regionale (DGR) n. 289 del 25 marzo 2010 e, precisamente, Cosenza - Crotona, Catanzaro - Vibo Valentia e Reggio Calabria, al fine di assicurare la totale copertura della registrazione oncologica su tutto il territorio calabrese. Sono previste, altresì, le sub articolazioni di Vibo Valentia e Crotona, dotate di autonomia gestionale, i cui dati confluiscono nei registri, rispettivamente, di Catanzaro e Cosenza.
- 1 bis.² *In linea con le finalità di rilevante interesse pubblico di cui agli articoli 85, comma 1, lett. b) e 98, comma 1, lett. c) del Codice in materia di protezione dei dati personali, le finalità programmatiche del Registro tumori di popolazione della Regione Calabria sono così definite:*
 - a) *realizzare la raccolta, l'elaborazione e la registrazione dei dati statistici completi, di buona qualità e validati scientificamente, provenienti da molteplici fonti di flussi informativi nel campo sanitario, per incidenza, prevalenza e sopravvivenza, secondo l'andamento spaziale e temporale, dei casi di tumore che si verificano nella popolazione della Regione;*
 - b) *rappresentare uno strumento di consultazione per progetti regionali, nazionali ed internazionali, di ricerca anche transnazionale in oncologia;*
 - c) *essere di supporto ai Piani regionali per le cure palliative e la terapia del dolore;*
 - d) *contribuire, attraverso i dati prodotti, alla valutazione della appropriatezza dei trattamenti terapeutici in oncologia, alla rilevazione di eventuali differenze nell'accesso alle cure erogate al paziente oncologico, in relazione alle condizioni socio-economiche e all'area geografica di provenienza;*
 - e) *consentire interventi mirati di prevenzione primaria e valutazione per l'attivazione di campagne specifiche di diagnosi precoce oncologica, quali screening oncologici;*
 - f) *essere strumento di monitoraggio sull'efficacia dei programmi di screening oncologici, tradizionali e/o sperimentali attivi ed operativi presso le Aziende Sanitarie locali della Regione;*
 - g) *essere strumento di supporto per gli studi epidemiologici finalizzati all'analisi dell'impatto dell'ambiente sull'incidenza della patologia oncologica attraverso uno studio integrato matrici ambientali-matrici umane;*
 - h) *realizzare un'informazione continua e completa nei confronti della popolazione della Regione Calabria.*

Art. 2

(Istituzione del Centro di Coordinamento dei Registri Tumori)

1. E' istituito il Centro di coordinamento regionale dei registri tumori composto da:
 - a) il Dirigente generale del Dipartimento tutela della salute e politiche sanitarie, o un suo delegato;
 - b) i responsabili dei registri sub regionali di Cosenza - Crotona, Catanzaro - Vibo Valentia e Reggio Calabria;
 - c) i responsabili delle sub - articolazioni di Vibo Valentia e Crotona;

¹ Parole inserite dall'art. 1, comma 1, della l.r. 20 aprile 2016, n.12.

² Comma inserito dall'art. 1, comma 2, della l.r. 20 aprile 2016, n.12.

- d) il Direttore generale dell'Agencia regionale per la protezione dell'ambiente della Calabria (ARPACAL), o da un suo delegato;
 - e) l'Assessore regionale alla tutela dell'ambiente, o da un suo delegato;
 - f) il Presidente dell'Associazione italiana dei registri tumori (AIRTum), o da un suo delegato.
2. Il Centro di coordinamento regionale ha il compito di proporre soluzioni idonee al conseguimento, in tempi brevi, dell'obiettivo dell'accreditamento all'AIRTum dei registri tumori non ancora accreditati e di proporre opportuni studi per le valutazioni di merito dell'impatto sull'ambiente del "fenomeno cancro". Ha il compito, inoltre, di proporre ogni idonea azione finalizzata al miglioramento della prevenzione, della diagnosi e della terapia della patologia oncologica nel territorio della Regione Calabria, in sinergia con la Commissione oncologica regionale. L'incarico di componente del Centro di coordinamento dei registri tumori è a titolo gratuito e senza compenso alcuno.
 3. Il Centro di coordinamento regionale ha sede presso la Direzione strategica dell'Azienda sanitaria provinciale (ASP) di Catanzaro.

Art. 3

(Interventi ed articolazioni sul territorio regionale)

1. Con la presente legge, si interviene per il superamento del progetto allegato alla DGR n. 289/2010, non ravvisandosi, ormai, alcuna necessità di collaborazioni con soggetti esterni alla Regione Calabria, per come originariamente previsto dalla predetta deliberazione.
2. Per la finalità di cui al comma 1, si demanda ai responsabili dei registri di Cosenza, Catanzaro e Reggio Calabria di approntare, entro 30 giorni dall'entrata in vigore della presente legge, le Linee guida regionali per la realizzazione dei tre registri e di seguire i lavori delle aree della Calabria non coperte da registro.
3. Si stabilisce, inoltre, di allocare i registri tumori di Cosenza, Catanzaro e Reggio Calabria e delle sub articolazioni di Crotona e Vibo Valentia, presso la Direzione strategica di ciascuna delle rispettive Aziende sanitarie provinciali.
4. La rete dei registri calabresi segue le norme di registrazione oncologica, secondo le indicazioni dell'AIRTum.
5. Nella fase di organizzazione del registro tumori della popolazione delle aree non coperte, si stabilisce ogni necessaria collaborazione istituzionale con l'AIRTum, posto che al punto 3 del Regolamento e procedure per l'accreditamento di Registro tumori di popolazione AIRTum (11 giugno 2014) è prevista l'attività gratuita di tutoring di orientamento.
6. Il Centro di coordinamento regionale ed i singoli registri della Calabria si avvalgono di tutte le possibili e necessarie collaborazioni inter ed interaziendali al fine di attuare gli scopi della presente legge.

Art. 3 bis³

(Regolamento regionale)

1. *La Giunta regionale, entro il 31 luglio 2016, sentita la commissione consiliare competente, adotta, ai sensi dell'articolo 43, comma terzo, dello Statuto, un regolamento che definisce contenuti, tempi e strumenti dei flussi informativi.*
2. *Il regolamento di cui al comma 1 definisce, inoltre, le modalità di attuazione della normativa statale in materia di protezione dei dati personali, in conformità al parere espresso dal Garante ai sensi degli articoli 20 e 154, comma 1, lett. g), del d.lgs. 196/2003, con riferimento al trattamento dei dati sensibili necessario alla tenuta e al funzionamento del Registro. Sono definiti, altresì, le tipologie di dati sensibili, le operazioni eseguibili, le specifiche finalità perseguite dal Registro tumori di popolazione della Regione Calabria, i soggetti che possono avere accesso ai registri e le misure per la custodia e per la sicurezza dei dati.*

³ **Articolo inserito dall'art. 2, comma 1, della l.r. 20 aprile 2016, n.12.**

Art. 4*(Clausola di invarianza degli oneri finanziari)*

1. Dall'attuazione della presente legge non derivano nuovi o maggiori oneri finanziari a carico del bilancio regionale.
2. Per gli scopi e le funzioni della presente legge, le Aziende sanitarie provvedono in isorisorse, con personale proprio; pertanto, non sono previsti oneri aggiuntivi, né occorre impegnare fondi previsti nel bilancio della Regione Calabria.

Art. 5*(Entrata in vigore)*

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nel Bollettino ufficiale telematico della Regione Calabria (BURC).



DECRETO LEGISLATIVO 30 giugno 2003 , n. 196

Codice in materia di protezione dei dati personali **((, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE))**.

Vigente al : 29-6-2023

PARTE I

DISPOSIZIONI GENERALI

TITOLO I

((PRINCIPI E DISPOSIZIONI GENERALI

CAPO I

(OGGETTO, FINALITA' E AUTORITA' DI CONTROLLO))

IL PRESIDENTE DELLA REPUBBLICA

VISTI gli [articoli 76 e 87 della Costituzione](#);

VISTO l'[articolo 1 della legge 24 marzo 2001, n. 127](#), recante delega a Governo per l'emanazione di un testo unico in materia di trattamento dei dati personali;

VISTO l'[articolo 26 della legge 3 febbraio 2003, n. 14](#), recante disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee (legge comunitaria 2002);

((Vista la [legge 25 ottobre 2017, n. 163](#), recante delega al Governo

per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017» e, in particolare, l'articolo 13, che delega il Governo all'emanazione di uno o piu' decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del [Regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016](#);

Vista la [legge 24 dicembre 2012, n. 234](#), recante norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea;

Visto il [Regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016](#), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva 95/46/CE \(regolamento generale sulla protezione dei dati\)](#));)

VISTA la [legge 31 dicembre 1996, n. 675](#), e successive modificazioni;

VISTA la [legge 31 dicembre 1996, n. 676](#), recante delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

VISTA la [direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995](#), relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati;

VISTA la [direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002](#), relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;

VISTA la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 9 maggio 2003;

SENTITO il Garante per la protezione dei dati personali;

ACQUISITO il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

VISTA la deliberazione del Consiglio dei Ministri, adottata nella riunione del 27 giugno 2003;

SULLA PROPOSTA del Presidente del Consiglio dei Ministri, del Ministro per la funzione pubblica e del Ministro per le politiche comunitarie, di concerto con i Ministri della giustizia, dell'economia e delle finanze, degli affari esteri e delle comunicazioni;

EMANA il seguente decreto legislativo:

Art. 1
(((Oggetto).))

((Il trattamento dei dati personali avviene secondo le norme del [regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016](#), di seguito «Regolamento», e del presente codice, nel

rispetto della dignita' umana, dei diritti e delle liberta' fondamentali della persona.))

Art. 2
(((Finalita').))

((1. Il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del regolamento.))

Art. 2-bis
(((Autorita' di controllo).))

((1. L'Autorita' di controllo di cui all'articolo 51 del regolamento e' individuata nel Garante per la protezione dei dati personali, di seguito «Garante», di cui all'articolo 153.))

((CAPO II

(PRINCIPI))

Art. 2-ter

(Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri).

1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento e' costituita ((...)) da una norma di legge o ((...)) di regolamento ((o da atti amministrativi generali)). ((49))

((1-bis. Fermo restando ogni altro obbligo previsto dal Regolamento e dal presente codice, il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'[articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165](#), ivi comprese le autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'[articolo 1, comma 3, della legge 31 dicembre 2009, n. 196](#), nonché da parte di una società a controllo pubblico statale o, limitatamente ai gestori di servizi pubblici, locale, di cui all'articolo 16 del testo unico in materia di società a partecipazione pubblica, di cui al [decreto legislativo 19 agosto](#)

2016, n. 175, con esclusione, per le società a controllo pubblico, dei trattamenti correlati ad attività svolte in regime di libero mercato, e' anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti. In modo da assicurare che tale esercizio non possa arrecare un pregiudizio effettivo e concreto alla tutela dei diritti e delle libertà degli interessati, le disposizioni di cui al presente comma sono esercitate nel rispetto dell'articolo 6 del Regolamento)).

2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e' ammessa se prevista ai sensi del comma 1 **((o se necessaria ai sensi del comma 1-bis)). ((PERIODO SOPPRESSO DAL D.L. 8 OTTOBRE 2021, N. 139, CONVERTITO CON MODIFICAZIONI DALLA L. 3 DICEMBRE 2021, N. 205)).**

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 **((o se necessarie ai sensi del comma 1-bis. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione)).**

4. Si intende per:

a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

AGGIORNAMENTO (49)

Il D.L. 8 ottobre 2021, n. 139, convertito con modificazioni dalla L. 3 dicembre 2021, n. 205, ha disposto (con l'art. 9, comma 5) che "Gli articoli 2-ter, comma 1, 2-sexies, comma 1, e 58, commi 1 e 2, del codice di cui al decreto legislativo n. 196 del 2003 [...], come modificati dal presente articolo, si applicano anche ai casi in cui disposizioni di legge già in vigore stabiliscono che i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di

interesse pubblico rilevante, la finalita' del trattamento nonche' le misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato e i suoi interessi sono previsti da uno o piu' regolamenti".

Art. 2-quater

(((Regole deontologiche).))

((1. Il Garante promuove, nell'osservanza del principio di rappresentativita' e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al capo IX del Regolamento, ne verifica la conformita' alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. Lo schema di regole deontologiche e' sottoposto a consultazione pubblica per almeno sessanta giorni.

3. Conclusa la fase delle consultazioni, le regole deontologiche sono approvate dal Garante ai sensi dell'articolo 154-bis, comma 1, lettera b), pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono riportate nell'allegato A del presente codice.

4. Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceita' e la correttezza del trattamento dei dati personali.))

Art. 2-quinquies

(((Consenso del minore in relazione ai servizi della societa' dell'informazione).))

((1. In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni puo' esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della societa' dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di eta' inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, e' lecito a condizione che sia prestato da chi esercita la responsabilita' genitoriale.

2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, conciso ed esaustivo, facilmente accessibile e comprensibile dal minore, al fine di rendere significativo il consenso prestato da quest'ultimo, le informazioni e le comunicazioni relative al trattamento che lo riguarda.))

Art. 2-sexies

(Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante).

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o ((...)) di regolamento **((o da atti amministrativi generali))** che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. **((49))**

((1-bis. I dati personali relativi alla salute, privi di elementi identificativi diretti, sono trattati, nel rispetto delle finalità istituzionali di ciascuno, dal Ministero della salute, dall'Istituto superiore di sanità, dall'Agenzia nazionale per i servizi sanitari regionali, dall'Agenzia italiana del farmaco, dall'Istituto nazionale per la promozione della salute delle popolazioni migranti e per il contrasto delle malattie della povertà e, relativamente ai propri assistiti, dalle regioni anche mediante l'interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, ivi incluso il Fascicolo sanitario elettronico (FSE), aventi finalità compatibili con quelle sottese al trattamento, con le modalità e per le finalità fissate con decreto del Ministro della salute, ai sensi del comma 1, previo parere del Garante, nel rispetto di quanto previsto dal Regolamento, dal presente codice, dal [codice dell'amministrazione digitale](#), di cui al [decreto legislativo 7 marzo 2005, n. 82](#), e dalle linee guida dell'Agenzia per l'Italia digitale in materia di interoperabilità)).

2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie:

- a) accesso a documenti amministrativi e accesso civico;
- b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
- c) tenuta di registri pubblici relativi a beni immobili o mobili;
- d) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
- e) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
- f) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare, nonché documentazione

delle attività istituzionali di organi pubblici, con particolare riguardo alla redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;

g) esercizio del mandato degli organi rappresentativi, ivi compresa la loro sospensione o il loro scioglimento, nonché l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, ovvero di rimozione o sospensione da cariche pubbliche;

h) svolgimento delle funzioni di controllo, indirizzo politico, inchiesta parlamentare o sindacato ispettivo e l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo;

i) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale, comprese quelle di prevenzione e contrasto all'evasione fiscale;

l) attività di controllo e ispettive;

m) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

n) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

o) rapporti tra i soggetti pubblici e gli enti del terzo settore;

p) obiezione di coscienza;

q) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

r) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

s) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

t) attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano;

u) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

v) programmazione, gestione, controllo e valutazione

dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale;

z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;

aa) tutela sociale della maternita' ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

bb) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

cc) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonche' per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

dd) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunita' nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilita' civile, disciplinare e contabile, attivita' ispettiva.

3. Per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-septies.

AGGIORNAMENTO (49)

Il [D.L. 8 ottobre 2021, n. 139](#), convertito con modificazioni dalla [L. 3 dicembre 2021, n. 205](#), ha disposto (con l'art. 9, comma 5) che "Gli articoli 2-ter, comma 1, 2-sexies, comma 1, e 58, commi 1 e 2, del codice di cui al [decreto legislativo n. 196 del 2003](#) [...], come modificati dal presente articolo, si applicano anche ai casi in cui disposizioni di legge gia' in vigore stabiliscono che i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, la finalita' del trattamento nonche' le misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato e i suoi interessi sono previsti da uno o piu' regolamenti".

Art. 2-septies

((**Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute**).))

(1. In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformita' alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.

2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 e' adottato con cadenza almeno biennale e tenendo conto:

a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;

b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;

c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

3. Lo schema di provvedimento e' sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni.

4. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento, e riguardano anche le cautele da adottare relativamente a:

a) contrassegni sui veicoli e accessi a zone a traffico limitato;

b) profili organizzativi e gestionali in ambito sanitario;

c) modalita' per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute;

d) prescrizioni di medicinali.

5. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalita' del trattamento e possono individuare, in conformita' a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati e' consentito. In particolare, le misure di garanzia individuano le misure di sicurezza, ivi comprese quelle tecniche di cifratura e di pseudonomizzazione, le misure di minimizzazione, le specifiche modalita' per l'accesso selettivo ai dati e per rendere le informazioni agli interessati, nonche' le eventuali altre misure necessarie a garantire i diritti degli interessati.

6. Le misure di garanzia che riguardano i dati genetici e il trattamento dei dati relativi alla salute per finalita' di prevenzione, diagnosi e cura nonche' quelle di cui al comma 4, lettere b), c) e d), sono adottate sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanita'. Limitatamente ai dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del

regolamento, o altre cautele specifiche.

7. Nel rispetto dei principi in materia di protezione dei dati personali, con riferimento agli obblighi di cui all'articolo 32 del Regolamento, e' ammesso l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, nel rispetto delle misure di garanzia di cui al presente articolo.

8. I dati personali di cui al comma 1 non possono essere diffusi.)

Art. 2-octies

((Principi relativi al trattamento di dati relativi a condanne penali e reati).))

((1. Fatto salvo quanto previsto dal [decreto legislativo 18 maggio 2018, n. 51](#), il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento, che non avviene sotto il controllo dell'autorita' pubblica, e' consentito, ai sensi dell'articolo 10 del medesimo regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le liberta' degli interessati.

2. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonche' le garanzie di cui al medesimo comma sono individuati con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'[articolo 17, comma 3, della legge 23 agosto 1988, n. 400](#), sentito il Garante.

3. Fermo quanto previsto dai commi 1 e 2, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza e' consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:

a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del regolamento;

b) l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;

c) la verifica o l'accertamento dei requisiti di onorabilita', requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;

d) l'accertamento di responsabilita' in relazione a sinistri o eventi attinenti alla vita umana, nonche' la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attivita' assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

- e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- f) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
- g) l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'[articolo 134 del testo unico delle leggi di pubblica sicurezza](#);
- h) l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
- i) l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
- l) l'attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese ai sensi dell'[articolo 5-ter del decreto-legge 24 gennaio 2012, n. 1](#), convertito, con modificazioni, dalla [legge 24 marzo 2012, n. 27](#);
- m) l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.
4. Nei casi in cui le disposizioni di cui al comma 3 non individuano le garanzie appropriate per i diritti e le libertà degli interessati, tali garanzie sono previste con il decreto di cui al comma 2.
5. Quando il trattamento dei dati di cui al presente articolo avviene sotto il controllo dell'autorità pubblica si applicano le disposizioni previste dall'articolo 2-sexies.
6. Con il decreto di cui al comma 2 è autorizzato il trattamento dei dati di cui all'articolo 10 del Regolamento, effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata, stipulati con il Ministero dell'interno o con le prefetture-UTG. In relazione a tali protocolli, il decreto di cui al comma 2 individua, le tipologie dei dati trattati, gli interessati, le operazioni di trattamento eseguibili, anche in relazione all'aggiornamento e alla conservazione e prevede le garanzie appropriate per i diritti e le libertà degli interessati. Il decreto è adottato, limitatamente agli ambiti di cui al presente comma, di concerto con il Ministro dell'interno.))

Art. 2-novies

((Trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.))

((1. Le disposizioni degli articoli 2-sexies, 2-septies e 2-octies del presente decreto legislativo recano principi applicabili, in conformita' ai rispettivi ordinamenti, ai trattamenti delle categorie di dati personali di cui agli articoli 9, paragrafo 1, e 10 del Regolamento, disciplinati dalla Presidenza della Repubblica, dal Senato della Repubblica, dalla Camera dei deputati e dalla Corte costituzionale.))

Art. 2-decies
(((Inutilizzabilita' dei dati).))

((1. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, salvo quanto previsto dall'articolo 160-bis.))

((CAPO III

(DISPOSIZIONI IN MATERIA DI DIRITTI DELL'INTERESSATO))

Art. 2-undecies
(Limitazioni ai diritti dell'interessato).

1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;

b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;

c) all'attivita' di Commissioni parlamentari d'inchiesta istituite ai sensi dell'[articolo 82 della Costituzione](#);

d) alle attivita' svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalita' inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei

mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

((f) alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante attuazione della [direttiva \(UE\) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019](#), riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, ovvero che segnala violazioni ai sensi degli [articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385](#), o degli [articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58](#);)((52))

f-bis) agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale.

2. Nei casi di cui al comma 1, lettera c), si applica quanto previsto dai regolamenti parlamentari ovvero dalla legge o dalle norme istitutive della Commissione d'inchiesta.

3. Nei casi di cui al comma 1, lettere a), b), d) e), f) e f-bis) i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d), e), f) e f-bis). In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facoltà di cui al presente comma.

AGGIORNAMENTO (52)

Il [D.Lgs. 10 marzo 2023, n. 24](#), ha disposto (con l'art. 24, comma 1) che "Le disposizioni di cui al presente decreto hanno effetto a decorrere dal 15 luglio 2023".

Art. 2-duodecies

((Limitazioni per ragioni di giustizia.))

((1. In applicazione dell'articolo 23, paragrafo 1, lettera f), del Regolamento, in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonche' dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalita' previste dalle disposizioni di legge o di Regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dall'articolo 23, paragrafo 2, del Regolamento.

2. Fermo quanto previsto dal comma 1, l'esercizio dei diritti e l'adempimento degli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento possono, in ogni caso, essere ritardati, limitati o esclusi, con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalita' della limitazione, nella misura e per il tempo in cui cio' costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari.

3. Si applica l'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo.

4. Ai fini del presente articolo si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonche' i trattamenti svolti nell'ambito delle attivita' ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attivita' amministrativo-gestionale di personale, mezzi o strutture, quando non e' pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.))

Art. 2-terdecies

(((Diritti riguardanti le persone decedute).))

((1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualita' di suo mandatario, o per ragioni familiari meritevoli di protezione.

2. L'esercizio dei diritti di cui al comma 1 non e' ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della societa' dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.

3. La volonta' dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto puo' riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.

4. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.

5. In ogni caso, il divieto non puo' produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonche' del diritto di difendere in giudizio i propri interessi.)

((CAPO IV

(DISPOSIZIONI RELATIVE AL TITOLARE DEL TRATTAMENTO E AL RESPONSABILE DEL TRATTAMENTO)

)

Art. 2-quaterdecies

(((Attribuzione di funzioni e compiti a soggetti designati).))

((1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilita' e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorita'.

2. Il titolare o il responsabile del trattamento individuano le modalita' piu' opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorita' diretta.))

Art. 2-quinquiesdecies

((ARTICOLO ABROGATO DAL [D.L. 8 OTTOBRE 2021, N. 139](#), CONVERTITO CON MODIFICAZIONI DALLA [L. 3 DICEMBRE 2021, N. 205](#)))

Art. 2-sexiesdecies

(((Responsabile della protezione dei dati per i trattamenti effettuati dalle autorita' giudiziarie nell'esercizio delle loro funzioni).))

((1. Il responsabile della protezione dati e' designato, a norma delle disposizioni di cui alla sezione 4 del capo IV del Regolamento, anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni.))

Art. 2-septiesdecies

(((Organismo nazionale di accreditamento).))

((1. L'organismo nazionale di accreditamento di cui all'articolo 43, paragrafo 1, lettera b), del Regolamento e' l'Ente unico nazionale di accreditamento, istituito ai sensi del [Regolamento \(CE\) n. 765/2008, del Parlamento europeo e del Consiglio, del 9 luglio 2008](#), fatto salvo il potere del Garante di assumere direttamente, con deliberazione pubblicata nella Gazzetta Ufficiale della Repubblica italiana e in caso di grave inadempimento dei suoi compiti da parte dell'Ente unico nazionale di accreditamento, l'esercizio di tali funzioni, anche con riferimento a una o piu' categorie di trattamenti.))

Art. 3

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 4

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 5

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 6

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

TITOLO II

DIRITTI DELL'INTERESSATO

((TITOLO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 7

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 8

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 9

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 10

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

TITOLO III

REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

((TITOLO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 11

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 12

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 13

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 14

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 15

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 16

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 17

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 18

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 19

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 20

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 21

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 22

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 23

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 24

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 25

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 26

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 27

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

TITOLO IV

SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

((TITOLO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 28

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 29

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 30

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

TITOLO V

SICUREZZA DEI DATI E DEI SISTEMI

((TITOLO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 31

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 32

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 32-bis

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 33

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 34

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 35

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 36

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

TITOLO VI

ADEMPIMENTI

((TITOLO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 37

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

((39))

AGGIORNAMENTO (39)

Il [D.Lgs. 10 agosto 2018, n. 101](#) ha disposto (con l'art. 22, comma 8) che "Il registro dei trattamenti di cui all'[articolo 37, comma 4, del codice in materia di protezione dei dati personali](#), di cui al [decreto legislativo n. 196 del 2003](#), cessa di essere alimentato a far data dal 25 maggio 2018. Da tale data e fino al 31 dicembre 2019, il registro resta accessibile a chiunque secondo le modalita' stabilite nel suddetto [articolo 37, comma 4, del decreto legislativo n. 196 del 2003](#)".

Art. 38

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 39

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 40

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 41

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

TITOLO VII

TRASFERIMENTO DEI DATI ALL'ESTERO

((TITOLO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 42

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 43

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 44

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 45

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

PARTE II

**((DISPOSIZIONI SPECIFICHE PER I TRATTAMENTI NECESSARI PER ADEMPIERE AD UN OBBLIGO
LEGALE O PER L'ESECUZIONE DI UN COMPITO DI INTERESSE PUBBLICO O CONNESSO ALL'ESERCIZIO
DI PUBBLICI POTERI NONCHE' DISPOSIZIONI PER I TRATTAMENTI DI CUI AL CAPO IX DEL
REGOLAMENTO**

TITOLO 0.I

((DISPOSIZIONI SULLA BASE GIURIDICA))

Art. 45-bis

(((Base giuridica).))

((1. Le disposizioni contenute nella presente parte sono stabilite in attuazione dell'articolo 6, paragrafo 2, nonché dell'articolo 23, paragrafo 1, del regolamento.))

TITOLO I

TRATTAMENTI IN AMBITO GIUDIZIARIO

CAPO I

PROFILI GENERALI

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 46

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 47

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 48

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 49

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO II

MINORI

Art. 50

(Notizie o immagini relative a minori)

1. Il divieto di cui all'[articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448](#), di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale. (***La violazione del divieto di cui al presente articolo e' punita ai sensi dell'[articolo 684 del codice penale](#)***)).

CAPO III

INFORMATICA GIURIDICA

Art. 51

(Principi generali)

1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all'autorita' giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorita' nella rete Internet.

2. Le sentenze e le altre decisioni dell'autorita' giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorita' nella rete Internet, osservando le cautele previste dal presente capo.

Art. 52

(Dati identificativi degli interessati)

1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, l'interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, ((...)) l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento.

2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.

3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: "In caso di diffusione omettere le generalità e gli altri dati identificativi di....".

4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l'annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l'indicazione delle generalità e degli altri dati identificativi dell'interessato.

5. Fermo restando quanto previsto dall'[articolo 734-bis del codice penale](#) relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone.

6. Le disposizioni di cui al presente articolo si applicano anche in caso di deposito di lodo ai sensi dell'[articolo 825 del codice di procedura civile](#). La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l'annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi ((dell'[articolo 209 del Codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50](#))) provvede in modo analogo in caso di richiesta di una parte.

7. Fuori dei casi indicati nel presente articolo è ammessa la

diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali.

TITOLO II

TRATTAMENTI DA PARTE DI FORZE DI POLIZIA

CAPO I

PROFILI GENERALI

Art. 53

((ARTICOLO ABROGATO DAL [D.LGS. 18 MAGGIO 2018, N. 51](#))

((34))

AGGIORNAMENTO (34)

Il [D.Lgs. 18 maggio 2018, n. 51](#) ha disposto (con l'art. 49, comma 3) che "I decreti adottati in attuazione degli articoli 53 e 57 del Codice continuano ad applicarsi fino all'adozione di diversa disciplina ai sensi degli articoli 5, comma 2, e 9, comma 5".

Art. 54

((ARTICOLO ABROGATO DAL [D.LGS. 18 MAGGIO 2018, N. 51](#))

Art. 55

((ARTICOLO ABROGATO DAL [D.LGS. 18 MAGGIO 2018, N. 51](#))

Art. 56

((ARTICOLO ABROGATO DAL [D.LGS. 18 MAGGIO 2018, N. 51](#))

Art. 57

(Disposizioni di attuazione)

1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro della giustizia, sono individuate le modalita' di attuazione dei principi del presente codice relativamente al trattamento dei dati effettuato per le

finalita' di cui all'articolo 53 dal Centro elaborazioni dati e da organi, uffici o comandi di polizia, anche ad integrazione e modifica del [decreto del Presidente della Repubblica 3 maggio 1982, n. 378](#), e in attuazione della Raccomandazione R (87) 15 del Consiglio d'Europa del 17 settembre 1987, e successive modificazioni. Le modalita' sono individuate con particolare riguardo:

a) al principio secondo cui la raccolta dei dati e' correlata alla specifica finalita' perseguita, in relazione alla prevenzione di un pericolo concreto o alla repressione di reati, in particolare per quanto riguarda i trattamenti effettuati per finalita' di analisi;

b) all'aggiornamento periodico dei dati, anche relativi a valutazioni effettuate in base alla legge, alle diverse modalita' relative ai dati trattati senza l'ausilio di strumenti elettronici e alle modalita' per rendere conoscibili gli aggiornamenti da parte di altri organi e uffici cui i dati sono stati in precedenza comunicati;

c) ai presupposti per effettuare trattamenti per esigenze temporanee o collegati a situazioni particolari, anche ai fini della verifica dei requisiti dei dati ai sensi dell'articolo 11, dell'individuazione delle categorie di interessati e della conservazione separata da altri dati che non richiedono il loro utilizzo;

d) all'individuazione di specifici termini di conservazione dei dati in relazione alla natura dei dati o agli strumenti utilizzati per il loro trattamento, nonche' alla tipologia dei procedimenti nell'ambito dei quali essi sono trattati o i provvedimenti sono adottati;

e) alla comunicazione ad altri soggetti, anche all'estero o per l'esercizio di un diritto o di un interesse legittimo, e alla loro diffusione, ove necessaria in conformita' alla legge;

f) all'uso di particolari tecniche di elaborazione e di ricerca delle informazioni, anche mediante il ricorso a sistemi di indice.

((46))

AGGIORNAMENTO (46)

Il [D.L. 14 giugno 2019, n. 53](#) ha disposto (con l'art. 9, comma 1) che il presente articolo riprende vigore dal 15 giugno 2019 fino al 31 dicembre 2019.

TITOLO III

DIFESA E SICUREZZA DELLO STATO

CAPO I

PROFILI GENERALI

Art. 58

(Trattamenti di dati personali per fini di sicurezza nazionale o difesa).

1. Ai trattamenti di dati personali effettuati dagli organismi di cui agli [articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124](#), sulla base dell'articolo 26 della predetta legge o di altre disposizioni di legge o regolamento (***o previste da atti amministrativi generali***), ovvero relativi a dati coperti da segreto di Stato ai sensi degli articoli 39 e seguenti della medesima legge, si applicano le disposizioni di cui all'articolo 160, comma 4, nonche', in quanto compatibili, le disposizioni di cui agli [articoli 2, 3, 8, 15, 16, 18, 25, 37, 41, 42 e 43 del decreto legislativo 18 maggio 2018, n. 51](#). ***((49))***

2. Fermo restando quanto previsto dal comma 1, ai trattamenti effettuati da soggetti pubblici per finalita' di difesa o di sicurezza dello Stato, in base ***((a))*** disposizioni di legge ***((o di regolamento o previste da atti amministrativi generali,))*** che prevedano specificamente il trattamento, si applicano le disposizioni di cui al comma 1 del presente articolo, nonche' quelle di cui agli [articoli 23 e 24 del decreto legislativo 18 maggio 2018, n. 51](#). ***((49))***

3. Con uno o piu' regolamenti sono individuate le modalita' di applicazione delle disposizioni di cui ai commi 1 e 2, in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies, anche in relazione all'aggiornamento e alla conservazione. I regolamenti, negli ambiti di cui al comma 1, sono adottati ai sensi dell'[articolo 43 della legge 3 agosto 2007, n. 124](#), e, negli ambiti di cui al comma 2, sono adottati con decreto del Presidente del Consiglio dei ministri, ai sensi dell'[articolo 17, comma 3, della legge 23 agosto 1988, n. 400](#), su proposta dei Ministri competenti.

4. Con uno o piu' regolamenti adottati con decreto del Presidente della Repubblica su proposta del Ministro della difesa, sono disciplinate le misure attuative del presente decreto in materia di esercizio delle funzioni di difesa e sicurezza nazionale da parte delle Forze armate.

AGGIORNAMENTO (49)

Il [D.L. 8 ottobre 2021, n. 139](#), convertito con modificazioni dalla [L. 3 dicembre 2021, n. 205](#), ha disposto (con l'art. 9, comma 5) che "Gli articoli 2-ter, comma 1, 2-sexies, comma 1, e 58, commi 1 e 2, del codice di cui al [decreto legislativo n. 196 del 2003](#) [...], come modificati dal presente articolo, si applicano anche ai casi in cui disposizioni di legge già in vigore stabiliscono che i tipi di dati che possono essere trattati, le operazioni eseguibili, il motivo di interesse pubblico rilevante, la finalità del trattamento nonché le misure appropriate e specifiche per tutelare i diritti fondamentali dell'interessato e i suoi interessi sono previsti da uno o più regolamenti".

TITOLO IV

TRATTAMENTI IN AMBITO PUBBLICO

CAPO I

ACCESSO A DOCUMENTI AMMINISTRATIVI

Art. 59

(Accesso a documenti amministrativi (**(e accesso civico)**))

1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla [legge 7 agosto 1990, n. 241](#), e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati (**(di cui agli articoli 9 e 10 del regolamento)**) e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. (**(PERIODO SOPPRESSO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))**).

(1-bis. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal [decreto legislativo 14 marzo 2013, n. 33](#).)

Art. 60

((Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale).))

((1. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento e' consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, e' di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalita' o in un altro diritto o liberta' fondamentale.))

CAPO II

REGISTRI PUBBLICI E ALBI PROFESSIONALI

Art. 61

(Utilizzazione di dati pubblici ((e regole deontologiche)))

((1. Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui deve essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da piu' archivi, tenendo presenti le pertinenti Raccomandazioni del Consiglio d'Europa.

2. Agli effetti dell'applicazione del presente codice i dati personali diversi da quelli di cui agli articoli 9 e 10 del regolamento, che devono essere inseriti in un albo professionale in conformita' alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 2-ter del presente codice, anche mediante reti di comunicazione elettronica. Puo' essere altresì menzionata l'esistenza di provvedimenti che a qualsiasi titolo incidono sull'esercizio della professione.))

3. L'ordine o collegio professionale puo', a richiesta della persona iscritta nell'albo che vi ha interesse, integrare i dati di cui al comma 2 con ulteriori dati pertinenti e non eccedenti in relazione all'attivita' professionale.

4. A richiesta dell'interessato l'ordine o collegio professionale puo' altresì fornire a terzi notizie o informazioni relative, in

particolare, a speciali qualificazioni professionali non menzionate nell'albo, ovvero alla disponibilita' ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni o seminart.

CAPO III

STATO CIVILE, ANAGRAFI E LISTE ELETTORALI

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 62

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 63

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO IV

FINALITA' DI RILEVANTE INTERESSE PUBBLICO

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 64

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 65

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 66

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 67

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 68

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 69

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 70

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 71

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 72

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 73

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO V

PARTICOLARI CONTRASSEGNI

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 74

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

TITOLO V

TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

CAPO I

PRINCIPI GENERALI

Art. 75

((*Specifiche condizioni in ambito sanitario*).))

((1. Il trattamento dei dati personali effettuato per finalita' di tutela della salute e incolumita' fisica dell'interessato o di terzi o della collettivita' deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del regolamento, dell'articolo 2-septies del presente codice, nonche' nel rispetto delle specifiche disposizioni di settore.))

Art. 76

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO II

((MODALITA' PARTICOLARI PER INFORMARE L'INTERESSATO E PER IL TRATTAMENTO DEI DATI

PERSONALI))

Art. 77

(((Modalita' particolari).))

((1. Le disposizioni del presente titolo individuano modalita' particolari utilizzabili dai soggetti di cui al comma 2:

a) per informare l'interessato ai sensi degli articoli 13 e 14 del Regolamento;

b) per il trattamento dei dati personali.

2. Le modalita' di cui al comma 1 sono applicabili:

a) dalle strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie e dagli esercenti le professioni sanitarie;

b) dai soggetti pubblici indicati all'articolo 80.))

Art. 78

(((Informazioni)) del medico di medicina generale o del pediatra)

1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati **((negli articoli 13 e 14 del Regolamento))**.

2. **((Le informazioni possono essere fornite))** per il complessivo trattamento dei dati personali necessario per attivita' di **((diagnosi, assistenza e terapia sanitaria))**, svolte dal medico o dal pediatra a tutela della salute o dell'incolumita' fisica dell'interessato, su richiesta dello stesso o di cui questi e' informato in quanto effettuate nel suo interesse.

((3. Le informazioni possono riguardare, altresi', dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto.))

4. **((Le informazioni))**, se non e' diversamente specificato dal medico o dal pediatra, **((riguardano))** anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

a) sostituisce temporaneamente il medico o il pediatra;

b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;

c) puo' trattare lecitamente i dati nell'ambito di un'attivita' professionale prestata in forma associata;

d) fornisce farmaci prescritti;

e) comunica dati personali al medico o pediatra in conformita' alla disciplina applicabile.

5. **((Le informazioni rese))** ai sensi del presente articolo **((evidenziano))** analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le liberta' fondamentali, nonche' per la dignita' dell'interessato, in particolare in caso di trattamenti effettuati:

((a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformita' alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, e' manifestato liberamente;))

b) nell'ambito della teleassistenza o telemedicina;

c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica.

((c-bis) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'[articolo 12 del decreto-legge 18 ottobre 2012, n. 179](#), convertito, con modificazioni, dalla [legge 17 dicembre 2012, n. 221](#);

c-ter) ai fini dei sistemi di sorveglianza e dei registri di cui all'[articolo 12 del decreto-legge 18 ottobre 2012, n. 179](#), convertito, con modificazioni, dalla [legge 17 dicembre 2012, n. 221](#).)

Art. 79

(((Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie)))

((1. Le strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie possono avvalersi delle modalita' particolari di cui all'articolo 78 in riferimento ad una pluralita' di prestazioni erogate anche da distinti reparti ed unita' della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate.))

2. Nei casi di cui al comma 1 l'organismo o le strutture annotano l'avvenuta **((informazione))** con modalita' uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unita' che, anche in tempi diversi, trattano dati relativi al medesimo interessato. **((39))**

3. Le modalita' **((particolari di cui all'articolo 78))** possono essere utilizzate in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie.

4. Sulla base di adeguate misure organizzative in applicazione del comma 3, le modalita' **((particolari))** possono essere utilizzate per piu' trattamenti di dati effettuati nei casi di cui al presente articolo e dai soggetti di cui all'articolo 80.

AGGIORNAMENTO (39)

Il [D.Lgs. 10 agosto 2018, n. 101](#) ha disposto (con l'art. 6, comma 1, lettera e)) che "al comma 2, le parole «l'organismo e le strutture» sono sostituite dalle seguenti: «la struttura o le sue articolazioni»".

Art. 80

((*Informativa da parte di altri soggetti*))

((1. Nel fornire le informazioni di cui agli articoli 13 e 14 del Regolamento, oltre a quanto previsto dall'articolo 79, possono avvalersi della facolta' di fornire un'unica informativa per una pluralita' di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti servizi o strutture di altri soggetti pubblici, diversi da quelli di cui al predetto articolo 79, operanti in ambito sanitario o della protezione e sicurezza sociale.

2. Le informazioni di cui al comma 1 sono integrate con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attivita' amministrative effettuate per motivi di interesse pubblico rilevante che non richiedono il consenso degli interessati.))

Art. 81

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 82

(Emergenze e tutela della salute e dell'incolumita' fisica)

1. ((Le informazioni di cui agli articoli 13 e 14 del Regolamento possono essere rese)) senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica per la quale la competente autorita' ha adottato un'ordinanza contingibile ed urgente ai sensi dell'[articolo 117 del decreto legislativo 31 marzo 1998, n. 112](#).

2. ((Tali informazioni possono altresì essere rese)) senza ritardo, successivamente alla prestazione, in caso di:

((a) impossibilita' fisica, incapacita' di agire o incapacita' di intendere o di volere dell'interessato, quando non e' possibile rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'[articolo 4 della legge 22 dicembre 2017, n. 219](#) o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato;))

b) rischio grave, imminente ed irreparabile per la salute o dell'interessato.

3. **((Le informazioni di cui al comma 1 possono essere rese))** senza ritardo, successivamente alla prestazione, anche in caso di prestazione medica che puo' essere pregiudicata **((dal loro preventivo rilascio))**, in termini di tempestivita' o efficacia.

4. Dopo il raggiungimento della maggiore eta' **((le informazioni sono fornite))** all'interessato **((nel caso in cui non siano state fornite in precedenza))**.

Art. 83

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 84

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO III

FINALITA' DI RILEVANTE INTERESSE PUBBLICO

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 85

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 86

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO IV

PRESCRIZIONI MEDICHE

Art. 87

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 88

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 89

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 89-bis

(((Prescrizioni di medicinali))).

((1. Per le prescrizioni di medicinali, laddove non e' necessario inserire il nominativo dell'interessato, si adottano cautele particolari in relazione a quanto disposto dal Garante nelle misure di garanzia di cui all'articolo 2-septies, anche ai fini del controllo della correttezza della prescrizione ovvero per finalita' amministrative o per fini di ricerca scientifica nel settore della sanita' pubblica.))

CAPO V

DATI GENETICI

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 90

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO VI

DISPOSIZIONI VARIE

Art. 91

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 92

(Cartelle cliniche)

1. Nei casi in cui **((strutture, pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie))** redigono e conservano una cartella clinica in conformita' alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilita' dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta e' giustificata dalla documentata necessita':

a) **((di esercitare))** o difendere un diritto in sede giudiziaria **((, ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento,))** di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalita' o in un altro diritto o liberta' fondamentale **((...))**;

b) di tutelare, in conformita' alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalita' o in un altro diritto o liberta' fondamentale **((...))**.

Art. 93

(Certificato di assistenza al parto)

1. Ai fini della dichiarazione di nascita il certificato di assistenza al parto e' sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita. Si osservano, altresì, le disposizioni dell'articolo 109.

2. Il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendono identificabile la madre che abbia dichiarato di non voler essere nominata avvalendosi della facoltà di cui all'[articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396](#), possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento.

3. Durante il periodo di cui al comma 2 la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati relativi alla madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

Art. 94

((**ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)**))

TITOLO VI

ISTRUZIONE

CAPO I

PROFILI GENERALI

Art. 95

((**ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)**))

Art. 96

((*Trattamento di dati relativi a studenti*).))

((1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché le istituzioni di alta formazione artistica e coreutica e le università statali o non

statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalita' e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalita'.

2. Resta ferma la disposizione di cui all'[articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249](#), sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.)

TITOLO VII

(((TRATTAMENTI A FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE, DI RICERCA SCIENTIFICA O STORICA O A FINI STATISTICI)))

CAPO I

PROFILI GENERALI

Art. 97

(((Ambito applicativo).))

((1. Il presente titolo disciplina il trattamento dei dati personali effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ai sensi dell'articolo 89 del regolamento.))

Art. 98

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 99

(((Durata del trattamento).))

((1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini

statistici puo' essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

2. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, e' cessato il trattamento nel rispetto di quanto previsto dall'articolo 89, paragrafo 1, del Regolamento.)

Art. 100

(Dati relativi ad attivita' di studio e ricerca)

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico i soggetti pubblici, ivi comprese le universita' e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attivita' di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli *((di cui agli articoli 9 e 10 del Regolamento))*.

2. Resta fermo il diritto dell'interessato di *((rettifica, cancellazione, limitazione e opposizione ai sensi degli articoli 16, 17, 18 e 21 del Regolamento))*.

3. I dati di cui al presente articolo non costituiscono documenti amministrativi ai sensi della [legge 7 agosto 1990, n. 241](#).

4. I dati di cui al presente articolo possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.

((4-bis. I diritti di cui al comma 2 si esercitano con le modalita' previste dalle regole deontologiche.))

CAPO II

((TRATTAMENTO A FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE O DI RICERCA STORICA))

Art. 101

(Modalita' di trattamento)

1. I dati personali raccolti **((a fini di archiviazione nel pubblico interesse o di ricerca storica))** non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalita' nel rispetto **((dell'articolo 5 del regolamento))**.

2. I documenti contenenti dati personali, trattati **((a fini di archiviazione nel pubblico interesse o di ricerca storica))**, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi. I dati personali diffusi possono essere utilizzati solo per il perseguimento dei medesimi scopi.

3. I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

Art. 102

(((Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica)))

((1. Il Garante promuove, ai sensi dell'articolo 2-quater, la sottoscrizione di regole deontologiche per i soggetti pubblici e privati, ivi comprese le societa' scientifiche e le associazioni professionali, interessati al trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica.))

((2. Le regole deontologiche di cui al comma 1 individuano garanzie adeguate per i diritti e le liberta' dell'interessato in particolare:))

a) le regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, in armonia con le disposizioni del presente codice **((e del Regolamento))** applicabili ai trattamenti di dati per finalita' giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica;

b) le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse e' informato dall'utente della prevista diffusione di dati;

c) le modalita' di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati **((a fini di archiviazione nel pubblico interesse o di ricerca storica))**, anche in riferimento all'uniformita' dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.

Art. 103

(((Consultazione di documenti conservati in archivi).))

((1. La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati dichiarati di interesse storico particolarmente importante e' disciplinata dal [decreto legislativo 22 gennaio 2004, n. 42](#) e dalle relative regole deontologiche.))

CAPO III

((TRATTAMENTO A FINI STATISTICI O DI RICERCA SCIENTIFICA))

Art. 104

(Ambito applicativo e dati identificativi (***a fini statistici o di ricerca scientifica***)))

1. Le disposizioni del presente capo si applicano ai trattamenti di dati per (***fini statistici***) o, in quanto compatibili, per (***per fini di ricerca scientifica***).

2. Agli effetti dell'applicazione del presente capo, in relazione ai dati identificativi si tiene conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare o da altri per identificare l'interessato, anche in base alle conoscenze acquisite in relazione al progresso tecnico.

Art. 105

(Modalita' di trattamento)

1. I dati personali trattati (***a fini statistici o di ricerca scientifica***) non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, ne' per trattamenti di dati per scopi di altra natura.

2. (***I fini statistici e di ricerca scientifica***) devono essere chiaramente determinati e resi noti all'interessato, nei modi di cui (***agli articoli 13 e 14 del regolamento***) anche in relazione a quanto previsto dall'articolo 106, comma 2, lettera b), del presente codice e dall'[articolo 6-bis del decreto legislativo 6 settembre 1989, n. 322](#) (...).

3. Quando specifiche circostanze individuate (***dalle regole deontologiche***) di cui all'articolo 106 sono tali da consentire ad un

soggetto di rispondere in nome e per conto di un altro, in quanto familiare o convivente, **((le informazioni all'interessato possono essere date))** anche per il tramite del soggetto rispondente.

4. Per il trattamento effettuato **((a fini statistici o di ricerca scientifica))** rispetto a dati raccolti per altri scopi, **((le informazioni all'interessato non sono dovute))** quando richiede uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicita' individuate **((dalle regole deontologiche))** di cui all'articolo 106.

Art. 106

(((Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica).))

((1. Il Garante promuove, ai sensi dell'articolo 2-quater, regole deontologiche per i soggetti pubblici e privati, ivi comprese le societa' scientifiche e le associazioni professionali, interessati al trattamento dei dati per fini statistici o di ricerca scientifica, volte a individuare garanzie adeguate per i diritti e le liberta' dell'interessato in conformita' all'articolo 89 del Regolamento.

2. Con le regole deontologiche di cui al comma 1, tenendo conto, per i soggetti gia' compresi nell'ambito del Sistema statistico nazionale, di quanto gia' previsto dal [decreto legislativo 6 settembre 1989, n. 322](#), e, per altri soggetti, sulla base di analoghe garanzie, sono individuati in particolare:

a) i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal medesimo [decreto legislativo n. 322 del 1989](#), siano effettuati per idonei ed effettivi fini statistici o di ricerca scientifica;

b) per quanto non previsto dal presente codice, gli ulteriori presupposti del trattamento e le connesse garanzie, anche in riferimento alla durata della conservazione dei dati, alle informazioni da rendere agli interessati relativamente ai dati raccolti anche presso terzi, alla comunicazione e diffusione, ai criteri selettivi da osservare per il trattamento di dati identificativi, alle specifiche misure di sicurezza e alle modalita' per la modifica dei dati a seguito dell'esercizio dei diritti dell'interessato, tenendo conto dei principi contenuti nelle pertinenti raccomandazioni del Consiglio d'Europa;

c) l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare direttamente o indirettamente l'interessato, anche in relazione alle conoscenze acquisite in base al progresso tecnico;

d) le garanzie da osservare nei casi in cui si puo' prescindere dal consenso dell'interessato, tenendo conto dei principi contenuti nelle raccomandazioni di cui alla lettera b);

e) modalita' semplificate per la prestazione del consenso degli interessati relativamente al trattamento dei dati di cui all'articolo

9 del regolamento;

f) i casi nei quali i diritti di cui agli articoli 15, 16, 18 e 21 del Regolamento possono essere limitati ai sensi dell'articolo 89, paragrafo 2, del medesimo Regolamento;

g) le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire alle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies;

h) le misure da adottare per favorire il rispetto del principio di minimizzazione e delle misure tecniche e organizzative di cui all'articolo 32 del Regolamento, anche in riferimento alle cautele volte ad impedire l'accesso da parte di persone fisiche che non sono autorizzate o designate e l'identificazione non autorizzata degli interessati, all'interconnessione dei sistemi informativi anche nell'ambito del Sistema statistico nazionale e all'interscambio di dati per fini statistici o di ricerca scientifica da effettuarsi con enti ed uffici situati all'estero;

i) l'impegno al rispetto di regole deontologiche da parte delle persone che, ai sensi dell'articolo 2-quaterdecies, risultano autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento, che non sono tenute in base alla legge al segreto d'ufficio o professionale, tali da assicurare analoghi livelli di sicurezza e di riservatezza.))

Art. 107

(((Trattamento di categorie particolari di dati personali).))

((1. Fermo restando quanto previsto dall'articolo 2-sexies e fuori dei casi di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di dati di cui all'articolo 9 del Regolamento, quando è richiesto, può essere prestato con modalità semplificate, individuate dalle regole deontologiche di cui all'articolo 106 o dalle misure di cui all'articolo 2-septies.))

Art. 108

(((Sistema statistico nazionale).))

((1. Il trattamento di dati personali da parte di soggetti che fanno parte del Sistema statistico nazionale, oltre a quanto previsto dalle regole deontologiche di cui all'articolo 106, comma 2, resta inoltre disciplinato dal [decreto legislativo 6 settembre 1989, n. 322](#), in particolare per quanto riguarda il trattamento dei dati di cui all'articolo 9 del Regolamento indicati nel programma statistico nazionale, le informative all'interessato, l'esercizio dei relativi diritti e i dati non tutelati dal segreto statistico ai sensi dell'articolo 9, comma 4, del medesimo [decreto legislativo n. 322 del 1989](#).))

Art. 109

(Dati statistici relativi all'evento della nascita)

1. Per la rilevazione dei dati statistici relativi agli eventi di nascita, compresi quelli relativi ai nati affetti da malformazioni e ai nati morti, nonché per i flussi di dati anche da parte di direttori sanitari, si osservano, oltre alle disposizioni di cui al [decreto del Ministro della sanità 16 luglio 2001, n. 349](#), le modalità tecniche determinate dall'istituto nazionale ((**di statistica, sentiti i Ministri**)) della salute, dell'interno e il Garante.

Art. 110

((**(Ricerca medica, biomedica ed epidemiologica).**))

((1. **Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'[articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502](#), ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.**

2. **In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.))**

Art. 110-bis

((**(Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici).**))

((1. **Il Garante può autorizzare il trattamento ulteriore di dati personali, compresi quelli dei trattamenti speciali di cui**

all'articolo 9 del Regolamento, a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attivita' quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalita' della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le liberta' e i legittimi interessi dell'interessato, in conformita' all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del trattamento ulteriore dei dati personali da parte di terzi, anche sotto il profilo della loro sicurezza.

3. Il trattamento ulteriore di dati personali da parte di terzi per le finalita' di cui al presente articolo puo' essere autorizzato dal Garante anche mediante provvedimenti generali, adottati d'ufficio e anche in relazione a determinate categorie di titolari e di trattamenti, con i quali sono stabilite le condizioni dell'ulteriore trattamento e prescritte le misure necessarie per assicurare adeguate garanzie a tutela degli interessati. I provvedimenti adottati a norma del presente comma sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana.

4. Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attivita' clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attivita' di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.)

TITOLO VIII

((TRATTAMENTI NELL'AMBITO DEL RAPPORTO DI LAVORO))

CAPO I

PROFILI GENERALI

Art. 111

((Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro).))

((1. Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalita' di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalita' per le informazioni da rendere all'interessato.))

Art. 111-bis

((Informazioni in caso di ricezione di curriculum).))

((1. Le informazioni di cui all'articolo 13 del Regolamento, nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del curriculum medesimo. Nei limiti delle finalita' di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei curricula non e' dovuto.))

Art. 112

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO II

((TRATTAMENTO DI DATI RIGUARDANTI I PRESTATORI DI LAVORO))

Art. 113

(Raccolta di dati e pertinenza)

1. Resta fermo quanto disposto dall'[articolo 8 della legge 20](#)

[maggio 1970, n. 300](#) ((, *nonche' dall'[articolo 10 del decreto legislativo 10 settembre 2003, n. 276.](#)*)).

CAPO III

((CONTROLLO A DISTANZA, LAVORO AGILE E TELELAVORO))

Art. 114

((*Garanzie in materia di controllo a distanza*))

1. Resta fermo quanto disposto dall'[articolo 4 della legge 20 maggio 1970, n. 300](#).

Art. 115

((*Telelavoro, lavoro agile e lavoro domestico*))

1. Nell'ambito del rapporto di lavoro domestico (***del telelavoro e del lavoro agile***) il datore di lavoro e' tenuto a garantire al lavoratore il rispetto della sua personalita' e della sua liberta' morale.

2. Il lavoratore domestico e' tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

CAPO IV

ISTITUTI DI PATRONATO E DI ASSISTENZA SOCIALE

Art. 116

(Conoscibilita' di dati su mandato dell'interessato)

1. Per lo svolgimento delle proprie attivita' gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato **((dall'interessato medesimo))**.

2. Il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le linee-guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni.

TITOLO IX

((ALTRI TRATTAMENTI IN AMBITO PUBBLICO O DI INTERESSE PUBBLICO))

CAPO I

((ASSICURAZIONI))

Art. 117

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 118

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 119

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 120

Sinistri

1. L'Istituto per la vigilanza sulle assicurazioni ((...)) definisce con proprio provvedimento le procedure e le modalita' di funzionamento della banca di dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli a motore immatricolati in Italia, stabilisce le modalita' di accesso alle informazioni

raccolte dalla banca dati per gli organi giudiziari e per le pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie, nonché le modalità e i limiti per l'accesso alle informazioni da parte delle imprese di assicurazione.

2. Il trattamento e la comunicazione ai soggetti di cui al comma 1 dei dati personali sono consentiti per lo svolgimento delle funzioni indicate nel medesimo comma.

3. Per quanto non previsto dal presente articolo si applicano le disposizioni dall'[articolo 135 del codice delle assicurazioni private](#) ((di cui al [decreto legislativo 7 settembre 2005, n. 209](#))).

TITOLO X

COMUNICAZIONI ELETTRONICHE

CAPO I

SERVIZI DI COMUNICAZIONE ELETTRONICA

Art. 121

((*Servizi interessati e definizioni*))

1. Le disposizioni del presente titolo si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, comprese quelle che supportano i dispositivi di raccolta dei dati e di identificazione.

((1-bis. Ai fini dell'applicazione delle disposizioni del presente titolo si intende per:

a) «comunicazione elettronica», ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad uncontraente o utente ricevente, identificato o identificabile;

b) «chiamata», la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;

c) «reti di comunicazione elettronica», i sistemi di

trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) «rete pubblica di comunicazioni», una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;

e) «servizio di comunicazione elettronica», i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'[articolo 2, lettera c\), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002](#);

f) «contraente», qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) «utente», qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) «dati relativi al traffico», qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) «dati relativi all'ubicazione», ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) «servizio a valore aggiunto», il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto e' necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) «posta elettronica», messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.))

Art. 122

(Informazioni raccolte nei riguardi dell'contraente o dell'utente)

1. L'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o l'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con ((...)) modalità semplificate ((...)). Ciò non vieta l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio. Ai fini della determinazione delle modalità semplificate di cui al primo periodo il Garante tiene anche conto delle proposte formulate dalle associazioni maggiormente rappresentative a livello nazionale dei consumatori e delle categorie economiche coinvolte, anche allo scopo di garantire l'utilizzo di metodologie che assicurino l'effettiva consapevolezza del contraente o dell'utente.

2. Ai fini dell'espressione del consenso di cui al comma 1, possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente.

2-bis. Salvo quanto previsto dal comma 1, è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

Art. 123

(Dati relativi al traffico)

1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.

2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'contraente, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico puo' trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'contraente o l'utente cui i dati si riferiscono hanno manifestato preliminarmente il proprio consenso, che e' revocabile in ogni momento.

4. Nel fornire **((le informazioni di cui agli articoli 13 e 14 del Regolamento))** il fornitore del servizio informa l'contraente o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

5. Il trattamento dei dati personali relativi al traffico e' consentito unicamente **((a persone che, ai sensi dell'articolo 2-quaterdecies, risultano autorizzate al trattamento e che operano))** sotto la diretta autorita' del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento e' limitato a quanto e' strettamente necessario per lo svolgimento di tali attivita' e deve assicurare l'identificazione **((della persona autorizzata))** che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

6. L'Autorita' per le garanzie nelle comunicazioni puo' ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione.

Art. 124

(Fatturazione dettagliata)

1. L'**((contraente))** ha diritto di ricevere in dettaglio, a richiesta e senza alcun aggravio di spesa, la dimostrazione degli elementi che compongono la fattura relativi, in particolare, alla data e all'ora di inizio della conversazione, al numero selezionato, al tipo di numerazione, alla localita', alla durata e al numero di scatti addebitati per ciascuna conversazione.

2. Il fornitore del servizio di comunicazione elettronica accessibile al pubblico e' tenuto ad abilitare l'utente ad effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente ed in modo agevole, avvalendosi per il pagamento di modalita' alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate.

3. Nella documentazione inviata all'**((contraente))** relativa alle

comunicazioni effettuate non sono evidenziati i servizi e le comunicazioni di cui al comma 2, ne' le comunicazioni necessarie per attivare le modalita' alternative alla fatturazione.

4. Nella fatturazione all'((**contraente**)) non sono evidenziate le ultime tre cifre dei numeri chiamati. Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati, l'((**contraente**)) puo' richiedere la comunicazione dei numeri completi delle comunicazioni in questione.

5. Il Garante, accertata l'effettiva disponibilita' delle modalita' di cui al comma 2, puo' autorizzare il fornitore ad indicare nella fatturazione i numeri completi delle comunicazioni.

Art. 125

(Identificazione della linea)

1. Se e' disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'utente chiamante la possibilita' di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'contraente chiamante deve avere tale possibilita' linea per linea. **((Rimane in ogni caso fermo quanto previsto dall'[articolo 2, comma 1, della legge 11 gennaio 2018, n. 5.](#)))**

2. Se e' disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'contraente chiamato la possibilita' di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione delle chiamate entranti.

3. Se e' disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avviene prima che la comunicazione sia stabilita, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'contraente chiamato la possibilita', mediante una funzione semplice e gratuita, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante e' stata eliminata dall'utente o contraente chiamante.

4. Se e' disponibile la presentazione dell'identificazione della linea collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'contraente chiamato la possibilita' di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea collegata all'utente chiamante.

5. Le disposizioni di cui al comma 1 si applicano anche alle chiamate dirette verso Paesi non appartenenti all'unione europea. Le disposizioni di cui ai commi 2, 3 e 4 si applicano anche alle

chiamate provenienti da tali Paesi.

6. Se e' disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e gli utenti dell'esistenza di tale servizio e delle possibilita' previste ai commi 1, 2, 3 e 4.

Art. 126

(Dati relativi all'ubicazione)

1. I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'contraente ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto.

2. Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonche' sull'eventualita' che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto.

3. L'utente e l'contraente che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni.

4. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, e' consentito unicamente (***a persone autorizzate al trattamento, ai sensi dell'articolo 2-quaterdecies, che operano***) sono la diretta autorita' del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento e' limitato a quanto e' strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione (***della persona autorizzata***) che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

Art. 127

(Chiamate di disturbo e di emergenza)

1. L'(***contraente***) che riceve chiamate di disturbo puo' richiedere che il fornitore della rete pubblica di comunicazioni o

del servizio di comunicazione elettronica accessibile al pubblico renda temporaneamente inefficace la soppressione della presentazione dell'identificazione della linea chiamante e conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione puo' essere disposta per i soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni.

2. La richiesta formulata per iscritto dall'((**contraente**)) specifica le modalita' di ricezione delle chiamate di disturbo e nel caso in cui sia preceduta da una richiesta telefonica e' inoltrata entro quarantotto ore.

3. I dati conservati ai sensi del comma 1 possono essere comunicati all'((**contraente**)) che dichiara di utilizzarli per esclusive finalita' di tutela rispetto a chiamate di disturbo. Per i servizi di cui al comma 1 il fornitore assicura procedure trasparenti nei confronti degli abbonati e puo' richiedere un contributo spese non superiore ai costi effettivamente sopportati.

4. Il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico predispone procedure trasparenti per garantire, linea per linea, l'inefficacia della soppressione dell'identificazione della linea chiamante, nonche', ove necessario, il trattamento dei dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'((**contraente**)) o dell'utente, da parte dei servizi abilitati in base alla legge a ricevere chiamate d'emergenza. I servizi sono individuati con decreto del Ministro delle comunicazioni, sentiti il Garante e l'Autorita' per le garanzie nelle comunicazioni.

Art. 128

(Trasferimento automatico della chiamata)

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta le misure necessarie per consentire a ciascun ((**contraente**)), gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico delle chiamate verso il proprio terminale effettuato da terzi.

Art. 129

((**(Elenchi dei contraenti)**))

((1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorita' per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 4, e in conformita' alla normativa dell'Unione europea, le modalita' di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi

cartacei o elettronici a disposizione del pubblico.

2. Il provvedimento di cui al comma 1 individua idonee modalita' per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per finalita' di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale nonche' per le finalita' di cui all'articolo 21, paragrafo 2, del Regolamento, in base al principio della massima semplificazione delle modalita' di inclusione negli elenchi a fini di mera ricerca del contraente per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonche' in tema di verifica, rettifica o cancellazione dei dati senza oneri.))

Art. 130

(Comunicazioni indesiderate)

1. Fermo restando quanto stabilito dagli [articoli 8 e 21 del decreto legislativo 9 aprile 2003, n. 70](#), l'uso di sistemi automatizzati di chiamata o di comunicazione di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale e' consentito con il consenso del contraente o utente. **((Resta in ogni caso fermo quanto previsto dall'[articolo 1, comma 14, della legge 11 gennaio 2018, n. 5](#).)**)

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalita' ivi indicate, mediante posta elettronica, telefax, messaggi del tipo Mms (Multimedia Messaging Service) o Sms (Short Message Service) o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalita' di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli **((6 e 7 del Regolamento))** nonche' ai sensi di quanto previsto dal comma 3-bis **((...))**.

3-bis. In deroga a quanto previsto dall'articolo 129, il trattamento dei dati di cui **((al comma 1 del predetto articolo,))** mediante l'impiego del telefono e della posta cartacea per le finalita' **((di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale))**, e' consentito nei confronti di chi non abbia esercitato il diritto di opposizione, con modalita' semplificate e anche in via telematica, mediante l'iscrizione della numerazione della quale e' intestatario e degli altri dati personali di cui **((al comma 1 del predetto articolo,))** in un registro pubblico delle opposizioni. (20)

3-ter. Il registro di cui al comma 3-bis e' istituito con decreto

del Presidente della Repubblica da adottare ai sensi dell'[articolo 17, comma 2, della legge 23 agosto 1988, n. 400](#), previa deliberazione del Consiglio dei ministri, acquisito il parere del Consiglio di Stato e delle Commissioni parlamentari competenti in materia, che si pronunciano entro trenta giorni dalla richiesta, nonche', per i relativi profili di competenza, il parere dell'Autorita' per le garanzie nelle comunicazioni, che si esprime entro il medesimo termine, secondo i seguenti criteri e principi generali:

a) attribuzione dell'istituzione e della gestione del registro ad un ente o organismo pubblico titolare di competenze inerenti alla materia;

b) previsione che l'ente o organismo deputato all'istituzione e alla gestione del registro vi provveda con le risorse umane e strumentali di cui dispone o affidandone la realizzazione e la gestione a terzi, che se ne assumono interamente gli oneri finanziari e organizzativi, mediante contratto di servizio, nel rispetto del ([codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50](#)). I soggetti che si avvalgono del registro per effettuare le comunicazioni corrispondono tariffe di accesso basate sugli effettivi costi di funzionamento e di manutenzione. Il Ministro dello sviluppo economico, con proprio provvedimento, determina tali tariffe;

c) previsione che le modalita' tecniche di funzionamento del registro consentano ad ogni utente di chiedere che sia iscritta la numerazione della quale e' intestatario secondo modalita' semplificate ed anche in via telematica o telefonica;

d) previsione di modalita' tecniche di funzionamento e di accesso al registro mediante interrogazioni selettive che non consentano il trasferimento dei dati presenti nel registro stesso, prevedendo il tracciamento delle operazioni compiute e la conservazione dei dati relativi agli accessi;

e) disciplina delle tempistiche e delle modalita' dell'iscrizione al registro, senza distinzione di settore di attivita' o di categoria merceologica, e del relativo aggiornamento, nonche' del correlativo periodo massimo di utilizzabilita' dei dati verificati nel registro medesimo, prevedendosi che l'iscrizione abbia durata indefinita e sia revocabile in qualunque momento, mediante strumenti di facile utilizzo e gratuitamente;

f) obbligo per i soggetti che effettuano trattamenti di dati per le finalita' (***di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale***), di garantire la presentazione dell'identificazione della linea chiamante e di fornire all'utente idonee informative, in particolare sulla possibilita' e sulle modalita' di iscrizione nel registro per opporsi a futuri contatti;

g) previsione che l'iscrizione nel registro non precluda i trattamenti dei dati altrimenti acquisiti e trattati nel rispetto degli articoli (***6 e 7 del Regolamento***).

3-quater. La vigilanza e il controllo sull'organizzazione e il funzionamento del registro di cui al comma 3-bis e sul trattamento dei dati sono attribuiti al Garante.

4. Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, puo' non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalita' di cui al presente comma, e' informato della possibilita' di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. E' vietato in ogni caso l'invio di comunicazioni per le finalita' di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identita' del mittente o in violazione dell'[articolo 8 del decreto legislativo 9 aprile 2003, n. 70](#), o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui **((agli articoli da 15 a 22 del Regolamento))**, oppure esortando i destinatari a visitare siti web che violino il predetto [articolo 8 del decreto legislativo n. 70 del 2003](#).

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante puo', provvedendo ai sensi **((dell'articolo 58 del Regolamento))**, altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

AGGIORNAMENTO (20)

Il [D.L. 25 settembre 2009, n. 135](#), convertito con modificazioni dalla [L. 20 novembre 2009, n. 166](#), ha disposto (con l'art. 20-bis comma 2) che il registro previsto dal comma 3-bis del presente articolo, e' istituito entro sei mesi dalla data di entrata in vigore della legge di conversione del suddetto presente decreto. Fino al suddetto termine, restano in vigore i provvedimenti adottati dal Garante per la protezione dei dati personali ai sensi dell'[articolo 154 del D.Lgs 196/2003](#).

Art. 131

(((Informazioni a contraenti e utenti)))

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa l'contraente e, ove possibile, l'utente circa la sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei.

2. L'contraente informa l'utente quando il contenuto delle comunicazioni o conversazioni puo' essere appreso da altri a causa del tipo di apparecchiature terminali utilizzate o del collegamento realizzato tra le stesse presso la sede dell'contraente medesimo.

3. L'utente informa l'altro utente quando, nel corso della conversazione, sono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti.

Art. 132

(Conservazione di dati di traffico per altre finalita').

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalita' di accertamento e repressione dei reati, mentre, per le medesime finalita', i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione. (31) (32) (33)

1-bis. I dati relativi alle chiamate senza risposta, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, sono conservati per trenta giorni. (15) (17) (33)

2. COMMA ABROGATO DAL [D.LGS. 30 MAGGIO 2008, N. 109](#).

3. Entro il termine di conservazione imposto dalla legge, se sussistono sufficienti indizi di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'[articolo 4 del codice di procedura penale](#), e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, ove rilevanti per l'accertamento dei fatti, i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato, su richiesta del pubblico ministero o su istanza del difensore dell'imputato, della persona sottoposta a indagini, della persona offesa e delle altre parti private.

3-bis. Quando ricorrono ragioni di urgenza e vi e' fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini, il pubblico ministero dispone la acquisizione dei dati con decreto motivato che e' comunicato immediatamente, e comunque non oltre quarantotto ore, al giudice competente per il rilascio dell'autorizzazione in via ordinaria. Il giudice, nelle quarantotto ore successive, decide sulla convalida con decreto motivato. PERIODO SOPPRESSO DAL [D.L. 30 SETTEMBRE 2021, N. 132](#), CONVERTITO CON

MODIFICAZIONI DALLA [L. 23 NOVEMBRE 2021, N. 178](#).

3-ter. Rispetto ai dati conservati per le finalita' indicate al comma 1 i diritti di cui agli articoli da 12 a 22 del Regolamento possono essere esercitati con le modalita' di cui all'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo.

3-quater. I dati acquisiti in violazione delle disposizioni dei commi 3 e 3-bis non possono essere utilizzati.

4. COMMA ABROGATO DAL [D.LGS. 30 MAGGIO 2008, N. 109](#).

4-bis. COMMA ABROGATO DAL [D.LGS. 30 MAGGIO 2008, N. 109](#).

4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonche' gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del [codice di procedura penale](#), di cui al [decreto legislativo 28 luglio 1989, n. 271](#), possono ordinare, anche in relazione alle eventuali richieste avanzate da autorita' investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalita' indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al [decreto legislativo n. 271 del 1989](#), ovvero per finalita' di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, puo' prevedere particolari modalita' di custodia dei dati e l'eventuale indisponibilita' dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui e' rivolto l'ordine previsto dal comma 4-ter deve ottemperarvi senza ritardo, fornendo immediatamente all'autorita' richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici e' tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attivita' conseguentemente svolte per il periodo indicato dall'autorita'. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca piu' grave reato, le disposizioni dell'[articolo 326 del codice penale](#).

4-quinquies. I provvedimenti adottati ai sensi del comma 4-ter sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia.

5. Il trattamento dei dati per le finalita' di cui al comma 1 e' effettuato nel rispetto delle misure e degli accorgimenti a garanzia

dell'interessato prescritti dal Garante ((**con provvedimento di carattere generale**)), volti a garantire che i dati conservati possiedano i medesimi requisiti di qualita', sicurezza e protezione dei dati in rete, nonche' ad indicare le modalita' tecniche per la periodica distruzione dei dati, decorsi i termini di cui al comma 1 .

5-bis. E' fatta salva la disciplina di cui all'[articolo 24 della legge 20 novembre 2017, n. 167](#).

AGGIORNAMENTO (15)

Il [D.Lgs. 30 maggio 2008, n. 109](#) ha disposto (con l'art. 6, comma 3) che la disposizione del comma 1-bis del presente articolo, ha effetto decorsi tre mesi dalla data di entrata in vigore del presente [D.Lgs. 109/08](#).

AGGIORNAMENTO (17)

Il [D.Lgs. 30 maggio 2008, n. 109](#), come modificato dal [D.L. 2 ottobre 2008, n. 151](#), convertito con modificazioni dalla [L. 28 novembre 2008, n. 186](#), ha disposto (con l'art. 6, comma 3) che la disposizione del comma 1-bis del presente articolo ha effetto a decorrere dal 31 marzo 2009.

AGGIORNAMENTO (31)

Il [D.L. 18 febbraio 2015, n. 7](#), convertito, con modificazioni, dalla [L. 17 aprile 2015, n. 43](#), ha disposto (con l'art. 4-bis, comma 1) che "Al fine di poter agevolare le indagini esclusivamente per i reati di cui agli [articoli 51, comma 3-quater](#), e [407, comma 2, lettera a\)](#), del codice di procedura penale, in deroga a quanto stabilito dall'articolo 132, comma 1, del codice di cui al [decreto legislativo 30 giugno 2003, n. 196](#), e successive modificazioni, e fermo restando quanto stabilito dall'articolo 123, comma 2, del medesimo codice, i dati relativi al traffico telefonico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto sono conservati dal fornitore fino al 31 dicembre 2016 per finalita' di accertamento e repressione dei reati. Per le medesime finalita' i dati relativi al traffico telematico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, esclusi comunque i contenuti della comunicazione, sono conservati dal fornitore fino al 31 dicembre 2016".

Ha inoltre disposto (con l'art. 4-bis, comma 3) che la presente modifica cessa di applicarsi a decorrere dal 1° gennaio 2017.

AGGIORNAMENTO (32)

Il [D.L. 18 febbraio 2015, n. 7](#), convertito con modificazioni dalla [L. 17 aprile 2015, n. 43](#), come modificato dal [D.L. 30 dicembre 2015, n. 210](#), convertito con modificazioni dalla [L. 25 febbraio 2016, n. 21](#), ha disposto (con l'art. 4-bis, comma 1) che "I dati relativi al

traffico telefonico o telematico, esclusi comunque i contenuti di comunicazione, detenuti dagli operatori dei servizi di telecomunicazione alla data di entrata in vigore della legge di conversione del presente decreto, nonché quelli relativi al traffico telefonico o telematico effettuato successivamente a tale data, sono conservati, in deroga a quanto stabilito dall'articolo 132, comma 1, del codice di cui al [decreto legislativo 30 giugno 2003, n. 196](#), e successive modificazioni, fino al 30 giugno 2017, per le finalità di accertamento e di repressione dei reati di cui agli [articoli 51, comma 3-quater](#), e [407, comma 2, lettera a\)](#), del [codice di procedura penale](#)".

Ha inoltre disposto (con l'art. 4-bis, comma 3) che "Le disposizioni di cui ai commi 1 e 2 cessano di applicarsi a decorrere dal 1° luglio 2017".

AGGIORNAMENTO (33)

La [L. 20 novembre 2017, n. 167](#) ha disposto (con l'art. 24, comma 1) che "In attuazione dell'[articolo 20 della direttiva \(UE\) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017](#), sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli [articoli 51, comma 3-quater](#), e [407, comma 2, lettera a\)](#), del [codice di procedura penale](#) il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'[articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7](#), convertito, con modificazioni, dalla [legge 17 aprile 2015, n. 43](#), è stabilito in settantadue mesi, in deroga a quanto previsto dall'[articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali](#), di cui al [decreto legislativo 30 giugno 2003, n. 196](#)".

Art. 132-bis

((*Procedure istituite dai fornitori*))

((1. I fornitori istituiscono procedure interne per corrispondere alle richieste effettuate in conformità alle disposizioni che prevedono forme di accesso a dati personali degli utenti.

2. A richiesta, i fornitori forniscono al Garante, per i profili di competenza, informazioni sulle procedure di cui al comma 1, sul numero di richieste ricevute, sui motivi legali adottati e sulle risposte date.))

Art. 132-ter

((*Sicurezza del trattamento*))

((1. Nel rispetto di quanto disposto dall'articolo 32 del Regolamento, ai fornitori di servizi di comunicazione elettronica accessibili al pubblico si applicano le disposizioni del presente articolo.

2. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta, ai sensi dell'articolo 32 del Regolamento, anche attraverso altri soggetti a cui sia affidata l'erogazione del servizio, misure tecniche e organizzative adeguate al rischio esistente.

3. I soggetti che operano sulle reti di comunicazione elettronica garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati.

4. Le misure di cui ai commi 2 e 3 garantiscono la protezione dei dati relativi al traffico ed all'ubicazione e degli altri dati personali archiviati o trasmessi dalla distruzione anche accidentale, da perdita o alterazione anche accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti, nonché garantiscono l'attuazione di una politica di sicurezza.

5. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.))

Art. 132-quater

(((Informazioni sui rischi)))

((1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, mediante linguaggio chiaro, idoneo e adeguato rispetto alla categoria e alla fascia di età dell'interessato a cui siano fornite le suddette informazioni, con particolare attenzione in caso di minori di età, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare a norma dell'articolo 132-ter, commi 2, 3 e 5, tutti i possibili rimedi e i relativi costi presumibili. Analoghe informazioni sono rese al Garante e all'Autorità per le garanzie nelle comunicazioni.))

CAPO II

INTERNET E RETI TELEMATICHE

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 133

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO III

VIDEOSORVEGLIANZA

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 134

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

TITOLO XI

LIBERE PROFESSIONI E INVESTIGAZIONE PRIVATA

((TITOLO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 135

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

TITOLO XII

((GIORNALISMO, LIBERTA' DI INFORMAZIONE E DI ESPRESSIONE))

CAPO I

PROFILI GENERALI

Art. 136

(Finalita' giornalistiche e altre manifestazioni del pensiero)

1. Le disposizioni del presente titolo si applicano ((, **ai sensi dell'articolo 85 del Regolamento,**)) al trattamento:

a) effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalita';

b) effettuato dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti di cui agli [articoli 26 e 33 della legge 3 febbraio 1963, n. 69](#);

c) ((...)) finalizzato esclusivamente alla pubblicazione o diffusione ((**anche**)) occasionale di articoli, saggi e altre manifestazioni del pensiero anche ((**nell'espressione accademica, artistica e letteraria.**)).

Art. 137

(Disposizioni applicabili).

1. Con riferimento a quanto previsto dall'articolo 136, possono essere trattati i dati di cui agli articoli 9 e 10 del Regolamento anche senza il consenso dell'interessato, purché nel rispetto delle regole deontologiche di cui all'articolo 139.

2. Ai trattamenti indicati nell'articolo 136 non si applicano le disposizioni relative:

a) alle misure di garanzia di cui all'articolo 2-septies ((...));

b) al trasferimento dei dati verso paesi terzi o organizzazioni internazionali, contenute nel Capo V del Regolamento.

3. In caso di diffusione o di comunicazione dei dati per le finalità di cui all'articolo 136 restano fermi i limiti del diritto di cronaca a tutela dei diritti di cui all'articolo 1, paragrafo 2, del Regolamento e all'articolo 1 del presente codice e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico. Possono essere trattati i dati personali relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico.

Art. 138
(Segreto professionale)

1. In caso di richiesta dell'interessato di conoscere l'origine dei dati personali ai sensi (**dell'articolo 15, paragrafo 1, lettera g), del Regolamento**) restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

CAPO II

**((REGOLE DEONTOLOGICHE RELATIVE AD ATTIVITA' GIORNALISTICHE E AD ALTRE MANIFESTAZIONI
DEL PENSIERO))**

Art. 139
((Regole deontologiche relative ad attività giornalistiche).

1. **Il Garante promuove, ai sensi dell'articolo 2-quater, l'adozione da parte del Consiglio nazionale dell'ordine dei giornalisti di regole deontologiche relative al trattamento dei dati di cui all'articolo 136, che prevedono misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quanto riguarda quelli relativi alla salute e alla vita o all'orientamento sessuale. Le regole possono anche prevedere forme particolari per le informazioni di cui agli articoli 13 e 14 del Regolamento.**

2. **Le regole deontologiche o le modificazioni od integrazioni alle stesse che non sono adottate dal Consiglio entro sei mesi dalla**

proposta del Garante sono adottate in via sostitutiva dal Garante e sono efficaci sino a quando diviene efficace una diversa disciplina secondo la procedura di cooperazione.

3. Le regole deontologiche e le disposizioni di modificazione ed integrazione divengono efficaci quindici giorni dopo la loro pubblicazione nella Gazzetta Ufficiale della Repubblica italiana ai sensi dell'articolo 2-quater.

4. In caso di violazione delle prescrizioni contenute nelle regole deontologiche, il Garante puo' vietare il trattamento ai sensi dell'articolo 58 del Regolamento.

5. Il Garante, in cooperazione con il Consiglio nazionale dell'ordine dei giornalisti, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio e' tenuto a recepire.))

TITOLO XIII

MARKETING DIRETTO

((TITOLO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 140

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

PARTE III

TUTELA DELL'INTERESSATO E SANZIONI

TITOLO I

TUTELA AMMINISTRATIVA E GIURISDIZIONALE

((CAPO 0.I

(ALTERNATIVITA' DELLE FORME DI TUTELA))

Art. 140-bis

(((Forme alternative di tutela).

1. Qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, l'interessato puo' proporre reclamo al Garante o ricorso dinanzi all'autorita' giudiziaria.

2. Il reclamo al Garante non puo' essere proposto se, per il medesimo oggetto e tra le stesse parti, e' stata gia' adita l'autorita' giudiziaria.

3. La presentazione del reclamo al Garante rende improponibile un'ulteriore domanda dinanzi all'autorita' giudiziaria tra le stesse parti e per il medesimo oggetto, salvo quanto previsto dall'[articolo 10, comma 4, del decreto legislativo 1° settembre 2011, n. 150.](#)))

CAPO I

TUTELA DINANZI AL GARANTE

((...))

Art. 141

(((Reclamo al Garante).

1. L'interessato puo' rivolgersi al Garante mediante reclamo ai sensi dell'articolo 77 del Regolamento.))

((...))

Art. 142

((*Proposizione del reclamo*)).

1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto.

2. Il reclamo è sottoscritto dall'interessato o, su mandato di questo, da un ente del terzo settore soggetto alla disciplina del [decreto legislativo 3 luglio 2017, n. 117](#), che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati, con riguardo alla protezione dei dati personali.

3. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale mandato, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.

4. Il Garante predispone un modello per il reclamo, da pubblicare nel proprio sito istituzionale, di cui favorisce la disponibilità con strumenti elettronici.

5. Il Garante disciplina con proprio regolamento il procedimento relativo all'esame dei reclami, nonché modalità semplificate e termini abbreviati per la trattazione di reclami che abbiano ad oggetto la violazione degli articoli da 15 a 22 del Regolamento.))

Art. 143

((*Decisione del reclamo*)).

1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento può adottare i provvedimenti di cui all'articolo 58 del Regolamento nel rispetto delle disposizioni di cui all'articolo 56 dello stesso.

2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.

3. Il Garante decide il reclamo entro nove mesi dalla data di presentazione e, in ogni caso, entro tre mesi dalla predetta data informa l'interessato sullo stato del procedimento. In presenza di

motivate esigenze istruttorie, che il Garante comunica all'interessato, il reclamo e' deciso entro dodici mesi. In caso di attivazione del procedimento di cooperazione di cui all'articolo 60 del Regolamento, il termine rimane sospeso per la durata del predetto procedimento.

4. Avverso la decisione e' ammesso ricorso giurisdizionale ai sensi dell'articolo 152.))

**Art. 144
 (((Segnalazioni).**

1. Chiunque puo' rivolgere una segnalazione che il Garante puo' valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento.

2. I provvedimenti del Garante di cui all'articolo 58 del Regolamento possono essere adottati anche d'ufficio.))

**Art. 144-bis
 (((Revenge porn).))**

((1. Chiunque, compresi i minori ultraquattordicenni, abbia fondato motivo di ritenere che registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito che lo riguardano, destinati a rimanere privati, possano essere oggetto di invio, consegna, cessione, pubblicazione o diffusione attraverso piattaforme digitali senza il suo consenso ha facolta' di segnalare il pericolo al Garante, il quale, nelle quarantotto ore dal ricevimento della segnalazione, decide ai sensi degli articoli 143 e 144 del presente codice.

2. Quando le registrazioni audio, le immagini o i video o gli altri documenti informatici riguardano minori, la segnalazione al Garante puo' essere effettuata anche dai genitori o dagli esercenti la responsabilita' genitoriale o la tutela.

3. Per le finalita' di cui al comma 1, l'invio al Garante di registrazioni audio, immagini o video o altri documenti informatici a contenuto sessualmente esplicito riguardanti soggetti terzi, effettuato dall'interessato, non integra il reato di cui all'[articolo 612-ter del codice penale](#).

4. I gestori delle piattaforme digitali destinatari dei provvedimenti di cui al comma 1 conservano il materiale oggetto della segnalazione, a soli fini probatori e con misure indicate dal Garante, anche nell'ambito dei medesimi provvedimenti, idonee a impedire la diretta identificabilita' degli interessati, per dodici mesi a decorrere dal ricevimento del provvedimento stesso.

5. Il Garante, con proprio provvedimento, puo' disciplinare specifiche modalita' di svolgimento dei procedimenti di cui al comma 1 e le misure per impedire la diretta identificabilita' degli interessati di cui al medesimo comma.

6. I fornitori di servizi di condivisione di contenuti audiovisivi, ovunque stabiliti, che erogano servizi accessibili in Italia, indicano senza ritardo al Garante o pubblicano nel proprio sito internet un recapito al quale possono essere comunicati i provvedimenti adottati ai sensi del comma 1. In caso di inadempimento dell'obbligo di cui al periodo precedente, il Garante diffida il fornitore del servizio ad adempiere entro trenta giorni. In caso di inottemperanza alla diffida si applica la sanzione amministrativa pecuniaria di cui all'articolo 83, paragrafo 4, del Regolamento.

7. Quando il Garante, a seguito della segnalazione di cui al comma 1, acquisisce notizia della consumazione del reato di cui all'[articolo 612-ter del codice penale](#), anche in forma tentata, nel caso di procedibilita' d'ufficio trasmette al pubblico ministero la segnalazione ricevuta e la documentazione acquisita).

((49))

AGGIORNAMENTO (49)

Il [D.L. 8 ottobre 2021, n. 139](#), convertito con modificazioni dalla [L. 3 dicembre 2021, n. 205](#), ha disposto (con l'art. 9, comma 6) che "In fase di prima attuazione, l'obbligo di indicazione o di pubblicazione del recapito previsto dall'articolo 144-bis, comma 6, del codice di cui al [decreto legislativo n. 196 del 2003](#), introdotto dalla lettera g) del comma 1 del presente articolo, e' adempiuto nel termine di sei mesi dalla data di entrata in vigore della legge di conversione del presente decreto".

SEZIONE III

TUTELA ALTERNATIVA A QUELLA GIURISDIZIONALE

((SEZIONE ABROGATA DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 145

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 146

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 147

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 148

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 149

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 150

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 151

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO II

TUTELA GIURISDIZIONALE

Art. 152

(Autorita' giudiziaria ordinaria)

((1. Tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonche' il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo regolamento, sono attribuite all'autorita' giudiziaria ordinaria.))

1-bis. Le controversie di cui al comma 1 sono disciplinate dall'[articolo 10 del decreto legislativo 1° settembre 2011, n.](#)

150. (26)

2. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
3. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
4. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
5. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
6. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
7. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
8. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
9. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
10. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
11. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
12. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
13. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)
14. COMMA ABROGATO DAL [D.LGS. 1 SETTEMBRE 2011, N. 150.](#) (26)

AGGIORNAMENTO (26)

Il [D.Lgs. 1 settembre 2011, n. 150](#) ha disposto (con l'art. 36, commi 1 e 2) che "1. Le norme del presente decreto si applicano ai procedimenti instaurati successivamente alla data di entrata in vigore dello stesso.

2. Le norme abrogate o modificate dal presente decreto continuano ad applicarsi alle controversie pendenti alla data di entrata in vigore dello stesso."

TITOLO II

((AUTORITA' DI CONTROLLO INDIPENDENTE))

CAPO I

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Art. 153

(Garante per la protezione dei dati personali).

1. Il Garante e' composto dal Collegio, che ne costituisce il vertice, e dall'Ufficio. Il Collegio e' costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti devono essere eletti tra coloro che presentano la propria candidatura nell'ambito di una procedura di selezione il cui avviso deve essere pubblicato nei siti internet della Camera, del Senato e del Garante almeno sessanta

giorni prima della nomina. Le candidature devono pervenire almeno trenta giorni prima della nomina e i curricula devono essere pubblicati negli stessi siti internet. Le candidature possono essere avanzate da persone che assicurino indipendenza e che risultino di comprovata esperienza nel settore della protezione dei dati personali, con particolare riferimento alle discipline giuridiche o dell'informatica.

2. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vice presidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

3. L'incarico di presidente e quello di componente hanno durata settennale e non sono rinnovabili. Per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, anche non remunerata, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.

4. I membri del Collegio devono mantenere il segreto, sia durante sia successivamente alla cessazione dell'incarico, in merito alle informazioni riservate cui hanno avuto accesso nell'esecuzione dei propri compiti o nell'esercizio dei propri poteri.

5. All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'[articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382](#). Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.

6. Al presidente (***e ai componenti***) compete una indennità di funzione pari alla retribuzione in godimento al primo Presidente della Corte di cassazione, nei limiti previsti dalla legge per il trattamento economico annuo onnicomprensivo di chiunque riceva a carico delle finanze pubbliche emolumenti o retribuzioni nell'ambito di rapporti di lavoro dipendente o autonomo con pubbliche amministrazioni statali. (***L'indennità di funzione di cui al primo periodo e' da ritenere onnicomprensiva ad esclusione del rimborso delle spese effettivamente sostenute e documentate in occasione di attività istituzionali***).

7. Alle dipendenze del Garante e' posto l'Ufficio di cui all'articolo 155.

8. Il presidente, i componenti, il segretario generale e i dipendenti si astengono dal trattare, per i due anni successivi alla cessazione dell'incarico ovvero del servizio presso il Garante, procedimenti dinanzi al Garante, ivi compresa la presentazione per conto di terzi di reclami richieste di parere o interpellati.

AGGIORNAMENTO (13)

Il [D.L. 31 dicembre 2007, n. 248](#), convertito con modificazioni

dalla [L. 28 febbraio 2008, n. 31](#), ha disposto (con l'art. 47-quater, comma 1) che nelle more dell'approvazione della legge di riordino delle autorità indipendenti, la durata in carica del presidente e dei membri del Garante per la protezione dei dati personali di cui al presente articolo, comma 4, è equiparata a quella del presidente e dei membri delle autorità istituite con la [legge 10 ottobre 1990, n. 287](#), e con la [legge 31 luglio 1997, n. 249](#), con decorrenza dalla data del decreto di nomina.

Inoltre ha stabilito che tali incarichi non sono rinnovabili.

Art. 154
(Compiti).

1. Oltre a quanto previsto da specifiche disposizioni e dalla Sezione II del Capo VI del regolamento, il Garante, ai sensi dell'articolo 57, paragrafo 1, lettera v), del Regolamento medesimo, anche di propria iniziativa e avvalendosi dell'Ufficio, in conformità alla disciplina vigente e nei confronti di uno o più titolari del trattamento, ha il compito di:

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico;

b) trattare i reclami presentati ai sensi del regolamento, e delle disposizioni del presente codice, anche individuando con proprio regolamento modalità specifiche per la trattazione, nonché fissando annualmente le priorità delle questioni emergenti dai reclami che potranno essere istruite nel corso dell'anno di riferimento;

c) promuovere l'adozione di regole deontologiche, nei casi di cui all'articolo 2-quater;

d) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;

e) trasmettere la relazione, predisposta annualmente ai sensi dell'articolo 59 del Regolamento, al Parlamento e al Governo entro il 31 maggio dell'anno successivo a quello cui si riferisce;

f) assicurare la tutela dei diritti e delle libertà fondamentali degli individui dando idonea attuazione al Regolamento e al presente codice;

g) provvedere altresì all'espletamento dei compiti ad esso attribuiti dal diritto dell'Unione europea o dello Stato e svolgere le ulteriori funzioni previste dall'ordinamento.

2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da atti comunitari o dell'Unione europea e, in particolare:

a) dal [Regolamento \(CE\) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006](#), sull'istituzione, l'esercizio e

l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) e [Decisione 2007/533/GAI](#) del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II);

b) dal [Regolamento \(UE\) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016](#), che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le [decisioni del Consiglio 2009/371/GAI](#), [2009/934/GAI](#), [2009/935/GAI](#), [2009/936/GAI](#) e [2009/968/GAI](#);

c) dal [Regolamento \(UE\) 2015/1525 del Parlamento europeo e del Consiglio, del 9 settembre 2015](#), che modifica il [Regolamento \(CE\) n. 515/97 del Consiglio](#) relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola e [decisione 2009/917/GAI](#) del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale;

d) dal [Regolamento \(CE\) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013](#), che istituisce l'Eurodac per il confronto delle impronte digitali per l'efficace applicazione del [Regolamento \(UE\) n. 604/2013](#) che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il [Regolamento \(UE\) n. 1077/2011](#) che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia;

e) dal [Regolamento \(CE\) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008](#), concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (Regolamento VIS) e [decisione n. 2008/633/GAI](#) del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi;

f) dal [Regolamento \(CE\) n. 1024/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012](#), relativo alla cooperazione amministrativa attraverso il sistema di informazione del mercato interno e che abroga la [decisione 2008/49/CE della Commissione \(Regolamento IMI\)](#) Testo rilevante ai fini del SEE;

g) dalle disposizioni di cui al capitolo IV della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con [legge 21 febbraio 1989, n. 98](#), quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.

3. Per quanto non previsto dal Regolamento e dal presente codice, il Garante disciplina con proprio Regolamento, ai sensi dell'articolo 156, comma 3, le modalita' specifiche dei procedimenti relativi all'esercizio dei compiti e dei poteri ad esso attribuiti dal Regolamento e dal presente codice.

4. Il Garante collabora con altre autorità amministrative indipendenti nazionali nello svolgimento dei rispettivi compiti.

5. Fatti salvi i termini piu' brevi previsti per legge, il parere del Garante, anche nei casi di cui agli articoli 36, paragrafo 4, del Regolamento, e' reso nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione puo' procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non puo' essere rispettato il termine di cui al presente comma, tale termine puo' essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.

((5-bis. Il parere di cui all'articolo 36, paragrafo 4, del Regolamento e' reso dal Garante nei soli casi in cui la legge o il regolamento in corso di adozione disciplina espressamente le modalita' del trattamento descrivendo una o piu' operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione, nonche' nei casi in cui la norma di legge o di regolamento autorizza espressamente un trattamento di dati personali da parte di soggetti privati senza rinviare la disciplina delle modalita' del trattamento a fonti subordinate.

5-ter. Quando il Presidente del Consiglio dei ministri dichiara che ragioni di urgenza non consentono la consultazione preventiva e comunque nei casi di adozione di decreti-legge, il Garante esprime il parere di cui al comma 5-bis:

a) in sede di esame parlamentare dei disegni di legge o dei disegni di legge di conversione dei decreti-legge;

b) in sede di esame definitivo degli schemi di decreto legislativo sottoposti al parere delle Commissioni parlamentari).

6. Copia dei provvedimenti emessi dall'autorita' giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalita' informatica e' trasmessa, a cura della cancelleria, al Garante.

7. Il Garante non e' competente per il controllo dei trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni.

Art. 154-bis
((Poteri).

1. Oltre a quanto previsto da specifiche disposizioni, dalla Sezione II del Capo VI del Regolamento e dal presente codice, ai sensi dell'articolo 58, paragrafo 6, del Regolamento medesimo, il Garante ha il potere di:

a) adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento;

b) approvare le regole deontologiche di cui all'articolo 2-quater.

2. Il Garante puo' invitare rappresentanti di un'altra autorita' amministrativa indipendente nazionale a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorita' amministrativa indipendente nazionale, prendendo parte alla discussione di argomenti di comune interesse; puo' richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorita' amministrativa indipendente nazionale.

3. Il Garante pubblica i propri provvedimenti sulla base di quanto previsto con atto di natura generale che disciplina anche la durata di tale pubblicazione, la pubblicita' nella Gazzetta Ufficiale della Repubblica italiana e sul proprio sito internet istituzionale nonche' i casi di oscuramento.

4. In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, come definite dalla [raccomandazione 2003/361/CE](#), il Garante per la protezione dei dati personali, nel rispetto delle disposizioni del Regolamento e del presente Codice, promuove, nelle linee guida adottate a norma del comma 1, lettera a), modalita' semplificate di adempimento degli obblighi del titolare del trattamento.))

Art. 154-ter
((Potere di agire e rappresentanza in giudizio).

1. Il Garante e' legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali.

2. Il Garante e' rappresentato in giudizio dall'Avvocatura dello Stato, ai sensi dell'[articolo 1 del regio decreto 30 ottobre 1933, n. 1611](#).

3. Nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato, puo' stare in giudizio tramite propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero avvocati del libero foro.))

CAPO II

L'UFFICIO DEL GARANTE

Art. 155

((Ufficio del Garante))

1. All'Ufficio del Garante, al fine di garantire la responsabilita' e l'autonomia ai sensi della [legge 7 agosto 1990, n. 241](#), e successive modificazioni, e del [decreto legislativo 30 marzo 2001, n. 165](#), e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonche' quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e le funzioni di gestione attribuite ai dirigenti. Si applicano altresì le disposizioni del medesimo [decreto legislativo n. 165 del 2001](#) espressamente richiamate dal presente codice.

Art. 156

(Ruolo organico e personale).

1. All'Ufficio del Garante e' preposto un segretario generale, nominato tra persone di elevata e comprovata qualificazione professionale rispetto al ruolo e agli obiettivi da conseguire, scelto anche tra i magistrati ordinari, amministrativi e contabili, gli avvocati dello Stato, i professori universitari di ruolo in materie giuridiche ed economiche, nonche' i dirigenti di prima fascia dello Stato.

2. **((A decorrere dal 1° gennaio 2022, il ruolo organico del personale dipendente e' stabilito nel limite di duecento unita'))**. Al ruolo organico del Garante si accede esclusivamente mediante concorso pubblico. Nei casi in cui sia ritenuto utile al fine di garantire l'economicita' e l'efficienza dell'azione amministrativa, nonche' di favorire il reclutamento di personale con maggiore esperienza nell'ambito delle procedure concorsuali di cui al secondo periodo, il Garante puo' riservare una quota non superiore al cinquanta per cento dei posti banditi al personale di ruolo delle amministrazioni pubbliche che sia stato assunto per concorso pubblico e abbia maturato un'esperienza almeno triennale nel rispettivo ruolo

organico. La disposizione di cui all'[articolo 30 del decreto legislativo 30 marzo 2001, n. 165](#), si applica esclusivamente nell'ambito del personale di ruolo delle autorità amministrative indipendenti di cui all'[articolo 22, comma 1, del decreto-legge 24 giugno 2014, n. 90](#), convertito, con modificazioni, dalla [legge 11 agosto 2014, n.114](#).

3. Con propri regolamenti pubblicati nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce:

a) l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti e dell'esercizio dei poteri di cui agli articoli 154, 154-bis, 160, nonché all'articolo 57, paragrafo 1, del Regolamento;

b) l'ordinamento delle carriere e le modalità di reclutamento del personale secondo i principi e le procedure di cui agli [articoli 1, 35 e 36 del decreto legislativo n. 165 del 2001](#);

c) la ripartizione dell'organico tra le diverse aree e qualifiche;

d) il trattamento giuridico ed economico del personale, secondo i criteri previsti dalla [legge 31 luglio 1997, n. 249](#), e, per gli incarichi dirigenziali, dagli articoli 19, comma 6, e 23-bis del [decreto legislativo 30 marzo 2001, n. 165](#), tenuto conto delle specifiche esigenze funzionali e organizzative. Nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti, al personale è attribuito (**il trattamento**) economico del personale dell'Autorità per le garanzie nelle comunicazioni;

e) la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato.

4. L'Ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'[articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382](#), in numero non superiore, complessivamente, a (**trenta unità**) e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo.

5. In aggiunta al personale di ruolo, l'Ufficio può assumere dipendenti con contratto a tempo determinato o avvalersi di consulenti incaricati ai sensi dell'[articolo 7, comma 6, del decreto legislativo n. 165 del 2001](#), in misura comunque non superiore a (**trenta unità**) complessive. Resta in ogni caso fermo, per i contratti a tempo determinato, il rispetto dell'[articolo 36 del decreto legislativo n. 165 del 2001](#).

6. Il personale addetto all'Ufficio del Garante ed i consulenti sono tenuti, sia durante che dopo il mandato, al segreto su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

7. Il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'articolo 158 e agli articoli 57, paragrafo 1, lettera h), 58, paragrafo 1, lettera b), e 62, del Regolamento riveste, nei limiti del servizio cui e' destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.

8. Le spese di funzionamento del Garante, in adempimento all'articolo 52, paragrafo 4, del Regolamento, ivi comprese quelle necessarie ad assicurare la sua partecipazione alle procedure di cooperazione e al meccanismo di coerenza introdotti dal Regolamento, nonche' quelle connesse alle risorse umane, tecniche e finanziarie, ai locali e alle infrastrutture necessarie per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposita missione e programma di spesa del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria e' soggetto al controllo della Corte dei conti. Il Garante puo' esigere dal titolare del trattamento il versamento di diritti di segreteria in relazione a particolari procedimenti.

AGGIORNAMENTO (29)

La [L. 27 dicembre 2013, n. 147](#) ha disposto (con l'art. 1, comma 268) che "Al fine di non disperdere la professionalita' acquisita dal personale con contratto di lavoro subordinato a tempo determinato assunto a seguito di superamento di apposita procedura selettiva pubblica, per titoli ed esami, nonche' per fare fronte agli accresciuti compiti derivanti dalla partecipazione alle attivita' di cooperazione fra autorita' di protezione di dati dell'Unione europea, il ruolo organico di cui all'articolo 156, comma 2, del codice di cui al [decreto legislativo 30 giugno 2003, n. 196](#), come incrementato in attuazione dell'[articolo 1, comma 542, della legge 27 dicembre 2006, n. 296](#), e' incrementato di dodici unita', previa contestuale riduzione nella medesima misura del contingente di cui al comma 5 del predetto articolo 156 del codice di cui al [decreto legislativo n. 196 del 2003](#)".

AGGIORNAMENTO (33)

La [L. 20 novembre 2017, n. 167](#) ha disposto (con l'art. 29, comma 1) che "Al fine di assicurare il regolare esercizio dei poteri di controllo affidati al Garante per la protezione dei dati personali e per fare fronte agli accresciuti compiti derivanti dalla partecipazione alle attivita' di cooperazione fra autorita' di protezione di dati dell'Unione europea, e' attribuito, a decorrere dall'anno 2018, un contributo aggiuntivo pari a 1.400.000 euro. Per le finalita' di cui al primo periodo, il ruolo organico di cui all'[articolo 156, comma 2, del codice in materia di protezione dei dati personali](#), di cui al [decreto legislativo 30 giugno 2003, n. 196](#),

come incrementato in attuazione dell'[articolo 1, comma 542, della legge 27 dicembre 2006, n. 296](#), e successivamente dall'[articolo 1, comma 268, della legge 27 dicembre 2013, n. 147](#), e' incrementato di 25 unita'; e' autorizzata a questo fine la spesa di euro 887.250 per l'anno 2017 e di euro 2.661.750 annui a decorrere dall'anno 2018".

CAPO III

ACCERTAMENTI E CONTROLLI

Art. 157

((Richiesta di informazioni e di esibizione di documenti).))

((1. Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante puo' richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati.))

Art. 158

((Accertamenti).))

((1. Il Garante puo' disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1, nonche' quelli effettuati ai sensi dell'articolo 62 del Regolamento, sono eseguiti da personale dell'Ufficio, con la partecipazione, se del caso, di componenti o personale di autorita' di controllo di altri Stati membri dell'Unione europea.

3. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali.

4. Gli accertamenti di cui ai commi 1 e 2, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative

appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al piu' tardi entro tre giorni dal ricevimento della richiesta del Garante quando e' documentata l'indifferibilita' dell'accertamento.

5. Con le garanzie di cui al comma 4, gli accertamenti svolti nei luoghi di cui al medesimo comma possono altresì riguardare reti di comunicazione accessibili al pubblico, potendosi procedere all'acquisizione di dati e informazioni on-line. A tal fine, viene redatto apposito verbale in contraddittorio con le parti ove l'accertamento venga effettuato presso il titolare del trattamento.)

Art. 159
(Modalita)

1. Il personale operante, munito di documento di riconoscimento, puo' essere assistito ove necessario da consulenti tenuti al segreto **((su cio' di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete))**. Nel procedere a rilievi e ad operazioni tecniche puo' altresì estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Degli accertamenti e' redatto sommario verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

2. Ai soggetti presso i quali sono eseguiti gli accertamenti e' consegnata copia dell'autorizzazione del presidente del tribunale, ove rilasciata. I medesimi soggetti sono tenuti a farli eseguire e a prestare la collaborazione a tal fine necessaria. In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese in tal caso occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento, che per questa parte costituisce titolo esecutivo ai sensi degli [articoli 474 e 475 del codice di procedura civile](#).

3. Gli accertamenti, se effettuati presso il titolare o il responsabile **((o il rappresentante del titolare o del responsabile))**, sono eseguiti dandone informazione a quest'ultimo o, se questo e' assente o non e' designato, **((alle persone autorizzate al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile ai sensi dell'articolo 2-quaterdecies))**. Agli accertamenti possono assistere persone indicate dal titolare o dal responsabile.

4. Se non e' disposto diversamente nel decreto di autorizzazione del presidente del tribunale, l'accertamento non puo' essere iniziato prima delle ore sette e dopo le ore venti, e puo' essere eseguito anche con preavviso quando cio' puo' facilitarne l'esecuzione.

5. Le informative, le richieste e i provvedimenti di cui al

presente articolo e agli articoli 157 e 158 possono essere trasmessi anche mediante posta elettronica ((...)).

6. Quando emergono indizi di reato si osserva la disposizione di cui all'articolo 220 delle norme di attuazione, di coordinamento e transitorie del [codice di procedura penale](#), approvate con [decreto legislativo 28 luglio 1989, n. 271](#).

Art. 160

((*Particolari accertamenti*).))

((1. Per i trattamenti di dati personali di cui all'articolo 58, gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.

2. Se il trattamento non risulta conforme alle norme del Regolamento ovvero alle disposizioni di legge o di Regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento e' stato richiesto dall'interessato, a quest'ultimo e' fornito in ogni caso un riscontro circa il relativo esito, se cio' non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato.

3. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificita' della verifica, il componente designato puo' farsi assistere da personale specializzato tenuto al segreto su cio' di cui sono venuti a conoscenza in ordine a notizie che devono rimanere segrete. Gli atti e i documenti acquisiti sono custoditi secondo modalita' tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal Regolamento di cui all'articolo 156, comma 3, lettera a).

4. Per gli accertamenti di cui al comma 3 relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.)) ((39))

AGGIORNAMENTO (39)

Il [D.Lgs. 10 agosto 2018, n. 101](#) ha disposto (con l'art. 22, comma 10) che "La disposizione di cui all'[articolo 160, comma 4, del codice in materia di protezione dei dati personali](#), di cui al [decreto legislativo n. 196 del 2003](#), nella parte in cui ha riguardo ai dati coperti da segreto di Stato, si applica fino alla data di entrata in vigore della disciplina relativa alle modalita' di opposizione al Garante per la protezione dei dati personali del segreto di Stato".

Art. 160-bis

((Validita', efficacia e utilizzabilita' nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento).))

((1. La validita', l'efficacia e l'utilizzabilita' nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali.))

TITOLO III

SANZIONI

CAPO I

VIOLAZIONI AMMINISTRATIVE

Art. 161

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 162

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 162-bis

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 162-ter

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 163

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 164

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 164-bis

((**ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)**))

Art. 165

((**ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)**))

Art. 166

(Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori).

1. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 4, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-quinquies, comma 2, ((...)), 92, comma 1, 93, comma 1, 123, comma 4, 128, 129, comma 2, e 132-ter. Alla medesima sanzione amministrativa e' soggetto colui che non effettua la valutazione di impatto di cui all'articolo 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma.

2. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-ter, 2-quinquies, comma 1, 2-sexies, 2-septies, comma 8, 2-octies, 2-terdecies, commi 1, 2, 3 e 4, 52, commi 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110-bis, commi 2 e 3, 111, 111-bis, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 5, 131, 132, 132-bis, comma 2, 132-quater, 157, nonche' delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-septies e 2-quater.

3. Il Garante e' l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58, paragrafo 2, del Regolamento, nonche' ad irrogare le sanzioni di cui all'articolo 83 del medesimo Regolamento e di cui ai commi 1 e 2.

4. Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 3 puo' essere avviato, nei confronti sia di soggetti privati, sia di autorita' pubbliche ed organismi pubblici, a seguito di reclamo ai sensi dell'articolo 77 del Regolamento o di attivita' istruttoria d'iniziativa del Garante, nell'ambito dell'esercizio dei poteri d'indagine di cui all'articolo 58, paragrafo 1, del Regolamento, nonche' in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante.

5. L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attivita' di cui al comma 4 configurino una o piu' violazioni indicate nel presente titolo e nell'articolo 83, paragrafi

4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 notificando al titolare o al responsabile del trattamento le presunte violazioni, nel rispetto delle garanzie previste dal Regolamento di cui al comma 9, salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalità del provvedimento da adottare. ***((Nei confronti dei titolari del trattamento di cui agli articoli 2-ter, comma 1-bis, e 58 del presente codice e all'[articolo 1, comma 1, del decreto legislativo 18 maggio 2018, n. 51](#), la predetta notifica può essere omessa esclusivamente nel caso in cui il Garante abbia accertato che le presunte violazioni hanno già arrecato e continuano ad arrecare un effettivo, concreto, attuale e rilevante pregiudizio ai soggetti interessati al trattamento, che il Garante ha l'obbligo di individuare e indicare nel provvedimento, motivando puntualmente le ragioni dell'omessa notifica. In assenza di tali presupposti, il giudice competente accerta l'inefficacia del provvedimento))***.

6. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 5, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità.

7. Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 3 si osservano, in quanto applicabili, gli [articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689](#); nei medesimi casi può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante ***((o dell'ingiunzione a realizzare campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali, sulla base di progetti previamente approvati dal Garante e che tengano conto della gravità della violazione. Nella determinazione della sanzione ai sensi dell'articolo 83, paragrafo 2, del Regolamento, il Garante tiene conto anche di eventuali campagne di comunicazione istituzionale volte alla promozione della consapevolezza del diritto alla protezione dei dati personali, realizzate dal trasgressore anteriormente alla commissione della violazione))***. I proventi delle sanzioni, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 8, per essere destinati alle specifiche attività di sensibilizzazione e di ispezione nonché di attuazione del Regolamento svolte dal Garante.

8. Entro il termine di cui all'[articolo 10, comma 3, del decreto legislativo n. 150 del 2011](#) previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla metà della sanzione irrogata.

9. Nel rispetto dell'articolo 58, paragrafo 4, del Regolamento, con

proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce le modalita' del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 3 ed i relativi termini, in conformita' ai principi della piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione, nonche' della distinzione tra funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione.

10. Le disposizioni relative a sanzioni amministrative previste dal presente codice e dall'articolo 83 del Regolamento non si applicano in relazione ai trattamenti svolti in ambito giudiziario.

CAPO II

ILLECITI PENALI

Art. 167

(Trattamento illecito di dati).

1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocimento all'interessato, e' punito con la reclusione da sei mesi a un anno e sei mesi.

2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ((...)) arreca nocimento all'interessato, e' punito con la reclusione da uno a tre anni.

3. Salvo che il fatto costituisca piu' grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocimento all'interessato.

4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.

5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attivita' di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al piu' tardi al termine dell'attivita' di accertamento delle violazioni delle disposizioni di cui al presente decreto.

6. Quando per lo stesso fatto e' stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa e' stata riscossa, la pena e' diminuita.

Art. 167-bis

((Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala).))

((1. Salvo che il fatto costituisca piu' grave reato, chiunque comunica o diffonde al fine di trarre profitto per se' o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, e' punito con la reclusione da uno a sei anni.

2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, e' punito con la reclusione da uno a sei anni, quando il consenso dell'interessato e' richiesto per le operazioni di comunicazione e di diffusione.

3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.))

Art. 167-ter

((Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala).))

((1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, acquisisce con mezzi fraudolenti un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala e' punito con la reclusione da uno a quattro anni.

2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.))

Art. 168

(((Falsita' nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante).))

((1. Salvo che il fatto costituisca piu' grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, e' punito con la reclusione da sei mesi a tre anni.

2. Fuori dei casi di cui al comma 1, e' punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarita' di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.))

Art. 169

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 170

(Inosservanza di provvedimenti del Garante).

1. Chiunque, **((non osservando))** il provvedimento adottato dal Garante ai sensi degli articoli 58, paragrafo 2, lettera f) del Regolamento, dell'articolo 2-septies, comma 1, nonche' i provvedimenti generali di cui all'articolo 21, comma 1, del decreto legislativo di attuazione dell'[articolo 13 della legge 25 ottobre 2017, n. 163](#) **((, arreca un concreto nocumento a uno o piu' soggetti interessati al trattamento))** e' punito **((, a querela della persona offesa,))** con la reclusione da tre mesi a due anni.

Art. 171

(((Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori).))

((1. La violazione delle disposizioni di cui agli articoli 4, comma 1, e 8 della [legge 20 maggio 1970, n. 300](#), e' punita con le sanzioni di cui all'articolo 38 della medesima legge.))

Art. 172

(Pene accessorie)

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza **((, ai sensi dell'[articolo 36, secondo](#) e [terzo comma, del codice penale](#))).**

TITOLO IV

DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI

CAPO I

DISPOSIZIONI DI MODIFICA

Art. 173

((**ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)**))

Art. 174

((**ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)**))

Art. 175

(Forze di polizia)

1. ((**COMMA ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)**)).
2. ((**COMMA ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)**)).
3. L'[articolo 10 della legge 1 aprile 1981, n. 121](#), e successive modificazioni, e' sostituito dal seguente:

"Art. 10 (Controlli)

1. Il controllo sul Centro elaborazione dati e' esercitato dal Garante per la protezione dei dati personali, nei modi previsti dalla legge e dai regolamenti.

2. I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie indicate nel primo comma dell'articolo 7, fermo restando quanto stabilito dall'[articolo 240 del codice di procedura penale](#). Quando nel corso di un procedimento giurisdizionale o amministrativo viene rilevata l'erroneita' o l'incompletezza dei dati e delle informazioni, o l'illegittimita' del loro trattamento, l'autorita' precedente ne da' notizia al Garante per la protezione dei dati personali.

3. La persona alla quale si riferiscono i dati puo' chiedere all'ufficio di cui alla lettera a) del primo comma dell'articolo 5 la conferma dell'esistenza di dati personali che lo riguardano, la loro comunicazione in forma intellegibile e, se i dati risultano trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.

4. Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre trenta giorni dalla richiesta, le

determinazioni adottate. L'ufficio puo' omettere di provvedere sulla richiesta se cio' puo' pregiudicare azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalita', dandone informazione al Garante per la protezione dei dati personali.

5. Chiunque viene a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, puo' chiedere al tribunale del luogo ove risiede il titolare del trattamento di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi."

Art. 176

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 177

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 178

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 179

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

CAPO II

DISPOSIZIONI TRANSITORIE

((CAPO ABROGATO DAL D.LGS. 10 AGOSTO 2018, N. 101))

Art. 180

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#))

Art. 181

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 182

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

CAPO III

ABROGAZIONI

Art. 183

(Norme abrogate)

1. Dalla data di entrata in vigore del presente codice sono abrogati:

- a) la [legge 31 dicembre 1996, n. 675](#);
- b) la [legge 3 novembre 2000, n. 325](#);
- c) il [decreto legislativo 9 maggio 1997, n. 123](#);
- d) il [decreto legislativo 28 luglio 1997, n. 255](#);
- e) l'[articolo 1 del decreto legislativo 8 maggio 1998, n. 135](#);
- f) il [decreto legislativo 13 maggio 1998, n. 171](#);
- g) il [decreto legislativo 6 novembre 1998, n. 389](#);
- h) il [decreto legislativo 26 febbraio 1999, n. 51](#);
- i) il [decreto legislativo 11 maggio 1999, n. 135](#);
- l) il [decreto legislativo 30 luglio 1999, n. 281](#), ad eccezione degli articoli 8, comma 1, 11 e 12;
- m) il [decreto legislativo 30 luglio 1999, n. 282](#);
- n) il [decreto legislativo 28 dicembre 2001, n. 467](#);
- o) il [decreto del Presidente della Repubblica 28 luglio 1999, n. 318](#).

2. Dalla data di entrata in vigore del presente codice sono abrogati gli [articoli 12, 13, 14, 15, 16, 17, 18, 19 e 20 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501](#).

3. Dalla data di entrata in vigore del presente codice sono o restano, altresì, abrogati:

- a) [l'art. 5, comma 9, del decreto del Ministro della sanita' 18 maggio 2001, n. 279](#), in materia di malattie rare;
- b) [l'articolo 12 della legge 30 marzo 2001, n. 152](#);
- c) [l'articolo 4, comma 3, della legge 6 marzo 2001, n. 52](#), in materia di donatori midollo osseo;
- d) [l'articolo 16, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445](#), in materia di certificati di assistenza al parto;
- e) [l'art. 2, comma 5, del decreto del Ministro della sanita' 27 ottobre 2000, n. 380](#), in materia di flussi informativi sui dimessi dagli istituti di ricovero;
- f) [l'articolo 2, comma 5-quater 1, secondo e terzo periodo, del decreto-legge 28 marzo 2000, n. 70](#), convertito, con modificazioni, dalla [legge 26 maggio 2000, n. 137](#), e successive modificazioni, in materia di banca dati sinistri in ambito assicurativo;
- g) [l'articolo 6, comma 4, del decreto legislativo 5 giugno 1998, n. 204](#), in materia di diffusione di dati a fini di ricerca e collaborazione in campo scientifico e tecnologico;
- h) [l'articolo 330-bis del decreto legislativo 16 aprile 1994, n. 297](#), in materia di diffusione di dati relativi a studenti;
- i) [l'articolo 8, quarto comma, e l'articolo 9, quarto comma, della legge 1 aprile 1981, n. 121](#).

4. Dalla data in cui divengono efficaci le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 118, i termini di conservazione dei dati personali individuati ai sensi dell'articolo 119, eventualmente previsti da norme di legge o di regolamento, si osservano nella misura indicata dal medesimo codice.

CAPO IV

NORME FINALI

Art. 184

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 185

((ARTICOLO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

Art. 186
(Entrata in vigore)

1. Le disposizioni di cui al presente codice entrano in vigore il 1 gennaio 2004, ad eccezione delle disposizioni di cui agli articoli 156, 176, commi 3, 4, 5 e 6, e 182, che entrano in vigore il giorno successivo alla data di pubblicazione del presente codice. Dalla medesima data si osservano altresì i termini in materia di ricorsi di cui agli articoli 149, comma 8, e 150, comma 2.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana.

E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 30 giugno 2003

CIAMPI

BERLUSCONI, Presidente del Consiglio dei Ministri
MAZZELLA, Ministro per la funzione pubblica
BUTTIGLIONE, Ministro per le politiche comunitarie
CASTELLI, Ministro della giustizia
TREMONTI, Ministro dell'economia e delle finanze
FRATFINI, Ministro degli affari esteri
GASPARRI, Ministro delle comunicazioni

Visto, il Guardasigilli: CASTELLI

ALLEGATO A.1

REGOLE DEONTOLOGICHE RELATIVE AL TRATTAMENTO DEI DATI PERSONALI NELL'ESERCIZIO
DELL'ATTIVITA' GIORNALISTICA

Regole deontologiche (ALLEGATO A)

(Delibera del Garante n. 491 del 29 novembre 2018, in G.U. 4 gennaio 2019, n. 3)

**((IL GARANTE
PER LA PROTEZIONE DEI DATI PERSONALI**

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il [regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la [direttiva 95/46/CE](#) (di seguito, «regolamento»);

Visto il [Codice in materia di protezione dei dati personali](#), recante disposizioni per l'adeguamento dell'ordinamento nazionale al [regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016](#), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva 95/46/CE](#) ([decreto legislativo 30 giugno 2003, n. 196](#), come modificato dal [decreto legislativo 10 agosto 2018, n. 101](#), di seguito «Codice»);

Visto l'art. 85 del citato regolamento che demanda al diritto degli Stati membri il compito di conciliare la protezione dei dati personali con il diritto alla libertà di espressione e di informazione, ivi incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria, anche attraverso l'introduzione di esenzioni o deroghe ai principi dettati dal regolamento per la generalità dei trattamenti (cfr. art. 85, par. 2, del regolamento);

Visto il Titolo XII del [Codice in materia di protezione dei dati personali](#), così come modificato dall'[art. 12 del decreto legislativo n. 101/2018](#), che, oltre a ridefinire l'ambito oggettivo del trattamento, includendovi anche quello effettuato nel contesto di attività di manifestazione del pensiero in campo accademico e letterario, prevede specificamente che il trattamento dei dati indicati dagli articoli 9, par. 1, e 10, del regolamento, ovvero dei dati particolari e dei dati relativi a condanne penali e reati, debba avvenire nel rispetto delle regole deontologiche il cui rispetto costituisce condizione essenziale per la liceità e la correttezza del trattamento di dati personali ai sensi dell'art. 2-quater, comma 4, del Codice;

Visto l'[art. 20, comma 4, del decreto legislativo n. 101/2018](#) che demanda al Garante il compito di effettuare, nel termine di novanta giorni dall'entrata in vigore del decreto stesso, una verifica della conformità al regolamento delle disposizioni contenute in alcuni

codici deontologici ivi indicati, tra i quali quelle contenute nel «Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica», adottato il 29 luglio 1998, attualmente inserito nel Codice in materia di protezione come allegato A.1 ed applicabile sino al completamento della menzionata procedura;

Rilevato che, sempre secondo quanto previsto dal citato [art. 20, comma 4, del decreto legislativo n. 101/2018](#), al termine della suddetta procedura di verifica, le «disposizioni ritenute compatibili, ridenominate regole deontologiche, sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono successivamente riportate nell'allegato A del Codice»;

Ritenuto che la valutazione di compatibilità di dette disposizioni con il regolamento non possa prescindere da una loro lettura che tenga integralmente conto del mutato quadro normativo di riferimento;

Ritenuto, per tale ragione, che:

i richiami alla [legge 31 dicembre 1996, n. 675](#) ed alla [direttiva 95/46/CE](#) contenuti in alcune disposizioni del codice deontologico debbano intendersi riferiti alle corrispondenti disposizioni del regolamento e del [Codice in materia di protezione dei dati personali](#), come modificato dal [d.lgs. n. 101/2018](#);

eventuali modifiche normative rilevanti nella disciplina di specie - quali l'inclusione dei dati genetici e dei dati biometrici fra le categorie di dati particolari - debbano essere prese in considerazione per determinare la compatibilità delle disposizioni esistenti con il quadro normativo attuale;

Ritenuto che tali elementi, relativi all'aggiornamento della disciplina in materia, debbano essere recepiti nelle «Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica» in ragione di quanto disposto dall'[art. 20, comma 4, del decreto legislativo n. 101/2018](#);

Ritenuto, all'esito della verifica della conformità al regolamento delle disposizioni previste nel «Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica», che le medesime, riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante, debbano essere pubblicate ai sensi dell'[art. 20, comma 4, del decreto legislativo n. 101/2018](#) come «Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attività giornalistica»;

Considerato che le predette «Regole deontologiche» sono volte a disciplinare i trattamenti in questione in attesa di un auspicabile aggiornamento delle stesse ai sensi degli articoli 2-quater e 136 del Codice;

Ritenuto di disporre la trasmissione delle suddette «Regole deontologiche» all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la relativa pubblicazione nella

Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'Allegato A) al Codice;

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

Tutto cio' premesso il Garante

ai sensi dell'[art. 20, comma 4, del decreto legislativo n. 101/2018](#), verificata la conformita' al regolamento delle disposizioni del «Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attivita' giornalistica», dispone che le medesime, riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante, siano pubblicate come «Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attivita' giornalistica» e ne dispone, altresì, la trasmissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'Allegato A) al Codice.

Roma, 29 novembre 2018

Il presidente e relatore: Soro

Il segretario generale: Busia

A.1. Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'attivita' giornalistica))

Art. 1.

((Principi generali))

((1. Le presenti norme sono volte a contemperare i diritti fondamentali della persona con il diritto dei cittadini all'informazione e con la liberta' di stampa.

2. In forza dell'[art. 21 della Costituzione](#), la professione giornalistica si svolge senza autorizzazioni o censure. In quanto condizione essenziale per l'esercizio del diritto dovere di cronaca, la raccolta, la registrazione, la conservazione e la diffusione di notizie su eventi e vicende relativi a persone, organismi collettivi, istituzioni, costumi, ricerche scientifiche e movimenti di pensiero, attuate nell'ambito dell'attivita' giornalistica e per gli scopi propri di tale attivita', si differenziano nettamente per la loro

natura dalla memorizzazione e dal trattamento di dati personali ad opera di banche dati o altri soggetti. Su questi principi trovano fondamento le necessarie deroghe previste dal considerando 153 e dall'[art. 85 del regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) (di seguito «regolamento») e dal decreto legislativo 30 giugno, 2003, n. 196 ([Codice in materia di protezione dei dati personali](#), di seguito «Codice»), così come modificato dal [decreto legislativo 10 agosto 2018, n. 101](#))).

Art. 2

((Banche dati di uso redazionale e tutela degli archivi personali dei giornalisti))

((1. Il giornalista che raccoglie notizie per una delle operazioni di cui all'art. 4, n. 2, del regolamento rende note la propria identità, la propria professione e le finalità della raccolta salvo che ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa; evita artifici e pressioni indebite. Fatta palese tale attività, il giornalista non è tenuto a fornire gli altri elementi dell'informativa di cui agli articoli 13 e 14 del regolamento.

2. Se i dati personali sono raccolti presso banche dati di uso redazionale, le imprese editoriali sono tenute a rendere noti al pubblico, mediante annunci, almeno due volte l'anno, l'esistenza dell'archivio e il luogo dove è possibile esercitare i diritti previsti dal regolamento. Le imprese editoriali indicano altresì fra i dati della gerenza il responsabile del trattamento al quale le persone interessate possono rivolgersi per esercitare i diritti previsti dal regolamento.

3. Gli archivi personali dei giornalisti, comunque funzionali all'esercizio della professione e per l'esclusivo perseguimento delle relative finalità, sono tutelati, per quanto concerne le fonti delle notizie, ai sensi dell'[art. 2 della legge n. 69/1963](#) e dell'art. 14, par. 5, lett. d), del regolamento, nonché dell'art. 138 del Codice.

4. Il giornalista può conservare i dati raccolti per tutto il tempo necessario al perseguimento delle finalità proprie della sua professione)).

Art. 3

((Tutela del domicilio))

((1. La tutela del domicilio e degli altri luoghi di privata dimora si estende ai luoghi di cura, detenzione o riabilitazione, nel rispetto delle norme di legge e dell'uso corretto di tecniche invasive)).

Art. 4

((Rettifica))

((1. Il giornalista corregge senza ritardo errori e inesattezze, anche in conformita' al dovere di rettifica nei casi e nei modi stabiliti dalla legge)).

Art. 5**((Diritto all'informazione e dati personali))**

((1. Nel raccogliere dati personali atti a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesioni a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonche' dati genetici, biometrici intesi a identificare in modo univoco una persona fisica e dati atti a rivelare le condizioni di salute e la sfera sessuale, il giornalista garantisce il diritto all'informazione su fatti di interesse pubblico, nel rispetto dell'essenzialita' dell'informazione, evitando riferimenti a congiunti o ad altri soggetti non interessati ai fatti.

2. In relazione a dati riguardanti circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico, e' fatto salvo il diritto di addurre successivamente motivi legittimi meritevoli di tutela)).

Art. 6**((Essenzialita' dell'informazione))**

((1. La divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalita' del fatto o della relativa descrizione dei modi particolari in cui e' avvenuto, nonche' della qualificazione dei protagonisti.

2. La sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica.

3. Commenti e opinioni del giornalista appartengono alla liberta' di informazione nonche' alla liberta' di parola e di pensiero costituzionalmente garantita a tutti)).

Art. 7**((Tutela del minore))**

((1. Al fine di tutelarne la personalita', il giornalista non

pubblica i nomi dei minori coinvolti in fatti di cronaca, ne' fornisce particolari in grado di condurre alla loro identificazione.

2. La tutela della personalita' del minore si estende, tenuto conto della qualita' della notizia e delle sue componenti, ai fatti che non siano specificamente reati.

3. Il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca; qualora, tuttavia, per motivi di rilevante interesse pubblico e fermo restando i limiti di legge, il giornalista decida di diffondere notizie o immagini riguardanti minori, dovra' farsi carico della responsabilita' di valutare se la pubblicazione sia davvero nell'interesse oggettivo del minore, secondo i principi e i limiti stabiliti dalla «Carta di Treviso»)).

Art. 8

((Tutela della dignita' delle persone))

((1. Salva l'essenzialita' dell'informazione, il giornalista non fornisce notizie o pubblica immagini o fotografie di soggetti coinvolti in fatti di cronaca lesive della dignita' della persona, ne' si sofferma su dettagli di violenza, a meno che ravvisi la rilevanza sociale della notizia o dell'immagine.

2. Salvo rilevanti motivi di interesse pubblico o comprovati fini di giustizia e di polizia, il giornalista non riprende ne' produce immagini e foto di persone in stato di detenzione senza il consenso dell'interessato.

3. Le persone non possono essere presentate con ferri o manette ai polsi, salvo che cio' sia necessario per segnalare abusi)).

Art. 9

((Tutela del diritto alla non discriminazione))

((1. Nell'esercitare il diritto dovere di cronaca, il giornalista e' tenuto a rispettare il diritto della persona alla non discriminazione per razza, religione, opinioni politiche, sesso, condizioni personali, fisiche o mentali)).

Art. 10

((Tutela della dignita' delle persone malate))

((1. Il giornalista, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignita', il diritto alla riservatezza e al decoro personale, specie nei casi di malattie gravi o terminali, e si astiene dal pubblicare dati analitici di interesse strettamente clinico.

2. La pubblicazione e' ammessa nell'ambito del perseguimento dell'essenzialita' dell'informazione e sempre nel rispetto della dignita' della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica)).

Art. 11

((Tutela della sfera sessuale della persona))

((1. Il giornalista si astiene dalla descrizione di abitudini sessuali riferite ad una determinata persona, identificata o identificabile.

2. La pubblicazione e' ammessa nell'ambito del perseguimento dell'essenzialita' dell'informazione e nel rispetto della dignita' della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica)).

Art. 12

((Tutela del diritto di cronaca nei procedimenti penali))

((1. Al trattamento dei dati relativi a procedimenti penali non si applica il limite previsto dall'art. 10 del regolamento, nonche' dall'art. 2-octies del Codice.

2. Il trattamento di dati personali idonei a rivelare provvedimenti di cui all'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale (1) e' ammesso nell'esercizio del diritto di cronaca, secondo i principi di cui all'art. 5.

(1) L'art. 686 c.p.p. e' stato abrogato e sostituito dall'art. 3 del d.P.R. 14 novembre 2002, n. 313, al quale occorre fare riferimento ai fini dell'individuazione dei provvedimenti giudiziari cui la disposizione si riferisce)).

Art. 13

((Ambito di applicazione, sanzioni disciplinari))

((1. Le presenti norme si applicano ai giornalisti professionisti, pubblicisti e praticanti e a chiunque altro, anche occasionalmente, eserciti attivita' pubblicistica.

2. Le sanzioni disciplinari, di cui al titolo III della legge n. 69/1963, si applicano solo ai soggetti iscritti all'albo dei giornalisti, negli elenchi o nel registro)).

ALLEGATO A.2

REGOLE DEONTOLOGICHE PER IL TRATTAMENTO A FINI DI ARCHIVIAZIONE NEL PUBBLICO INTERESSE

O PER SCOPI DI RICERCA STORICA

CAPO I

PRINCIPI GENERALI

(Delibera del Garante n. 513 del 19 dicembre 2018, in G.U. 15 gennaio 2019, n. 12)

**((IL GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI**

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il [regolamento \(Ue\) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva 95/46/CE \(Regolamento generale sulla protezione dei dati\)](#), (di seguito «Regolamento» e «RGPD»);

Visto il [decreto legislativo 10 agosto 2018, n. 101](#), recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del [regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva 95/46/CE](#)»;

Visto il [Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n. 196](#) (di seguito «Codice»), così come modificato dal predetto [decreto legislativo n. 101 del 2018](#);

Visto il [decreto legislativo 22 gennaio 2004, n. 42](#), recante «[Codice dei beni culturali e del paesaggio](#)», ai sensi dell'[art. 10 della legge 6 luglio 2002, n. 137](#);

Visto il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, allegato A.2 al Codice;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore la dott.ssa Augusta Iannini;

Premesso:

L'[art. 20, commi 3 e 4, del decreto legislativo 101 del 2018](#) ha conferito al Garante il compito di verificare, nel termine di novanta giorni dalla sua entrata in vigore, la conformita' al regolamento delle disposizioni contenute nei codici di deontologia e buona condotta di cui agli allegati A.1, A.2, A.3, A.4 e A.6 al Codice.

Le disposizioni ritenute compatibili, ridenominate regole deontologiche, dovranno essere pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministero della giustizia, saranno successivamente riportate nell'allegato A al Codice.

Il Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici cessa di produrre effetti dalla pubblicazione delle predette regole nella Gazzetta Ufficiale ([art. 20, comma 3, del decreto legislativo 101 del 2018](#)).

Resta fermo che successivamente, il Garante potra' promuovere la revisione di tali regole, secondo la procedura di cui all'art. 2-quater del Codice, in base alla quale lo schema delle regole deontologiche, nell'osservanza del principio di rappresentativita', deve essere sottoposto a consultazione pubblica, per almeno sessanta giorni.

A regime, l'art. 102 del Codice, cosi' come novellato dall'[art. 8 dal decreto legislativo n. 101/2018](#), prevede specificamente che le regole deontologiche individuino garanzie adeguate per i diritti e le liberta' dell'interessato e si applicano ai soggetti pubblici e privati, ivi comprese le societa' scientifiche e le associazioni professionali, interessati al trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica.

Osserva:

Nell'ambito del presente provvedimento sono individuate le disposizioni del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, allegato A2 al Codice, adottato con provvedimento del Garante n. 8 del 14 marzo 2001, ritenute non conformi al regolamento e, in allegato sono riportate le disposizioni conformi, ridenominate regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica.

Le regole si applicano ai trattamenti di dati personali effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, fermo restando il rispetto dei principi e degli specifici adempimenti

richiesti dal regolamento e dal Codice.

Il rispetto delle disposizioni contenute nelle regole deontologiche costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali e il mancato rispetto delle stesse comporta l'applicazione della sanzione di cui all'art. 83, paragrafo 5 del regolamento (articoli 2-quater, comma 4, e 166, comma 2, del Codice).

L'osservanza di tali regole non deve, in ogni caso, pregiudicare l'indagine, la ricerca, la documentazione e lo studio ovunque svolti, in relazione a figure, fatti e circostanze del passato.

In via generale, si rappresenta che si è tenuto conto dell'esigenza di contemperare il diritto alla libertà di ricerca storica con altri diritti fondamentali dell'individuo, in ossequio al principio di proporzionalità (cons. 4 RGPD), verificando la conformità delle disposizioni del codice di deontologia, in particolare, ai considerando e agli articoli dedicati alla ricerca storica e all'archiviazione nel pubblico interesse (cons. 156, art. 5, comma 1, lettera b) ed e), art. 9, art. 10, e art. 89, par. 1 RGPD).

1. Modifiche generali

Preliminarmente, si osserva che si è reso necessario aggiornare i riferimenti normativi presenti nel codice di deontologia e la semantica utilizzata rispetto al rinnovato quadro normativo europeo e nazionale di riferimento.

Si è reso necessario, inoltre, eliminare il preambolo del codice di deontologia, dovendosi, in base al richiamato [art. 20 del decreto legislativo 101 del 2018](#), ridenominare solo le disposizioni dello stesso. Il preambolo, invece, nel sintetizzare le condizioni di liceità del trattamento, evidenziava, altresì, i presupposti della sottoscrizione del codice di deontologia avvenuta nel 2001, nel rispetto del principio di rappresentatività, che, comunque, rimane alla base delle presenti regole.

Cionondimeno, i principi e le fonti di diritto sovranazionale ivi richiamati, sono in ogni caso da ritenersi a fondamento dei trattamenti di dati personali effettuati nell'ambito degli archivi e della ricerca storica.

2. Disposizioni ritenute incompatibili

Si è ritenuto di riformulare il Titolo del Capo II in «Disposizioni generali per gli archivisti e liceità dei relativi trattamenti» e la rubrica dell'art. 3 in «Disposizioni generali», nonché il titolo del Capo III in «Disposizioni generali per gli utenti e condizioni per la liceità dei relativi trattamenti» e la rubrica dell'art. 9 in «Disposizioni generali», al fine di prevenire sovrapposizioni tra le presenti regole deontologiche con i futuri codici di condotta, che potranno essere adottati ai sensi degli articoli 40 e ss. RGPD.

Parimenti, è stata aggiornata la rubrica dell'art. 7 da «Aggiornamento dei dati» in «Esercizio dei diritti», tenuto conto che

L'art. 16 del Regolamento ricomprende il diritto di aggiornamento nel diritto di rettifica e integrazione di cui all'art. 16 RGPD.

All'art. 8, «Fonti orali», e' stata eliminata la disposizione che consentiva al titolare del trattamento di fornire un'«informativa semplificata» in caso di trattamento di fonti orali; cio', in quanto il regolamento non prevede alcuna forma di deroga o semplificazione agli obblighi informativi, quando i dati sono raccolti presso gli interessati (cfr. art. 13 RGPD).

Parimenti, e' stata rilevata la non conformita' al regolamento dell'art. 11, comma 5, del codice di deontologia che - nell'esonerare dall'obbligo di fornire l'informativa agli interessati nei casi di raccolta di dati personali presso soggetti terzi, quando cio' risulti impossibile o comporti uno sforzo sproporzionato - non prevedeva misure appropriate per tutelare i diritti, le liberta' e i legittimi interessi dell'interessato, come richiesto dall'art. 14, par. 5 lettera b), del regolamento.

Sono state, altresì, modificate le rubriche degli articoli 12 e 13, rispettivamente, come segue «Applicazione delle regole deontologiche» e «Violazione delle regole deontologiche».

3. Regole deontologiche

I predetti elementi, relativi all'aggiornamento della disciplina in materia, sono recepiti nelle «Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica» in ragione di quanto disposto dall'[art. 20, comma 4, del decreto legislativo n. 101/2018](#) e riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante. Tali «Regole deontologiche» sono volte a disciplinare i trattamenti in questione in attesa di un auspicabile aggiornamento delle stesse ai sensi degli articoli 2-quater e 101 e ss. del Codice. Pertanto, si dispone la trasmissione delle suddette «Regole deontologiche» all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la relativa pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'Allegato A) al Codice.

Tutto cio' premesso il Garante:

Ai sensi dell'[art. 20, comma 4, del decreto legislativo n. 101/2018](#), verificata la conformita' al regolamento delle disposizioni del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici, allegato A.2 al Codice, dispone che le medesime, riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante, siano pubblicate come «Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica» e ne dispone, altresì, la trasmissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per

essere riportato nell'allegato A) al Codice.

Roma, 19 dicembre 2018

**Il presidente
Soro**

**Il relatore
Iannini**

**Il segretario generale
Busia**

Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica))

Art. 1.

((Finalita' e ambito di applicazione))

((1. Le presenti regole sono volte a garantire che l'utilizzazione di dati di carattere personale acquisiti nell'esercizio della libera ricerca storica e del diritto allo studio e all'informazione, nonché nell'accesso ad atti e documenti, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

2. Le presenti regole riguardano i trattamenti di dati personali effettuati per scopi storici in relazione ai documenti conservati presso archivi delle pubbliche amministrazioni, enti pubblici ed archivi privati dichiarati di notevole interesse storico. Le regole deontologiche si applicano, senza necessità di sottoscrizione, all'insieme dei trattamenti di dati personali comunque effettuati dagli utenti per scopi storici.

3. Il presenti regole recano, altresì, principi-guida di comportamento dei soggetti che trattano per scopi storici dati personali conservati presso archivi pubblici e archivi privati dichiarati di notevole interesse storico, e in particolare:

a) nei riguardi degli archivisti, individua regole di correttezza e di non discriminazione nei confronti degli utenti, indipendentemente dalla loro nazionalità, categoria di appartenenza, livello di istruzione;

b) nei confronti degli utenti, individua cautele per la raccolta, l'utilizzazione e la diffusione dei dati contenuti nei documenti.

4. La competente sovrintendenza archivistica riceve comunicazione da parte di proprietari, possessori e detentori di archivi privati non dichiarati di notevole interesse storico o di singoli documenti

di interesse storico, i quali manifestano l'intenzione di applicare le presenti regole nella misura per essi compatibile)).

Art. 2

((Definizioni))

((1. Nell'applicazione delle presenti regole deontologiche si tiene conto delle definizioni e delle indicazioni contenute nella disciplina in materia di trattamento dei dati personali. Ai medesimi fini si intende, altresì':

a) per «archivista», chiunque, persona fisica o giuridica, ente o associazione, abbia responsabilita' di controllare, acquisire, trattare, conservare, restaurare e gestire archivi storici, correnti o di deposito della pubblica amministrazione, archivi privati dichiarati di notevole interesse storico, nonché' gli archivi privati di cui al precedente art. 1, comma 4;

b) per «utente», chiunque chieda di accedere o acceda per scopi storici a documenti contenenti dati personali, anche per finalita' giornalistiche o di pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero;

c) per «documento», qualunque testimonianza scritta, orale o conservata su qualsiasi supporto che contenga dati personali)).

CAPO II

((DISPOSIZIONI GENERALI PER GLI ARCHIVISTI E LICEITA' DEI RELATIVI TRATTAMENTI))

Art. 3

((Disposizioni generali))

((1. Nel trattare i dati di carattere personale e i documenti che li contengono, gli archivisti adottano, in armonia con la legge e i regolamenti, le modalita' piu' opportune per favorire il rispetto dei diritti, delle liberta' fondamentali e della dignita' delle persone alle quali si riferiscono i dati trattati.

2. Gli archivisti di enti o istituzioni pubbliche si adoperano

per il pieno rispetto, anche da parte dei terzi con cui entrano in contatto per ragioni del proprio ufficio o servizio, delle disposizioni di legge e di regolamento in materia archivistica e, in particolare, di quanto previsto nel Capo III "Consultabilita' dei documenti degli archivi e tutela della riservatezza", artt. da 122-127 del [decreto legislativo n. 42 del 2004](#) e agli artt. da 101-103 del Codice.

3. I soggetti che operano presso enti pubblici svolgendo funzioni archivistiche, nel trattare dati di carattere personale si attengono ai doveri di lealta', correttezza, imparzialita', onesta' e diligenza propri dell'esercizio della professione e della qualifica o livello ricoperti. Essi conformano il proprio operato al principio di trasparenza della attivita' amministrativa.

4. I dati personali trattati per scopi storici possono essere ulteriormente utilizzati per tali scopi, e sono soggetti in linea di principio alla medesima disciplina indipendentemente dal documento in cui sono contenuti e dal luogo di conservazione, ferme restando le cautele e le garanzie previste per particolari categorie di dati o di trattamenti)).

Art. 4

((Conservazione e tutela))

((1. Gli archivisti si impegnano a:

a) favorire il recupero, l'acquisizione e la tutela dei documenti. A tal fine, operano in conformita' con i principi, i criteri metodologici e le pratiche della professione generalmente condivisi ed accettati, curando anche l'aggiornamento sistematico e continuo delle proprie conoscenze storiche, amministrative e tecnologiche;

b) tutelare l'integrita' degli archivi e l'autenticita' dei documenti, anche elettronici e multimediali, di cui promuovono la conservazione permanente, in particolare di quelli esposti a rischi di cancellazione, dispersione ed alterazione dei dati;

c) salvaguardare la conformita' delle riproduzioni dei documenti agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati;

d) sviluppare misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti e adottare, in presenza di specifici rischi, particolari cautele quali la consultazione in copia di alcuni documenti e la conservazione degli originali in cassaforte o armadi blindati)).

Art. 5

((Comunicazione e fruizione))

((1. Gli archivi sono organizzati secondo criteri tali da assicurare il principio della libera fruibilita' delle fonti.

2. L'archivista promuove il piu' largo accesso agli archivi e, attenendosi al quadro della normativa vigente, favorisce l'attivita' di ricerca e di informazione nonche' il reperimento delle fonti.

3. L'archivista informa il ricercatore sui documenti estratti temporaneamente da un fascicolo perche' esclusi dalla consultazione.

4. In caso di rilevazione sistematica dei dati realizzata da un archivio in collaborazione con altri soggetti pubblici o privati, per costituire banche dati di intere serie archivistiche, la struttura interessata sottoscrive una apposita convenzione per concordare le modalita' di fruizione e le forme di tutela dei soggetti interessati, attenendosi alle disposizioni della legge, in particolare per quanto riguarda il rapporto tra il titolare, il responsabile del trattamento e le persone autorizzate al trattamento)).

Art. 6

((Impegno di riservatezza))

((1. Gli archivisti si impegnano a:

a) non fare alcun uso delle informazioni non disponibili agli utenti o non rese pubbliche, ottenute in ragione della propria attivita' anche in via confidenziale, per proprie ricerche o per realizzare profitti e interessi privati. Nel caso in cui l'archivista svolga ricerche per fini personali o comunque estranei alla propria attivita' professionale, e' soggetto alle stesse regole e ai medesimi limiti previsti per gli utenti;

b) mantenere riservate le notizie e le informazioni concernenti i dati personali apprese nell'esercizio delle proprie attivita'.

2. L'archivista osserva tali doveri di riserbo anche dopo la cessazione dalla propria attivita')).

Art. 7

((Esercizio dei diritti))

((1. L'archivista favorisce l'esercizio del diritto degli interessati alla rettifica o all'integrazione dei dati, garantendone la conservazione secondo modalita' che assicurino la distinzione delle fonti originarie dalla documentazione successivamente acquisita.

2. Ai fini dell'applicazione dell'art. 15 RGPD, in presenza di eventuali richieste generalizzate di accesso ad un'ampia serie di dati o documenti, l'archivista pone a disposizione gli strumenti di ricerca e le fonti pertinenti fornendo al richiedente idonee indicazioni per una loro agevole consultazione.

3. In caso di esercizio di un diritto, concernente persone

decedute ai sensi dell'art. 2-terdecies del Codice, da parte di chi vi abbia interesse proprio o agisce a tutela dell'interessato, in relazione a dati personali che riguardano persone decedute e documenti assai risalenti nel tempo, la sussistenza dell'interesse e' valutata anche in riferimento al tempo trascorso)).

Art. 8

((Fonti orali))

((1. In caso di trattamento di fonti orali, e' necessario che gli intervistati abbiano espresso il proprio consenso in modo esplicito, eventualmente in forma verbale.

2. Gli archivi che acquisiscono fonti orali richiedono all'autore dell'intervista una dichiarazione scritta dell'avvenuta comunicazione degli scopi perseguiti nell'intervista stessa e del relativo consenso manifestato dagli intervistati)).

CAPO III

((DISPOSIZIONI GENERALI PER GLI UTENTI E CONDIZIONI PER LA LICEITA' DEI RELATIVI TRATTAMENTI))

Art. 9

((Disposizioni generali))

((1. Nell'accedere alle fonti e nell'esercitare l'attivita' di studio, ricerca e manifestazione del pensiero, gli utenti, quando trattino i dati di carattere personale, secondo quanto previsto dalla legge e dai regolamenti, adottano le modalita' piu' opportune per favorire il rispetto dei diritti, delle liberta' fondamentali e della dignita' delle persone interessate.

2. In applicazione del principio di cui al comma 1, gli utenti utilizzano i documenti sotto la propria responsabilita' e conformandosi agli scopi perseguiti e delineati nel progetto di ricerca, nel rispetto dei principi di pertinenza ed indispensabilita'

di cui all'art. 101, comma 2, del Codice)).

Art. 10

((Accesso agli archivi pubblici))

((1. L'accesso agli archivi pubblici e' libero. Tutti gli utenti hanno diritto ad accedere agli archivi con eguali diritti e doveri.

2. Fanno eccezione, ai sensi delle leggi vigenti, i documenti di carattere riservato relativi alla politica interna ed estera dello Stato che divengono consultabili cinquanta anni dopo la loro data e quelli contenenti i dati di cui agli artt. 9, par. 1, e 10 RGD, che divengono liberamente consultabili quaranta anni dopo la loro data. Il termine e' di settanta anni se i dati sono relativi alla salute ovvero alla vita o all'orientamento sessuale oppure rapporti riservati di tipo familiare.

3. L'autorizzazione alla consultazione dei documenti di cui al comma 2 puo' essere rilasciata prima della scadenza dei termini dal Ministro dell'interno, previo parere del direttore dell'Archivio di Stato o del sovrintendente archivistico competenti e udita la Commissione per le questioni inerenti alla consultabilita' degli atti di archivio riservati istituita presso il Ministero dell'interno, secondo quanto previsto all'[art. 123 del decreto legislativo n. 42 del 2004](#).

4. In caso di richiesta di autorizzazione a consultare i documenti di cui al comma 2 prima della scadenza dei termini, l'utente presenta all'ente che li conserva un progetto di ricerca che, in relazione alle fonti riservate per le quali chiede l'autorizzazione, illustri le finalita' della ricerca e le modalita' di diffusione dei dati. Il richiedente ha facolta' di presentare ogni altra documentazione utile.

5. L'autorizzazione di cui al comma 3 alla consultazione e' rilasciata a parita' di condizioni ad ogni altro richiedente. La valutazione della parita' di condizioni avviene sulla base del progetto di ricerca di cui al comma 4.

6. L'autorizzazione alla consultazione dei documenti, di cui al comma 3, prima dello scadere dei termini, puo' contenere cautele volte a consentire la comunicazione dei dati senza ledere i diritti, le liberta' e la dignita' delle persone interessate.

7. Le cautele possono consistere anche, a seconda degli obiettivi della ricerca desumibili dal progetto, nell'obbligo di non diffondere i nomi delle persone, nell'uso delle sole iniziali dei nominativi degli interessati, nell'oscuramento dei nomi in una banca dati, nella sottrazione temporanea di singoli documenti dai fascicoli o nel divieto di riproduzione dei documenti. Particolare attenzione e' prestata al principio della pertinenza e all'indicazione di fatti o circostanze che possono rendere facilmente individuabili gli interessati.

8. L'autorizzazione di cui al comma 3 e' personale e il titolare dell'autorizzazione non puo' delegare altri al conseguente trattamento dei dati. I documenti mantengono il loro carattere riservato e non possono essere ulteriormente utilizzati da altri soggetti senza la relativa autorizzazione)).

Art. 11

((Diffusione))

((1. L'interpretazione dell'utente, nel rispetto del diritto alla riservatezza, del diritto all'identita' personale e della dignita' degli interessati, rientra nella sfera della liberta' di parola e di manifestazione del pensiero costituzionalmente garantite.

2. Nel far riferimento allo stato di salute delle persone l'utente si astiene dal pubblicare dati analitici di interesse strettamente clinico e dal descrivere abitudini sessuali riferite ad una determinata persona identificata o identificabile.

3. La sfera privata delle persone note o che abbiano esercitato funzioni pubbliche deve essere rispettata nel caso in cui le notizie o i dati non abbiano alcun rilievo sul loro ruolo o sulla loro vita pubblica.

4. Al momento della diffusione dei dati il principio della pertinenza e' valutato dall'utente con particolare riguardo ai singoli dati personali contenuti nei documenti, anziche' ai documenti nel loro complesso. L'utente puo' diffondere i dati personali se pertinenti e indispensabili alla ricerca e se gli stessi non ledono la dignita' e la riservatezza delle persone.

5. L'utente puo' utilizzare i dati elaborati o le copie dei documenti contenenti dati personali, accessibili su autorizzazione, solo ai fini della propria ricerca, e ne cura la riservatezza anche rispetto ai terzi)).

Art. 12

((Applicazione delle regole deontologiche))

((1. I soggetti pubblici e privati, comprese le societa' scientifiche e le associazioni professionali, che siano tenuti ad applicare le presenti regole deontologiche, si impegnano, con i modi e nelle forme previste dai propri ordinamenti, a promuoverne la massima diffusione e la conoscenza, nonche' ad assicurarne il rispetto.

2. Nel caso degli archivi degli enti pubblici e degli archivi privati dichiarati di notevole interesse storico, le sovrintendenze archivistiche promuovono la diffusione e l'applicazione delle regole deontologiche)).

Art. 13

((Violazione delle regole deontologiche))

((1. Nell'ambito degli archivi pubblici le amministrazioni competenti applicano le sanzioni previste dai rispettivi ordinamenti.

2. Le società e le associazioni tenute ad applicare le presenti regole adottano, sulla base dei propri ordinamenti e regolamenti, le opportune misure in caso di violazione del codice stesso, ferme restando le sanzioni di legge.

3. La violazione delle prescrizioni delle presenti regole deontologiche da parte degli utenti e' comunicata agli organi competenti per il rilascio delle autorizzazioni a consultare documenti riservati prima del decorso dei termini di legge, ed e' considerata ai fini del rilascio dell'autorizzazione medesima. L'amministrazione competente, secondo il proprio ordinamento, puo' altresì escludere temporaneamente dalle sale di studio i soggetti responsabili della violazione delle regole delle presenti regole deontologiche. Gli stessi possono essere esclusi da ulteriori autorizzazioni alla consultazione di documenti riservati.

4. Oltre a quanto previsto dalla legge per la denuncia di reato cui sono tenuti i pubblici ufficiali, i soggetti di cui ai commi 1 e 2 possono segnalare al Garante le violazioni delle regole di condotta per l'eventuale adozione dei provvedimenti e delle sanzioni di competenza)).

Art. 14

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 26/3/2019, N. 72)))

ALLEGATO A.3

REGOLE DEONTOLOGICHE PER TRATTAMENTI A FINI STATISTICI O DI RICERCA SCIENTIFICA

EFFETTUATI NELL'AMBITO DEL SISTEMA STATISTICO NAZIONALE

CAPO I

AMBITO DI APPLICAZIONE E PRINCIPI GENERALI

(Delibera del Garante n. 514 del 19 dicembre 2018, in G.U. 14 gennaio 2019, n. 11)

**((IL GARANTE
PER LA PROTEZIONE DEI DATI PERSONALI**

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il [regolamento \(UE\) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva n. 95/46/CE \(regolamento generale sulla protezione dei dati\)](#) (di seguito «regolamento» e «RGPD»);

Visto il [decreto legislativo 10 agosto 2018, n. 101](#), recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del [regolamento \(UE\) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva n. 95/46/CE](#);

Visto il [Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n. 196](#) (di seguito Codice), così come modificato dal predetto [decreto legislativo n. 101 del 2018](#);

Visto il [decreto legislativo 6 settembre 1989, n. 322](#), recante norme sul Sistema statistico nazionale e sulla riorganizzazione dell'Istituto nazionale di statistica, ai sensi dell'[art. 24 della legge 23 agosto 1988, n. 400](#);

Visto l'[art. 5-ter del decreto legislativo 14 marzo 2013, n. 33](#), recante Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, relativo all'accesso per fini scientifici ai dati elementari raccolti per finalità statistiche;

Visto il Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, allegato A.3 al codice;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del garante n. 1/2000;

Relatore la prof.ssa Licia Califano;

Premesso

L'[art. 20, commi 3 e 4, del decreto legislativo 101 del 2018](#) ha conferito al garante il compito di verificare, nel termine di novanta

giorni dalla sua entrata in vigore, la conformita' al regolamento delle disposizioni contenute nei codici di deontologia e buona condotta di cui agli allegati A.1, A.2, A.3, A.4 e A.6 al Codice.

Le disposizioni ritenute compatibili, ridenominate regole deontologiche, dovranno essere pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministero della giustizia, saranno successivamente riportate nell'allegato A al codice.

Il Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifici effettuati nell'ambito del Sistema statistico nazionale cessa di produrre effetti dalla pubblicazione delle predette regole nella Gazzetta Ufficiale ([art. 20, comma 3, del decreto legislativo 101 del 2018](#)).

Successivamente, il garante potra' promuovere la revisione di tali regole, secondo la procedura di cui all'art. 2-quater del Codice, in base alla quale lo schema delle regole deontologiche, nell'osservanza del principio di rappresentativita', deve essere sottoposto a consultazione pubblica, per almeno sessanta giorni.

A regime, l'art. 106 del Codice, cosi' come novellato dall'[art. 8 dal decreto legislativo n. 101/2018](#), prevede specificamente che le regole deontologiche individuino garanzie adeguate per i diritti e le liberta' dell'interessato e si applicano ai soggetti pubblici e privati, ivi comprese le societa' scientifiche e le associazioni professionali, interessati al trattamento dei dati per fini statistici o di ricerca scientifica ricompresi nell'ambito del Sistema statistico nazionale.

Osserva

Nell'ambito del presente provvedimento sono individuate le disposizioni del Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, allegato A.3 al Codice, adottato con provvedimento del garante n. 13 del 31 luglio 2002, ritenute non conformi al regolamento e, in allegato, sono riportate le disposizioni conformi, ridenominate regole deontologiche per i trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale.

I soggetti tenuti all'applicazione delle allegate regole osservano, altresì, il principio di imparzialita' e di non discriminazione nei confronti di altri utilizzatori, in particolare nell'ambito della comunicazione per scopi statistici di dati depositati in archivi pubblici e trattati da enti pubblici o sulla base di finanziamenti pubblici. Cio', fermo restando il rispetto dei principi, delle garanzie e degli specifici adempimenti richiesti dal regolamento e dal Codice.

L'osservanza delle disposizioni contenute nelle regole deontologiche costituisce condizione essenziale per la liceita' e

correttezza del trattamento dei dati personali e il mancato rispetto delle stesse comporta l'applicazione della sanzione di cui all'art. 83, paragrafo 5, del regolamento (artt. 2-quater, comma 4, e 166, comma 2, del codice).

In via generale, si rappresenta che si e' tenuto conto dell'esigenza di contemperare il diritto alla liberta' di ricerca scientifica e statistica nell'ambito del Sistema statistico nazionale, in ossequio al principio di proporzionalita' (cons. 4 del regolamento), verificando la conformita' delle disposizioni del Codice di deontologia, in particolare, ai principali considerando e agli articoli dedicati alla ricerca statistica e scientifica (cons. 26, 50, 52, 53, 62, 156, 157, 159, 162, 163, art. 5, comma 1 lett. b) ed e), art. 9, art. 10, e art. 89 § 1, del regolamento).

L'attivita' istruttoria in ordine alla verifica della conformita' al regolamento delle disposizioni del Codice di deontologia allegato A,3 al Codice ha reso, talvolta, necessari degli interventi di revisione e aggiornamento volti, da un lato, ad assicurare una maggiore aderenza della norma al regolamento e al Codice e, dall'altro, a preservare regole che gli operatori del settore hanno, a suo tempo, condiviso e sulle quali fondano i trattamenti di dati personali inerenti alle proprie attivita'.

1. Modifiche generali

Preliminarmente, si osserva che si e' reso necessario aggiornare i riferimenti normativi presenti nel Codice di deontologia e la semantica utilizzata rispetto al rinnovato quadro normativo europeo e nazionale di riferimento.

Si e' reso necessario, inoltre, eliminare il preambolo del Codice di deontologia, dovendosi, in base al richiamato [art. 20 del decreto legislativo 101 del 2018](#), ridenominare solo le disposizioni dello stesso.

Cionondimeno, i principi e le fonti di diritto sovranazionale ivi richiamati, sono in ogni caso da ritenersi a fondamento dei trattamenti di dati personali effettuati per scopi statistici o di ricerca scientifica nell'ambito del Sistema statistico nazionale.

2. Disposizioni ritenute incompatibili

Art. 3, «Identificabilita' dell'interessato», e' stato ritenuto necessario, in primo luogo, sostituire la parola «identificativi» con la seguente locuzione «che ... identificano» l'unita' statistica, al comma 1, lett. a), in quanto la definizione di «dati identificativi» di cui all'art. 4, comma 1, lett. c), del Codice e' stata abrogata dal [decreto legislativo n. 101 del 2018](#), e non e' piu' prevista dal regolamento; in secondo luogo, il comma 1, lett. c), e' stato ritenuto incompatibile nella misura in cui introduceva, per la valutazione del rischio di identificabilita' degli interessati, dei

parametri predefiniti che non sono in linea con il quadro giuridico introdotto dal regolamento. Rispetto alle indicazioni fornite dal considerando 26, che per l'identificabilità di una persona indica, in particolare, che si tengano in considerazione «tutti i mezzi» di cui il titolare può ragionevolmente avvalersi, la disposizione in esame poneva come parametri predefiniti la tipologia di dati comunicati o diffusi, la proporzione tra i mezzi per l'identificazione e la lesione o il pericolo di lesione dei diritti degli interessati, cioè anche alla luce del vantaggio che ne poteva trarre il titolare. Tale disposizione, quindi, nel fornire ai titolari delle coordinate per valutare l'identificabilità dell'interessato attualmente superate, manifestava anche un approccio alla definizione e valutazione del rischio più circoscritte rispetto a quella del regolamento in cui tale valutazione deve tener conto delle nuove tecnologie utilizzate, della natura, dell'oggetto, del contesto e delle finalità di ogni tipo di trattamento (cfr. anche cons., 84, 89, 93 e 95 e artt. 5, § 1, lett. e), 24, 35 e 36 del regolamento).

L'art. 4, «Criteri per la valutazione del rischio di identificazione», è stato mantenuto considerandosi, in via generale, compatibile con il regolamento, nella misura in cui si limita a fornire alcuni parametri, orientativi, non esaustivi, per la valutazione del rischio di identificazione degli interessati. Al fine di assicurarne un'applicazione conforme al regolamento, si è, tuttavia, ritenuto necessario modificarlo con l'aggiunta di un «anche» (al primo comma, tra le parole «tiene conto» e «dei seguenti»), affinché sia chiaro che i parametri ivi indicati devono, comunque, considerarsi meramente esemplificativi e soprattutto non alternativi rispetto al nuovo quadro giuridico introdotto dal regolamento sopra descritto.

Parimenti, è risultato compatibile con il regolamento -salvi i necessari aggiornamenti ai riferimenti normativi- l'art. 4-bis, «Trattamento di dati personali, sensibili e giudiziari, nell'ambito del programma statistico nazionale» in base a quale, «nel Programma statistico nazionale sono illustrate le finalità perseguite e le garanzie previste dal [decreto legislativo 6 settembre 1989, n. 322](#) e dal [decreto legislativo 30 giugno 2003, n. 196](#) e successive modificazioni e integrazioni e dalle presenti regole deontologiche. Il Programma indica, altresì, i dati di cui agli artt. 9, § 1, e 10 del regolamento, le rilevazioni per le quali i dati sono trattati e le modalità di trattamento. Il Programma è adottato, con riferimento ai dati personali, sensibili e giudiziari, sentito il garante per la protezione dei dati personali, ai sensi dell'art. 58, § 3 lett. b) del regolamento».

Giova, infatti, evidenziare che tale norma è stata introdotta nel Codice di deontologia di cui trattasi con provvedimento del garante 170 del 24 luglio 2014, su sollecitazione dell'Istat, a seguito dell'abrogazione dell'[art. 6-bis, comma 2, del decreto legislativo n.](#)

322 del 1989 (cfr. art. 8-bis, decreto-legge 31 agosto 2013, n. 101, convertito con modificazioni in legge 30 ottobre 2013, n. 125), che aveva un contenuto sostanzialmente analogo.

Resta fermo che tale disposizione non e', in ogni caso, da sola, sufficiente a legittimare il trattamento, nell'ambito del Piano statistico nazionale, delle particolari categorie di dati e dei dati relativi a condanne penali e reati. La base giuridica e le condizioni di liceita' per il trattamento di tali dati, nell'ambito del Piano statistico nazionale, e', infatti, costituita anche, per le categorie particolari di dati, dall'art. 9 del regolamento e dagli articoli 2-sexies e 107 del codice, e, per i dati relativi a condanne penali e reati, dall'art. 10 del regolamento e dagli articoli 2-sexies e 2-octies del Codice.

L'art. 5, comma 2, lett. c), e' stato considerato incompatibile nella parte in cui, tra i presupposti del trattamento delle particolari categorie di dati da parte di soggetti privati che partecipano al Sistema statistico nazionale, prevedeva la preventiva autorizzazione del garante. Cio', in quanto, nel nuovo quadro normativo, risulta molto circoscritto l'ambito di applicazione dell'istituto dell'autorizzazione del garante (cfr. art. 36, § 5, del regolamento, art. 110-bis del Codice e art. 21 del decreto legislativo n. 101 del 2018).

Sono stati modificati il titolo del capo II da «informativa, comunicazione e diffusione» in «informazioni agli interessati, comunicazione e diffusione» e la rubrica dell'art. 6 da «Informativa» a «Informazioni agli interessati», ai sensi degli artt. 13 e 14 del regolamento.

L'art. 6 disciplina le ipotesi di impossibilita' di fornire le informazioni direttamente agli interessati quando i dati sono raccolti presso terzi. Tale articolo e' stato considerato incompatibile nella parte in cui, al comma 2, disponeva che il titolare dovesse preventivamente comunicare al garante le modalita' individuate per dare pubblicita' all'informativa, il quale avrebbe potuto prescrivere eventuali misure e accorgimenti. Cio', in quanto, in conformita' all'art. 14 del regolamento, il coinvolgimento del garante non e' piu' richiesto.

La disposizione e' risultata, inoltre, incompatibile con il regolamento nella parte in cui consentiva al titolare di fornire agli interessati un'informativa differita per la parte riguardante le specifiche finalita' e modalita' del trattamento, qualora cio' risultasse necessario per il raggiungimento dell'obiettivo dell'indagine (art. 6, comma 3). L'art. 13 del regolamento, infatti, non prevede alcuna forma di deroga o semplificazione agli obblighi informativi quando i dati sono raccolti presso gli interessati.

E' stato, altresì, considerato incompatibile il comma 4 dell'articolo in esame, in quanto, nel prevedere la possibilita' che il titolare possa raccogliere dati personali presso un soggetto rispondente in nome e per conto di un altro (cd. proxy), non

prevedeva le specifiche circostanze in cui tale modalita' di raccolta era ammessa (art. 105, comma 3, del codice).

L'art. 7, commi 2, 3 e 4, relativo alla comunicazione di dati personali a ricercatori di universita' o a istituti o enti di ricerca a soci di societa' scientifiche, non facenti parte del Sistema statistico nazionale, e l'art. 8, sulla comunicazione dei dati tra soggetti del Sistema statistico nazionale, sono stati considerati non conformi al rinnovato quadro normativo in quanto, ai sensi degli artt. 6, § 3, del regolamento e 2-ter del codice, si richiede una norma di legge o, nei casi previsti dalla legge, di regolamento per la comunicazione di dati tra soggetti pubblici o tra soggetti che svolgono compiti di interesse pubblico, quali sono i soggetti del Sistema statistico nazionale. Cio', tenuto anche conto delle condizioni individuate nello specifico quadro normativo di settore in materia accesso per fini scientifici ai dati elementari raccolti per finalita' statistiche, di cui all'[art. 5-ter del decreto legislativo n. 33 del 2013](#), che, di recente, ha trovato piena applicazione con l'approvazione da parte del Comstat delle linee guida per l'accesso a fini scientifici ai dati elementari del Sistema statistico nazionale ([Gazzetta Ufficiale n. 287 dell'11 dicembre 2018](#)).

E' stato modificato il titolo del capo III da «sicurezza e regole di condotta» in «disposizioni finali».

All'art. 11, «Conservazione dei dati», e' stato ritenuto necessario abrogare al comma 1, dalle parole «in tali casi» alle parole «finalita' perseguite», in quanto tali previsioni individuano predefiniti e specifici casi di deroga al principio di limitazione della conservazione di cui all'art. 5, § 1, lett. e), del regolamento che, pur ammettendo deroghe per i trattamenti effettuati a fini statistici e di ricerca scientifica, richiede, oltre a una valutazione del rischio, caso per caso, a cura del titolare (artt. 24 e 35 del regolamento), l'individuazione di misure tecniche e organizzative adeguate a tutela dell'interessato. Cio' vale anche per il comma 2, poiche' anche le garanzie previste dall'[art. 6-bis, comma 6, del decreto legislativo 6 settembre 1989, n. 322](#), devono essere applicate alla luce delle predette considerazioni.

L'art. 12, «Misure di sicurezza», e' stato ritenuto incompatibile, in quanto gli aspetti ivi disciplinati sono oggetto ora di specifiche previsioni del regolamento che, nel rispetto del principio di responsabilizzazione, richiede anche un diverso approccio alle misure di sicurezza che devono esser individuate, fin dalla progettazione e per impostazione predefinita (artt. 24 e 25 del regolamento), in conformita' all'art. 32 del regolamento. L'articolo, inoltre, forniva specifiche indicazioni per l'individuazione dei diversi livelli di accesso (natura dei dati e funzioni dei soggetti coinvolti) ai dati da parte dei soggetti legittimati che attualmente devono essere definiti alla luce dei, piu' ampi, criteri di cui all'art. 25, par. 2, del regolamento, in omaggio ai richiamati principi di privacy by default e by design.

L'art. 13, «Esercizio dei diritti», comma 1, e' stato considerato incompatibile, in quanto, consentirebbe al titolare la possibilita' di limitare il diritto di rettifica o integrazione senza individuare garanzie adeguate, come richiesto, invece, dall'art. 89 del regolamento.

E' stata, infine, riformulata, la rubrica dell'art. 14, in «Disposizioni finali», onde evitare ambiguita' rispetto alle regole deontologiche di cui all'art. 2-quater del codice e con i futuri codici di condotta, di cui all'art. 40 del regolamento.

3. Regole deontologiche

I predetti elementi, relativi all'aggiornamento della disciplina in materia, sono recepiti nelle «Regole deontologiche per il trattamento a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale» in ragione di quanto disposto dall'[art. 20, comma 4, del decreto legislativo n. 101/2018](#) e riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante.

Tali «Regole deontologiche» sono volte a disciplinare i trattamenti in questione in attesa di un auspicabile aggiornamento delle stesse ai sensi degli artt. 2-quater e 106 e seguenti del Codice. Pertanto, si dispone la trasmissione delle suddette «Regole deontologiche» all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la relativa pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'allegato A) al Codice.

Tutto cio' premesso il Garante

Ai sensi dell'[art. 20, comma 4, del decreto legislativo n. 101/2018](#), verificata la conformita' al regolamento delle disposizioni del Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, allegato A.3 al Codice, dispone che le medesime, riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante, siano pubblicate come «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale» e ne dispone, altresì, la trasmissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'allegato A) al Codice.

Roma, 19 dicembre 2018

Il presidente:

Soro

**Il relatore:
Califano**

**Il segretario generale:
Busia**

REGOLE DEONTOLOGICHE PER TRATTAMENTI A FINI STATISTICI O DI RICERCA SCIENTIFICA EFFETTUATI NELL'AMBITO DEL SISTEMA STATISTICO NAZIONALE.))

Art. 1.

((Ambito di applicazione))

((1. Le regole deontologiche si applicano ai trattamenti di dati personali per scopi statistici effettuati da:

a) enti ed uffici di statistica che fanno parte o partecipano al Sistema statistico nazionale, per l'attuazione del programma statistico nazionale o per la produzione di informazione statistica, in conformita' ai rispettivi ambiti istituzionali;

b) strutture diverse dagli uffici di cui alla lettera a), ma appartenenti alla medesima amministrazione o ente, qualora i relativi trattamenti siano previsti dal programma statistico nazionale e gli uffici di statistica attestino le metodologie adottate, osservando le disposizioni contenute nel [decreto legislativo 6 settembre 1989, n. 322](#), nel regolamento, nel Codice e successive modificazioni e integrazioni, nonche' nelle presenti regole deontologiche)).

Art. 2

((Definizioni))

((1. Ai fini delle presenti regole deontologiche si applicano le definizioni elencate nell'art. 4 del regolamento. Ai fini medesimi, si intende inoltre per:

a) «trattamento per scopi statistici», qualsiasi trattamento effettuato per finalita' di indagine statistica o di produzione, conservazione e diffusione di risultati statistici in attuazione del programma statistico nazionale o per effettuare informazione statistica in conformita' agli ambiti istituzionali dei soggetti di cui all'art. 1;

b) «risultato statistico», l'informazione ottenuta con il trattamento di dati personali per quantificare aspetti di un fenomeno collettivo;

c) «variabile pubblica», il carattere o la combinazione di caratteri, di tipo qualitativo o quantitativo, oggetto di una rilevazione statistica che faccia riferimento ad informazioni presenti in pubblici registri, elenchi, atti, documenti o fonti conoscibili da chiunque;

d) «unita' statistica», l'entita' alla quale sono riferiti o riferibili i dati trattati)).

Art. 3

((Identificabilita' dell'interessato))

((1. Agli effetti dell'applicazione delle presenti regole:

a) un interessato si ritiene identificabile quando, con l'impiego di mezzi ragionevoli, e' possibile stabilire un'associazione significativamente probabile tra la combinazione delle modalita' delle variabili relative ad una unita' statistica e i dati che la identificano;

b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie: risorse economiche; risorse di tempo; archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione; archivi, anche non nominativi, che forniscano ulteriori informazioni oltre a quelle oggetto di comunicazione o diffusione; risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilita' di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati; conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati)).

Art. 4

((Criteri per la valutazione del rischio di identificazione))

((1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto anche dei seguenti criteri:

a) si considerano dati aggregati le combinazioni di modalita' alle quali e' associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensita' data dalla sintesi dei valori assunti da un numero di unita' statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia e' pari a tre;

b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;

c) i risultati statistici relativi a sole variabili pubbliche

non sono soggetti alla regola della soglia;

d) la regola della soglia puo' non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unita' statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;

e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;

f) si presume che sia adeguatamente tutelata la riservatezza nel caso in cui tutte le unita' statistiche di una popolazione presentino la medesima modalita' di una variabile.

2. Nel programma statistico nazionale sono individuate le variabili che possono essere diffuse in forma disaggregata, ove cio' risulti necessario per soddisfare particolari esigenze conoscitive anche di carattere internazionale o comunitario.

3. Nella comunicazione di collezioni campionarie di dati, il rischio di identificazione deve essere per quanto possibile contenuto. Tale limite e la metodologia per la stima del rischio di identificazione sono individuati dall'Istat che, attenendosi ai criteri di cui all'art. 3 definisce anche le modalita' di rilascio dei dati dandone comunicazione alla Commissione per la garanzia dell'informazione statistica)).

Art. 4-bis

((Trattamento di particolari categorie di dati e di dati relativi a condanne penali e reati, nell'ambito del Programma statistico nazionale))

((Nel Programma statistico nazionale sono illustrate le finalita' perseguite e le garanzie previste dal [decreto legislativo 6 settembre 1989, n. 322](#) e dal [decreto legislativo 30 giugno 2003, n. 196](#) e successive modificazioni e integrazioni e dalle presenti regole deontologiche. Il Programma indica altresì i dati di cui agli artt. 9, par. 1, e 10 del regolamento, le rilevazioni per le quali i dati sono trattati e le modalita' di trattamento. Il Programma e' adottato, con riferimento ai dati personali, di cui agli art. 9 e 10 del regolamento, sentito il garante per la protezione dei dati personali, ai sensi dell'art. 58, par. 3, lett. b) regolamento)).

Art. 5

((Trattamento di particolari categorie di dati di cui all'art. 9, par. 1, del regolamento, da parte di soggetti privati))

((1. I soggetti privati che partecipano al Sistema statistico nazionale ai sensi della [legge 28 aprile 1998, n. 125](#), raccolgono o

trattano ulteriormente particolari categorie di dati per scopi statistici di regola in forma anonima, fermo restando quanto previsto dall'art. 6-bis, comma 1, del decreto legislativo 6 settembre 1989, n. 322, come introdotto dal decreto legislativo 30 luglio 1999, n. 281, e successive modificazioni e integrazioni.

2. In casi particolari in cui scopi statistici, legittimi e specifici, del trattamento delle particolari categorie di dati non possono essere raggiunti senza l'identificazione anche temporanea degli interessati, per garantire la legittimita' del trattamento medesimo e' necessario che concorrano i seguenti presupposti:

a) l'interessato abbia espresso liberamente il proprio consenso sulla base degli elementi previsti nelle informazioni sul trattamento di dati personali di cui all'art. 13 del regolamento;

b) il titolare adotti specifiche misure per mantenere separati i dati identificativi gia' al momento della raccolta, salvo che cio' risulti irragionevole o richieda uno sforzo manifestamente sproporzionato;

c) il trattamento sia compreso nel programma statistico nazionale.

3. Il consenso e' manifestato per iscritto. Qualora la raccolta delle particolari categorie di dati sia effettuata con particolari modalita', quali interviste telefoniche o assistite da elaboratore, il consenso, purché espresso, puo' essere documentato per iscritto. In tal caso, la documentazione delle informazioni rese all'interessato e dell'acquisizione del relativo consenso e' conservata dal titolare del trattamento per tre anni).

CAPO II

((INFORMAZIONI AGLI INTERESSATI, COMUNICAZIONE E DIFFUSIONE))

Art. 6

((Informazioni agli interessati))

((1. Oltre alle informazioni di cui all'art. 13 del regolamento, all'interessato o alle persone presso le quali i dati personali dell'interessato sono raccolti per uno scopo statistico e'

rappresentata l'eventualita' che essi possono essere trattati per altri scopi statistici, in conformita' a quanto previsto dal [decreto legislativo 6 settembre 1989, n. 322](#), dal regolamento e dal codice, e successive modificazioni e integrazioni.

2. Quando il trattamento riguarda dati personali non raccolti presso l'interessato e il conferimento delle informazioni a quest'ultimo richiede uno sforzo sproporzionato rispetto al diritto tutelato, in base a quanto previsto dall'art. 14, par. 5, lett. b) del regolamento, le informazioni stesse si considerano rese se il trattamento e' incluso nel programma statistico nazionale o e' oggetto di pubblicita' con idonee modalita')).

Art. 7

((Comunicazione a soggetti non facenti parte del Sistema statistico nazionale))

((1. Ai soggetti che non fanno parte del Sistema statistico nazionale possono essere comunicati, sotto forma di collezioni campionarie, dati individuali privi di ogni riferimento che ne permetta il collegamento con gli interessati e comunque secondo modalita' che rendano questi ultimi non identificabili)).

Art. 8

((Autorita' di controllo))

((1. La Commissione per la garanzia dell'informazione statistica di cui all'[art. 12 del decreto legislativo 6 settembre 1989, n. 322](#) contribuisce alla corretta applicazione delle disposizioni delle presenti regole, segnalando al garante i casi di inosservanza)).

CAPO III

((DISPOSIZIONI FINALI))

Art. 9

((Raccolta dei dati))

((1. I soggetti di cui all'art. 1 pongono specifica attenzione nella selezione del preposto alla raccolta dei dati e nella definizione dell'organizzazione e delle modalita' di rilevazione, in modo da garantire il rispetto delle presenti regole e la tutela dei diritti degli interessati.

2. In ogni caso, il personale preposto alla raccolta si attiene alle disposizioni contenute nelle presenti regole alle istruzioni ricevute. In particolare:

a) rende nota la propria identita', la propria funzione e le finalita' della raccolta, anche attraverso adeguata documentazione;

b) fornisce le informazioni di cui all'art. 13 del regolamento e di cui all'art. 6 delle presenti regole, nonche' ogni altro chiarimento che consenta all'interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici o indebite pressioni;

c) non svolge contestualmente presso gli stessi interessati attivita' di rilevazione di dati per conto di piu' titolari, salvo espressa autorizzazione;

d) provvede tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite nel corso della raccolta;

e) assicura una particolare diligenza nella raccolta delle particolari categorie di dati di cui agli artt. 9, par., 1 e 10 del regolamento)).

Art. 10

((Conservazione dei dati))

((1. I dati personali possono essere conservati anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati, nel rispetto del principio di limitazione della conservazione di cui all'art. 5, par.1, lett. e) del regolamento e all'[art. 6-bis del decreto legislativo 6 settembre 1989, n. 322](#) e successive modificazioni e integrazioni)).

Art. 11

((Esercizio dei diritti dell'interessato))

((1. In attuazione dell'[art. 6-bis, comma 8, del decreto legislativo 6 settembre 1989, n. 322](#), il titolare o il responsabile del trattamento annotano in appositi spazi o registri le modifiche richieste dall'interessato, senza variare i dati originariamente immessi nell'archivio, qualora tali operazioni non producano effetti significativi sull'analisi statistica o sui risultati statistici

connessi al trattamento. In particolare, non si procede alla variazione se le modifiche richieste contrastano con le classificazioni e con le metodologie statistiche adottate in conformita' alle norme internazionali comunitarie e nazionali)).

Art. 12.

((Disposizioni finali))

((1. Coloro che, anche per motivi di lavoro, studio e ricerca abbiano legittimo accesso ai dati personali trattati per scopi statistici, conformano il proprio comportamento anche alle seguenti disposizioni:

a) i dati personali possono essere utilizzati soltanto per gli scopi definiti all'atto della progettazione del trattamento;

b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme al regolamento, al codice, alle presenti regole e alle istruzioni ricevute;

c) i dati personali e le notizie non disponibili al pubblico di cui si venga a conoscenza in occasione dello svolgimento dell'attivita' statistica o di attivita' ad essa strumentali non possono essere diffusi, ne' altrimenti utilizzati per interessi privati, propri o altrui;

d) il lavoro svolto deve essere oggetto di adeguata documentazione;

e) le conoscenze professionali in materia di protezione dei dati personali devono essere adeguate costantemente all'evoluzione delle metodologie e delle tecniche;

f) la comunicazione e la diffusione dei risultati statistici devono essere favorite, in relazione alle esigenze conoscitive degli utenti, purché nel rispetto delle norme sulla protezione dei dati personali.

2. I soggetti di cui al comma 1 sono tenuti a conformarsi alle disposizioni delle presenti regole, anche quando non siano vincolati al rispetto del segreto d'ufficio o del segreto professionale. I titolari del trattamento adottano le misure opportune per garantire la conoscenza di tali disposizioni da parte dei responsabili del trattamento e delle persone autorizzate.

3. I comportamenti non conformi alle presenti regole di condotta devono essere immediatamente segnalati al responsabile o al titolare del trattamento)).

Art. 13

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 25/3/2019, N. 71)))

Art. 14

((**ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 25/3/2019, N. 71))**)

ALLEGATO A.4

REGOLE DEONTOLOGICHE PER TRATTAMENTI A FINI STATISTICI O DI RICERCA SCIENTIFICA

CAPO I

AMBITO DI APPLICAZIONE E PRINCIPI GENERALI

(Delibera del Garante n. 515 del 19 dicembre 2018, in G.U. 14 gennaio 2019, n. 11)

**((IL GARANTE
PER LA PROTEZIONE DEI DATI PERSONALI**

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il [regolamento \(UE\) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva 95/46/CE \(regolamento generale sulla protezione dei dati\)](#) (di seguito «Regolamento» e «RGPD»);

Visto il [decreto legislativo 10 agosto 2018, n. 101](#), recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del [regolamento \(UE\) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva 95/46/CE](#)»;

Visto il [Codice in materia di protezione dei dati personali, decreto legislativo 30 giugno 2003, n. 196](#), (di seguito Codice), così come modificato dal predetto [decreto legislativo n. 101 del 2018](#);

Visto il Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e scientifici

allegato A.4 al Codice;

Visto l'[art. 5-ter del decreto legislativo 14 marzo 2013, n. 33](#), Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicit , trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, relativo all'accesso per fini scientifici ai dati elementari raccolti per finalit  statistiche;

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del garante n. 1/2000;

Relatore la dott.ssa Giovanna Bianchi Clerici;

Premesso

L'[art. 20, commi 3 e 4, del decreto legislativo 101 del 2018](#) ha conferito al garante il compito di verificare, nel termine di 90 giorni dalla sua entrata in vigore, la conformit  al regolamento delle disposizioni contenute nei codici di deontologia e buona condotta di cui agli allegati A.1, A.2, A.3, A.4 e A.6 al Codice.

Le disposizioni ritenute compatibili, ridenominate regole deontologiche, dovranno essere pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministero della giustizia, saranno successivamente riportate nell'allegato A al Codice.

Il Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, allegato A.4 al Codice, cessa di produrre effetti dalla pubblicazione delle predette regole nella Gazzetta Ufficiale ([art. 20, comma 3, del decreto legislativo n. 101 del 2018](#)).

Resta fermo che successivamente, il Garante potr  promuovere la revisione di tali regole, secondo la procedura di cui all'art. 2-quater del Codice, in base alla quale lo schema delle regole deontologiche, nell'osservanza del principio di rappresentativit , deve essere sottoposto a consultazione pubblica, per almeno sessanta giorni.

Osserva

Nell'ambito del presente provvedimento sono individuate le disposizioni del Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici, allegato A4 al Codice, adottato con provvedimento del garante n. 2 del 16 giugno 2004, Gazzetta Ufficiale 14 agosto 2004, n. 190, ritenute non conformi al Regolamento e, in allegato sono riportate le disposizioni conformi, ridenominate regole deontologiche per trattamenti a fini statistici o di ricerca scientifica.

Le regole si applicano ai trattamenti di dati personali effettuati fini statistici, al di fuori del Sistema statistico nazionale, o di

ricerca scientifica, fermo restando il rispetto dei principi e degli specifici adempimenti richiesti dal Regolamento e dal Codice.

Il rispetto delle disposizioni contenute nelle regole deontologiche costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali e il mancato rispetto delle stesse comporta l'applicazione della sanzione di cui all'art. 83, paragrafo 5 del Regolamento (articoli 2-quater, comma 4, e 166, comma 2, del Codice).

A regime, l'art. 106 del Codice, così come novellato dall'[art. 8 dal decreto legislativo n. 101/2018](#), prevede specificamente che le regole deontologiche individuino garanzie adeguate per i diritti e le libertà dell'interessato e si applicano ai soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per fini statistici o di ricerca scientifica ricompresi nell'ambito del Sistema statistico nazionale.

In via generale, si rappresenta che si è tenuto conto dell'esigenza di contemperare il diritto alla libertà di ricerca con altri diritti fondamentali dell'individuo, in ossequio al principio di proporzionalità (cons. 4 del Regolamento), verificando la conformità delle disposizioni del Codice di deontologia, in particolare, ai considerando e agli articoli dedicati alla ricerca statistica e scientifica (cons. 26, 50, 52, 53, 62, 156, 157, 159, 162, 163, art. 5, comma 1 lettera b) ed e), art. 9, art. 10, e art. 89 § 1, del Regolamento).

1. Modifiche generali.

Preliminarmente, si osserva che si è reso necessario aggiornare i riferimenti normativi presenti nel Codice di deontologia e la semantica utilizzata rispetto al rinnovato quadro normativo europeo e nazionale di riferimento.

Si è reso necessario, inoltre, eliminare il preambolo del Codice di deontologia, dovendosi, in base al richiamato [art. 20 del decreto legislativo n. 101 del 2018](#), ridenominare solo le disposizioni dello stesso.

Cionondimeno, i principi e le fonti di diritto sovranazionale ivi richiamati, sono, in ogni caso, da ritenersi a fondamento dei trattamenti di dati personali effettuati a fini di ricerca scientifica o statistici (cons. 159 e 162 del Regolamento).

2. Disposizioni ritenute incompatibili.

All'art. 1, comma 1, lettera c), è stata eliminata la definizione di «dato identificativo indiretto», in quanto tale definizione è stata ritenuta incompatibile con il Regolamento. Il legislatore nazionale, infatti, nell'adeguare il Codice al Regolamento, con il [decreto legislativo n. 101 del 2018](#), ha abrogato l'art. 4, comma 1,

lettera c), del Codice, che conteneva la definizione di «dati identificativi», da intendersi come i «dati personali che permettono l'identificazione diretta dell'interessato».

Resta, invece valida la definizione di «istituto o ente di ricerca», di cui alla lettera e), dell'articolo in esame, che deve esser interpretata alla luce del nuovo quadro normativo di settore di cui all'[art. 5-ter del decreto legislativo 33 del 2013](#), che ha demandato al Comstat l'individuazione, sentito il garante, dei criteri per il riconoscimento degli enti di ricerca e delle strutture di ricerca di istituzioni pubbliche e private, avuto riguardo agli scopi istituzionali perseguiti, all'attività svolta e all'organizzazione interna in relazione all'attività di ricerca, nonché alle misure adottate per garantire la sicurezza dei dati. Tali criteri sono stati di recente individuati nelle linee guida per l'accesso a fini scientifici ai dati elementari del Sistema statistico nazionale ([Gazzetta Ufficiale n. 287 dell'11 dicembre 2018](#)).

L'art. 4, «Identificabilità dell'interessato», è stato ritenuto necessario, in primo luogo, sostituire la parola «identificativi», al comma 1, lettera a), con la seguente locuzione «dati che ... identificano» l'unità statistica in quanto la definizione di «dati identificativi» di cui all'art. 4, comma 1, lettera c), del Codice è stata abrogata dal [decreto legislativo n. 101 del 2018](#), e non è più prevista dal Regolamento; in secondo luogo, il comma 1, lettera c), è stato ritenuto incompatibile nella misura in cui introduceva, per la valutazione del rischio di identificabilità degli interessati, dei parametri predefiniti che non sono in linea con il quadro giuridico introdotto dal Regolamento. Rispetto alle indicazioni fornite dal considerando 26, che per l'identificabilità di una persona indica, in particolare, che si tengano in considerazione «tutti i mezzi» di cui il titolare può ragionevolmente avvalersi, la disposizione in esame poneva come parametri predefiniti la tipologia di dati comunicati o diffusi, la proporzione tra i mezzi per l'identificazione e la lesione o il pericolo di lesione dei diritti degli interessati, cioè anche alla luce del vantaggio che ne poteva trarre il titolare. Tale disposizione, quindi, nel fornire ai titolari delle coordinate per valutare l'identificabilità dell'interessato attualmente superate, manifestava anche un approccio alla definizione e valutazione del rischio più circoscritte rispetto a quella del Regolamento in cui tale valutazione deve tener conto delle nuove tecnologie utilizzate, della natura, dell'oggetto, del contesto e delle finalità di ogni tipo di trattamento, (cfr. anche cons. 84, 89, 93 e 95 e articoli 5, § 1, lettera e), 24, 35 e 36 del Regolamento).

L'art. 5, «Criteri per la valutazione del rischio di identificazione», è stato mantenuto considerandosi, in via generale, compatibile con il Regolamento, nella misura in cui si limita a fornire alcuni parametri, orientativi, non esaustivi, per la

valutazione del rischio di identificazione degli interessati. Al fine di assicurarne un'applicazione conforme al Regolamento, si e', tuttavia, ritenuto necessario modificarlo con l'aggiunta di un «anche» (al primo comma, tra le parole «tiene conto» e «dei seguenti»), affinche' sia chiaro che i parametri ivi indicati devono, comunque, considerarsi meramente esemplificativi e, soprattutto, non alternativi rispetto al nuovo quadro giuridico introdotto dal Regolamento sopra descritto.

Sono stati modificati il titolo del Capo II da «Informativa, comunicazione e diffusione» in «Informazioni agli interessati, comunicazione e diffusione» e la rubrica dell'art. 6 da «Informativa» a «Informazioni agli interessati», per omogeneita' con il Regolamento.

L'art. 6, «Informazioni agli interessati», il comma 2 e' risultato incompatibile con il Regolamento nella parte in cui prevedeva alcune deroghe all'obbligo di informativa in caso di raccolta dei dati presso gli interessati. In particolare, tale comma e' stato eliminato, che consentiva di fornire un'informativa differita, per la parte riguardante le specifiche finalita' e modalita' del trattamento, qualora cio' risultasse necessario per il raggiungimento dell'obiettivo dell'indagine. Cio', in quanto l'art. 13 del Regolamento non prevede alcuna forma di deroga o semplificazione agli obblighi informativi quando i dati sono raccolti presso gli interessati.

L'art. 6, comma 3, che consente ad un soggetto di rispondere in nome e per conto di un altro, e' stato considerato compatibile con il Regolamento e con l'art. 105, comma 3, del Codice, in quanto definisce le specifiche circostanze in cui tale modalita' di raccolta e' possibile. Sul punto, tuttavia, deve precisarsi che, il principio di responsabilizzazione impone, in ogni caso, al titolare del trattamento di porre in essere specifiche misure per verificare, ed essere in grado di dimostrare, che il rispondente sia effettivamente legittimato a fornire i dati di un terzo.

E' stato altresì ritenuto incompatibile l'art. 6, comma 4, che individuava alcuni casi di deroga all'obbligo di fornire, informazioni agli interessati quando i dati sono raccolti presso terzi, disponendo che il titolare dovesse dare preventiva informazione al garante delle modalita' prescelte, tra quelle indicate a titolo esemplificativo dalla norma. Parimenti, e' stato considerato incompatibile il comma 5 dell'articolo in esame, nella parte in cui, qualora il titolare avesse ritenuto di non utilizzare le forme di pubblicita' indicate al comma 4, poteva individuare idonee forme di pubblicita' da comunicare preventivamente al garante, che poteva prescrivere eventuali misure e accorgimenti. L'art. 14, § 5, lettera b), del Regolamento ora prevede, infatti, che le informazioni in caso di raccolta di dati presso terzi possano essere omesse nel caso in cui la comunicazione di tali informazioni risultasse impossibile o implicherebbe uno sforzo sproporzionato. Con

particolare riferimento ai trattamenti a fini di ricerca scientifica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'art. 89, § 1, non vi è, inoltre, l'obbligo di informare l'interessato nella misura in cui ciò rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento è tenuto comunque ad adottare misure appropriate per tutelare i diritti, la libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni.

L'art. 7 «Consenso» è stato eliminato perché le condizioni di liceità del trattamento, ed in particolare le condizioni per il consenso, sono disciplinate nel Regolamento (articoli 6 e 7).

L'art. 8 «Comunicazione e diffusione dei dati» è stato considerato incompatibile in quanto i presupposti di liceità di tali operazioni di trattamento sono adesso individuate nel Regolamento (articoli 6, 9 e 10) e nel Codice (articoli 2-ter, 2-sexies, 2-septies e 2-octies).

L'articolo in esame è stato, inoltre, considerato incompatibile nella parte in cui, al comma 4, ultimo alinea, e al comma 5 disciplinava il trasferimento di dati personali verso paesi terzi, adesso normato agli articoli 44 e seguenti del Regolamento.

È stata modificata la rubrica dell'art. 9 da «Trattamento di dati sensibili o giudiziari» in «Trattamento di categorie particolari di dati personali e di dati relativi a condanni penali e reati».

Fermi restando i presupposti di liceità del trattamento dei dati indicati nella rubrica dell'articolo in esame, nel Regolamento (articoli 6, 9 e 10) e nel Codice (articoli 2-ter, 2-sexies, 2-septies e 2-octies), l'art. 9, commi 2 e 3, è stato considerato incompatibile con il Regolamento nella misura in cui tali previsioni individuano predefiniti e specifici casi di applicazione del principio di minimizzazione di cui all'art. 5, § 1, lettera c), del Regolamento che pur tenendo conto della specificità dei trattamenti effettuati a fini statistici e di ricerca scientifica, richiede, oltre a una valutazione del rischio, caso per caso a cura del titolare, l'individuazione di misure tecniche e organizzative adeguate a tutela dell'interessato (articoli 24 e 35 del Regolamento).

L'art. 9, commi 4, lettera c), 5 e 6, è stato, invece, considerato incompatibile laddove individuava condizioni di liceità del trattamento per i dati sensibili o giudiziari differenti rispetto a quelle previste ora dal Regolamento e dal Codice.

L'art. 10 «Dati genetici» è stato considerato incompatibile in quanto il trattamento di tali dati deve essere effettuato in conformità all'art. 9 del Regolamento, all'art. 2-sexies, alle prescrizioni individuate dal garante ai sensi dell'[art. 21, del decreto legislativo 101 del 2018](#) e alle specifiche misure di garanzia che l'Autorità è chiamata ad adottare ai sensi dell'art. 2-septies del Codice.

L'art. 11 «Disposizioni particolari per la ricerca medica,

biomedica ed epidemiologica» e' stato modificato al comma 4 al solo fine di confermare le tutele assicurate in tale contesto agli interessati, cosi' come individuate dal richiamo, effettuato per relationem, all'art. 84 del Codice, ora abrogato. Restano ferme, in ogni caso, le misure di garanzia che saranno individuate dal garante, ai sensi dell'art. 2-septies, comma 4, lettera c).

L'art. 11, comma 5, e' stato, invece, considerato incompatibile, in quanto le circostanze in cui non e' necessario acquisire il consenso dell'interessato sono state individuate nel provvedimento prescrittivo adottato dal garante ai sensi dell'[art. 21 del decreto legislativo 101 del 2018](#) mentre le condizioni di liceita' del trattamento per le finalita' in esame sono previste dall'art. 110 del Codice.

E' stato modificato il titolo del Capo III da «Sicurezza e regole di condotta» in «Disposizioni finali».

L'art. 14 «Conservazione dei dati» e' stato aggiornato al primo comma con il rinvio al principio di limitazione della conservazione di cui all'art. 5, § 1, lettera e) del Regolamento. Le parti successive sono state eliminate in quanto sono risultate incompatibili con tale principio che unitamente al principio di responsabilizzazione, impone al titolare una nuova prospettiva e nuovi adempimenti per la valutazione del rischio, al fine di individuare, di volta in volta, adeguate misure, tecniche e organizzative, a garanzia degli interessati (articoli 24 e 35 del Regolamento).

L'art. 15 «Misure di sicurezza» e' stato ritenuto incompatibile, in quanto gli aspetti relativi alla sicurezza dei dati sono oggetto ora di specifiche previsioni del Regolamento che, nel rispetto del principio di responsabilizzazione, richiede anche un diverso approccio alle misure di sicurezza che devono esser individuate, fin dalla progettazione e per impostazione predefinita (articoli 24 e 25 del Regolamento), in conformita' all'art. 32 del Regolamento.

L'art. 16 «Esercizio dei diritti dell'interessato», al comma 1, e' stato considerato incompatibile, in quanto consentirebbe al titolare la possibilita' di limitare il diritto di rettifica o integrazione senza individuare garanzie adeguate, come richiesto, invece, dall'art. 89 del Regolamento. Il comma 2, e' stato riformulato per renderlo conforme al Regolamento.

E' stata, infine, aggiornata, la rubrica dell'art. 17, in «Disposizioni finali», onde evitare ambiguita' rispetto alle regole deontologiche di cui all'art. 2-quater del Codice e con i futuri codici di condotta, di cui all'art. 40 del Regolamento.

3. Regole deontologiche.

I predetti elementi, relativi all'aggiornamento della disciplina in materia, sono recepiti nelle «Regole deontologiche per il trattamento a fini statistici o di ricerca» in ragione di quanto disposto

dall'art. 20, comma 4, del decreto legislativo n. 101/2018 e riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante.

Tali «Regole deontologiche» sono volte a disciplinare i trattamenti in questione in attesa di un auspicabile aggiornamento delle stesse ai sensi degli articoli 2-quater e 106 e seguenti del Codice. Pertanto, si dispone la trasmissione delle suddette «Regole deontologiche» all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la relativa pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'Allegato A) al Codice.

Tutto cio' premesso il garante

Ai sensi dell'art. 20, comma 4, del decreto legislativo n. 101/2018, verificata la conformita' al regolamento delle disposizioni del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica, allegato A.4 al Codice, dispone che le medesime, riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante, siano pubblicate come «Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica» e ne dispone, altresì, la trasmissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'Allegato A) al Codice.

Roma, 19 dicembre 2018

**Il presidente
Soro**

**Il segretario generale
Busia**

**Il relatore
Bianchi Clerici**

**REGOLE DEONTOLOGICHE PER TRATTAMENTI
A FINI STATISTICI O DI RICERCA SCIENTIFICA))**

Art. 1.

((Definizioni))

((1. Ai fini delle presenti regole si applicano le definizioni

elencate nell'art. 4 del Regolamento con le seguenti integrazioni:

a) «risultato statistico», l'informazione ottenuta con il trattamento di dati personali per quantificare aspetti di un fenomeno collettivo;

b) «unita' statistica», l'entita' alla quale sono riferiti o riferibili i dati trattati;

c) «variabile pubblica», il carattere o la combinazione di caratteri, di tipo qualitativo o quantitativo, oggetto di una rilevazione statistica che faccia riferimento ad informazioni presenti in pubblici registri, elenchi, atti, documenti o fonti conoscibili da chiunque;

d) «istituto o ente di ricerca», un organismo pubblico o privato per il quale la finalita' di statistica o di ricerca scientifica risulta dagli scopi dell'istituzione e la cui attivita' scientifica e' documentabile;

e) «societa' scientifica», un'associazione che raccoglie gli studiosi di un ambito disciplinare, ivi comprese le relative associazioni professionali.

2. Salvo quando diversamente specificato, il riferimento a trattamenti per scopi statistici si intende comprensivo anche dei trattamenti per scopi scientifici)).

Art. 2

((Ambito di applicazione))

((1. Le presenti regole deontologiche si applicano all'insieme dei trattamenti effettuati per scopi statistici e scientifici -conformemente agli standard metodologici del pertinente settore disciplinare-, di cui sono titolari universita', altri enti o istituti di ricerca e societa' scientifiche, nonche' ricercatori che operano nell'ambito di dette universita', enti, istituti di ricerca e soci di dette societa' scientifiche.

2. Le presenti regole deontologiche non si applicano ai trattamenti per scopi statistici e scientifici connessi con attivita' di tutela della salute svolte da esercenti professioni sanitarie od organismi sanitari, ovvero con attivita' comparabili in termini di significativa ricaduta personalizzata sull'interessato, che restano regolati dalle pertinenti disposizioni)).

Art. 3

((Presupposti dei trattamenti))

((1. La ricerca e' effettuata sulla base di un progetto redatto conformemente agli standard metodologici del pertinente settore disciplinare, anche al fine di documentare che il trattamento sia effettuato per idonei ed effettivi scopi statistici o scientifici.

2. Il progetto di ricerca di cui al comma 1, inoltre:

a) specifica le misure da adottare nel trattamento di dati personali, al fine di garantire il rispetto delle presenti regole deontologiche, nonché della normativa in materia di protezione dei dati personali;

b) individua gli eventuali responsabili del trattamento

c) contiene una dichiarazione di impegno a conformarsi alle presenti regole deontologiche. Un'analoga dichiarazione è sottoscritta anche dai soggetti -ricercatori, responsabili e persone autorizzate al trattamento- che fossero coinvolti nel prosieguo della ricerca, e conservata conformemente a quanto previsto al comma 3.

3. Il titolare deposita il progetto presso l'università o ente di ricerca o società scientifica cui afferisce, la quale ne cura la conservazione, in forma riservata (essendo la consultazione del progetto possibile ai soli fini dell'applicazione della normativa in materia di dati personali), per cinque anni dalla conclusione programmata della ricerca.

4. Nel trattamento di dati relativi alla salute, i soggetti coinvolti osservano le regole di riservatezza e di sicurezza cui sono tenuti gli esercenti le professioni sanitarie o regole di riservatezza e sicurezza comparabili)).

Art. 4

((Identificabilità dell'interessato))

((1. Agli effetti dell'applicazione delle presenti regole:

a) un interessato si ritiene identificabile quando, con l'impiego di mezzi ragionevoli, è possibile stabilire un'associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati che la identificano;

b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:

risorse economiche;

risorse di tempo;

archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;

archivi, anche non nominativi, che forniscano ulteriori informazioni oltre quelle oggetto di comunicazione o diffusione;

risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;

conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la

produzione dei dati)).

Art. 5

((Criteri per la valutazione del rischio di identificazione))

((1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto anche dei seguenti criteri:

a) si considerano dati aggregati le combinazioni di modalita' alle quali e' associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensita' data dalla sintesi dei valori assunti da un numero di unita' statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia e' pari a tre;

b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;

c) i risultati statistici relativi a sole variabili pubbliche non sono soggette alla regola della soglia;

d) la regola della soglia puo' non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unita' statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;

e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;

f) si presume adeguatamente tutelata la riservatezza nel caso in cui tutte le unita' statistiche di una popolazione presentano la medesima modalita' di una variabile)).

CAPO II

((INFORMAZIONI AGLI INTERESSATI, COMUNICAZIONE E DIFFUSIONE))

Art. 6

((Informazioni agli interessati))

((1. Nella raccolta di dati per uno scopo statistico, nell'ambito delle informazioni di cui all'art. 13 RGPD del decreto e' rappresentata all'interessato l'eventualita' che i dati personali possono essere conservati e trattati per altri scopi statistici o scientifici, per quanto noto adeguatamente specificati anche con riguardo alle categorie di soggetti ai quali i dati potranno essere comunicati.

2. Quando, con riferimento a parametri scientificamente attendibili, gli obiettivi dell'indagine, la natura dei dati e le circostanze della raccolta sono tali da consentire ad un soggetto di rispondere in nome e per conto di un altro in quanto familiare o convivente, l'informativa all'interessato puo' essere data per il tramite del soggetto rispondente, purché il trattamento non riguardi categorie particolari di dati personali o personali relativi a condanne penali e reati di cui, rispettivamente, agli [articoli 9 e 10 del regolamento \(UE\) n. 2016/679](#).

3. Quando i dati sono raccolti presso terzi, ovvero il trattamento effettuato per scopi statistici o scientifici riguarda dati raccolti per altri scopi, e l'informativa comporta uno sforzo sproporzionato rispetto al diritto tutelato, il titolare adotta idonee forme di pubblicita', ad esempio, con le seguenti modalita':

per trattamenti riguardanti insiemi numerosi di soggetti distribuiti sull'intero territorio nazionale, inserzione su almeno un quotidiano di larga diffusione nazionale o annuncio presso un'emittente radiotelevisiva a diffusione nazionale;

per trattamenti riguardanti insiemi numerosi di soggetti distribuiti su un'area regionale (o provinciale), inserzione su un quotidiano di larga diffusione regionale (o provinciale) o annuncio presso un'emittente radiotelevisiva a diffusione regionale (o provinciale);

per trattamenti riguardanti insiemi di specifiche categorie di soggetti, identificate da particolari caratteristiche demografiche e/o da particolari condizioni formative o occupazionali o analoghe, inserzione in strumenti informativi di cui gli interessati sono normalmente destinatari)).

Art. 7

((Principi applicabili al trattamento delle particolari categorie di dati di cui all'art. 9, § 1 e di dati relativi a condanne penali e reati di cui all'art. 10 del Regolamento)).

((1. Le particolari categorie di dati di cui all'art. 9, § 1 e i dati relativi a condanne penali e reati di cui all'art. 10, trattati per scopi statistici e scientifici devono essere di regola in forma anonima.

2. I soggetti di cui all'art. 2, comma 1, possono trattare categorie particolari di dati personali per scopi statistici e

scientifici quando:

a) l'interessato ha espresso liberamente il proprio consenso sulla base degli elementi previsti per l'informativa;

b) il consenso e' manifestato per iscritto. Quando la raccolta delle categorie particolari di dati personali e' effettuata con modalita' -quali interviste telefoniche o assistite da elaboratore o simili- che rendono particolarmente gravoso per l'indagine acquisirlo per iscritto, il consenso, purché esplicito, può essere documentato per iscritto. In tal caso, la documentazione dell'informativa resa all'interessato e dell'acquisizione del relativo consenso e' conservata dal titolare del trattamento per tre anni)).

Art. 8

((Disposizioni particolari per la ricerca medica, biomedica ed epidemiologica))

((1. La ricerca medica, biomedica ed epidemiologica e' sottoposta all'applicazione delle presenti regole del nei limiti di cui all'art. 2, comma 2.

2. La ricerca di cui al comma 1 si svolge nel rispetto degli orientamenti e delle disposizioni internazionali e comunitarie in materia, quali la Convenzione sui diritti dell'uomo e sulla biomedicina del 4 aprile 1997, ratificata con [legge 28 marzo 2001, n. 145](#), la Raccomandazione del Consiglio d'Europa R(97)5 adottata il 13 febbraio 1997 relativa alla protezione dei dati sanitari e la dichiarazione di Helsinki dell'Associazione medica mondiale sui principi per la ricerca che coinvolge soggetti umani.

3. Nella ricerca di cui al comma 1, le informazioni sul trattamento di dati personali mettono in grado gli interessati di distinguere le attivita' di ricerca da quelle di tutela della salute.

4. Nel manifestare il proprio consenso ad un'indagine medica o epidemiologica, l'interessato e' richiesto di dichiarare se vuole conoscere o meno eventuali scoperte inattese che emergano a suo carico durante la ricerca. In caso positivo, i dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato -o, in caso di impossibilita' fisica, incapacita' di agire o incapacita' di intendere o di volere dell'interessato, a chi ne esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'[art. 4 della legge 22 dicembre 2017, n. 219](#) o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato-, da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare, fatta eccezione per i dati personali forniti in precedenza dal medesimo interessato. Il titolare, il responsabile o le persone designate possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che

nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono deputati a trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai predetti soggetti. L'atto di designazione individua appropriate modalita' e cautele rapportate al contesto nel quale e' effettuato il trattamento di dati. Quando, il consenso non puo' essere richiesto, tali eventi sono comunque comunicati all'interessato nel rispetto di quanto sopra qualora rivestano un'importanza rilevante per la tutela della salute dello stesso)).

Art. 9

((Attivita' di controllo))

((1. Le universita', gli altri istituti o enti di ricerca e le societa' scientifiche conservano la documentazione relativa ai progetti di ricerca presentati e agli impegni sottoscritti dai ricercatori. ai sensi dell'art. 3, commi 1 e 2, delle presenti regole deontologiche.

2. Gli enti di cui al comma 1:

a) assicurano la diffusione e il rispetto delle presenti regole deontologiche fra tutti coloro che, all'interno o all'esterno dell'organizzazione, sono in qualunque forma coinvolti nel trattamento dei dati personali realizzato nell'ambito delle ricerche, anche adottando opportune misure sulla base dei propri statuti e regolamenti;

b) segnalano al garante le violazioni delle regole deontologiche di cui vengono a conoscenza)).

CAPO III

((DISPOSIZIONI FINALI))

Art. 10

((Raccolta dei dati))

((1. I soggetti di cui all'art. 2, comma 1, pongono specifica

attenzione nella selezione del personale preposto alla raccolta dei dati e nella definizione dell'organizzazione e delle modalita' di rilevazione, in modo da garantire il rispetto delle presenti regole deontologiche e la tutela dei diritti degli interessati.

2. Il personale preposto alla raccolta si attiene alle disposizioni contenute rispetto nelle presenti regole deontologiche e alle istruzioni ricevute. In particolare:

a) rende nota la propria identita', la propria funzione e le finalita' della raccolta, anche attraverso adeguata documentazione;

b) fornisce le informazioni di cui all'art. 13 del regolamento ed all'art. 6 del presente Codice nonche' ogni altro chiarimento che consenta all'interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici ed indebite pressioni;

c) non svolge contestualmente presso gli stessi interessati attivita' di rilevazione di dati personali per conto di piu' titolari, salvo espressa autorizzazione;

d) provvede tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite nel corso della raccolta;

e) assicura una particolare diligenza nella raccolta delle particolari categorie di dati di cui agli articoli 9, § 1, e dei dati di cui all'art. 10 Regolamento)).

Art. 11

((Conservazione dei dati))

((1. I dati personali possono essere conservati per scopi statistici o scientifici anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati, in conformita' all'art. 5, § 1 lettera e) del Regolamento)).

Art. 12

((Esercizio dei diritti dell'interessato))

((1. Qualora, in caso di esercizio dei diritti di cui agli art. 15 e seguenti del Regolamento, sono necessarie modifiche ai dati che riguardano l'interessato, il titolare del trattamento provvede ad annotare, in appositi spazi o registri, le modifiche richieste dall'interessato, senza variare i dati originariamente immessi nell'archivio)).

Art. 13

((Disposizioni finali))

((1. I responsabili e le persone autorizzate del trattamento che per motivi di lavoro e ricerca, abbiano legittimo accesso ai dati personali trattati per scopi statistici e scientifici, conformano il proprio comportamento anche alle seguenti disposizioni:

a) i dati personali possono essere utilizzati soltanto per gli scopi definiti nel progetto di ricerca di cui all'art. 3;

b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute;

c) i dati personali e le notizie non disponibili al pubblico di cui si venga a conoscenza in occasione dello svolgimento dell'attività statistica o di attività ad essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui;

d) il lavoro svolto è oggetto di adeguata documentazione;

e) le conoscenze professionali in materia di protezione dei dati personali sono adeguate costantemente all'evoluzione delle metodologie e delle tecniche;

f) la comunicazione e la diffusione dei risultati statistici sono favorite, in relazione alle esigenze conoscitive della comunità scientifica e dell'opinione pubblica, nel rispetto della disciplina sulla protezione dei dati personali;

g) i comportamenti non conformi alle presenti regole deontologiche sono immediatamente segnalati al titolare o al responsabile trattamento)).

Art. 14

((Adeguamento))

((1. La corrispondenza delle disposizioni delle regole deontologiche alla normativa, anche di carattere internazionale, introdotta in materia di protezione dei dati personali trattati a fini di statistica e di ricerca scientifica è verificata nel tempo anche su segnalazione dei soggetti che le applicano. Ciò ai fini dell'introduzione nelle regole medesime delle modifiche necessarie al fine del coordinamento con dette fonti, ovvero, qualora tali modifiche incidano in maniera apprezzabile sulla disciplina delle presenti regole, e ai fini dell'adozione delle nuove regole ai sensi dell'art. 2-quater del Codice)).

Art. 15

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 25/3/2019, N. 71)))

Art. 16

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 25/3/2019, N. 71)))

Art. 17

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 25/3/2019, N. 71)))

Art. 18

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 25/3/2019, N. 71)))

Art. 19

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 25/3/2019, N. 71)))

((ALLEGATO A.5

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I SISTEMI INFORMATIVI GESTITI DA SOGGETTI PRIVATI IN TEMA DI CREDITI AL CONSUMO, AFFIDABILITA' E PUNTUALITA' NEI PAGAMENTI))

(Provvedimento del Garante n. 8 del 16 novembre 2004, in G.U. 23 dicembre 2004, n. 300)

((IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella seduta odierna, con la partecipazione del prof. Stefano Rodota', presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto l'[art. 27 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995](#), secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificita' settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visti gli [articoli 12 e 154, comma 1, lettera e\) del Codice in materia di protezione dei dati personali \(decreto legislativo 30](#)

giugno 2003, n. 196), i quali attribuiscono al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentativita' e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformita' alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto l'art. 117 del codice con il quale e' stato demandato al Garante il compito di promuovere la sottoscrizione di un Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo, nonche' riguardanti l'affidabilita' e la puntualita' nei pagamenti da parte degli interessati;

Visto il provvedimento generale del Garante adottato il 31 luglio 2002 (in Bollettino del Garante n. 30/2002, p. 47) con il quale, nelle more dell'adozione del predetto codice di deontologia e di buona condotta, sono state nel frattempo prescritte, ai soggetti privati che gestiscono sistemi informativi di rilevazione di rischi creditizi, nonche' alle banche e societa' finanziarie che vi accedono, alcune prime misure da adottare al fine di conformare il relativo trattamento ai principi in materia di protezione dei dati personali;

Visto il provvedimento del 10 aprile 2002, pubblicato nella Gazzetta Ufficiale della Repubblica italiana 8 maggio 2002, n. 106, con il quale il Garante ha promosso la sottoscrizione del codice di deontologia e di buona condotta;

Viste le comunicazioni pervenute al Garante in risposta al citato provvedimento del 10 aprile 2002, con le quali diversi soggetti privati, associazioni di categoria ed associazioni di consumatori hanno manifestato la volonta' di partecipare all'adozione di tale codice e rilevato che si e' anche formato un apposito gruppo di lavoro composto da rappresentanti dei predetti soggetti;

Considerato che il testo del codice di deontologia e di buona condotta e' stato oggetto di ampia diffusione anche attraverso la sua pubblicazione sul sito Internet di questa Autorita', resa nota tramite avviso nella Gazzetta Ufficiale della Repubblica italiana 18 agosto 2004, n. 193, al fine di favorire il piu' ampio dibattito e di permettere la raccolta di eventuali osservazioni e integrazioni al testo medesimo da parte di tutti i soggetti interessati;

Viste le osservazioni pervenute a seguito di tale avviso e le modifiche apportate allo schema del codice, poi sottoscritto il 12 novembre 2004;

Constatata la conformita' del codice di deontologia e di buona condotta alle leggi ed ai regolamenti anche in relazione a quanto previsto dall'art. 12 del Codice;

Visto l'art. 5 del codice di deontologia e di buona condotta;

Considerato che dalle predette consultazioni sono emersi anche alcuni dettagli operativi che rendono necessario indicare modalita' di attuazione idonee ed efficaci delle disposizioni in materia di informativa da rendere agli interessati ai sensi dell'art. 13 del Codice;

Ritenuto pertanto indispensabile prescrivere, ai sensi dell'art. 154, comma 1, lettera c), del Codice, un modello unico per l'informativa, basato su espressioni chiare, semplici e di agevole comprensione, e da adottare da tutti i soggetti privati titolari dei trattamenti di dati personali effettuati, in modo effettivo ed uniforme;

Rilevato che il rispetto delle disposizioni contenute nel codice di deontologia e di buona condotta costituisce condizione essenziale per la liceita' e la correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici (art. 12, comma 3, del Codice);

Rilevato altresì che i titolari del trattamento sono tenuti a fare uso del modello unico di informativa che il presente provvedimento prescrive, al quale potranno apportarvi eventuali modifiche sostanziali o integrazioni con esso compatibili, unicamente previo assenso di questa Autorita', salvi eventuali adattamenti meramente formali;

Considerato che, ai sensi dell'art. 12, comma 2, del codice, il codice di deontologia e di buona condotta deve essere pubblicato nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, riportato nell'allegato a) al medesimo Codice;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000, adottato con [deliberazione n. 15 del 28 giugno 2000](#) e pubblicato nella Gazzetta Ufficiale della Repubblica italiana n. 162 del 13 luglio 2000;

Relatore il dott. Mauro Paissan;

Tutto cio' premesso il Garante:

a) dispone la trasmissione del codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilita' e puntualita' nei pagamenti, che figura in allegato, all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministro della giustizia per essere riportato nell'allegato a) al Codice;

b) individua, in allegato alla presente deliberazione, il modello di informativa contenente i requisiti minimi che, ai sensi dell'art. 154, comma 1, lettera c), del codice, prescrive a tutti i titolari del trattamento interessati di utilizzare nei termini di cui in

motivazione.

Roma, 16 novembre 2004

Il presidente: Rodota'

**CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I SISTEMI INFORMATIVI
GESTITI DA SOGGETTI PRIVATI IN TEMA DI CREDITI AL CONSUMO,
AFFIDABILITA' E PUNTUALITA' NEI PAGAMENTI**

Preambolo

I sottoindicati soggetti privati sottoscrivono il presente codice di deontologia e di buona condotta sulla base delle seguenti premesse:

1) il trattamento di dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di credito al consumo o comunque riguardanti l'affidabilita' e la puntualita' dei pagamenti, deve svolgersi nel rispetto dei diritti, delle liberta' fondamentali e della dignita' delle persone interessate, in particolare del diritto alla protezione dei dati personali, del diritto alla riservatezza e del diritto all'identita' personale;

2) con il presente codice sono individuate adeguate garanzie e modalita' di trattamento a tutela dei diritti degli interessati da osservare nel perseguire finalita' di tutela del credito e di contenimento dei relativi rischi, in modo da agevolare anche l'accesso al credito al consumo e ridurre il rischio di eccessivo indebitamento da parte degli interessati;

3) la sottoscrizione del presente codice e' promossa dal Garante per la protezione dei dati personali nell'ambito delle associazioni rappresentative degli operatori del settore, ai sensi degli [articoli 12 e 117 del Codice in materia di protezione dei dati personali \(decreto legislativo 30 giugno 2003, n. 196/2003\)](#);

4) tutti coloro che utilizzano dati personali per le finalita' sopra indicate devono osservare le regole di comportamento stabilite dal presente codice come condizione essenziale per la liceita' e la correttezza del trattamento;

5) gli stessi operatori del settore devono rispettare, altresì, le garanzie previste dal predetto Codice, in particolare in tema di manifestazione del consenso e di altri presupposti di liceita';

6) il presente codice non riguarda sistemi informativi di cui sono titolari soggetti pubblici e, in particolare, il servizio di centralizzazione dei rischi gestito dalla Banca d'Italia (articoli 13, 53, comma 1, lettera b), 60, comma 1, 64, 67, comma 1, lettera b), 106, 107, 144 e 145 del [decreto legislativo 1° settembre 1993, n. 385](#) - Testo unico delle leggi in materia bancaria e creditizia;

delibera Cicr del 29 marzo 1994; provvedimento Banca d'Italia 10 agosto 1995 - [circolare Banca d'Italia 11 febbraio 1991, n. 139](#) e successivi aggiornamenti). Al sistema centralizzato di rilevazione dei rischi di importo contenuto istituito con deliberazione Cicr del 3 maggio 1999 (in Gazzetta Ufficiale 8 luglio 1999, n. 158) si applicano alcuni principi stabiliti dal presente codice in tema di informativa agli interessati e di esercizio dei diritti, in quanto compatibili con la specifica disciplina di riferimento (v., in particolare, le istruzioni della Banca d'Italia nella Gazzetta Ufficiale 21 novembre 2000, n. 272).)

Art. 1.

((Definizioni))

((1. Ai fini del presente codice di deontologia e di buona condotta, si applicano le definizioni elencate nel [Codice in materia di protezione dei dati personali \(art. 4 decreto legislativo 30 giugno 2003, n. 196\)](#), di seguito denominato «Codice». Ai medesimi fini, si intende inoltre per:

a) «richiesta/rapporto di credito»: qualsiasi richiesta o rapporto riguardanti la concessione, nell'esercizio di un'attività commerciale o professionale, di credito sotto forma di dilazione di pagamento, di finanziamento o di altra analoga facilitazione finanziaria ai sensi del testo unico delle leggi in materia bancaria e creditizia ([decreto legislativo 1° settembre 1993, n. 385](#));

b) «regolarizzazione degli inadempimenti»: l'estinzione delle obbligazioni pecuniarie inadempite (derivanti sia da un mancato pagamento, sia da un ritardo), senza perdite o residui anche a titolo di interessi e spese o comunque a seguito di vicende estintive diverse dall'adempimento, in particolare a seguito di transazioni o concordati;

c) «sistema di informazioni creditizie»: ogni banca di dati concernenti richieste/rapporti di credito, gestita in modo centralizzato da una persona giuridica, un ente, un'associazione o un altro organismo in ambito privato e consultabile solo dai soggetti che comunicano le informazioni in essa registrate e che partecipano al relativo sistema informativo. Il sistema può contenere, in particolare:

1) informazioni creditizie di tipo negativo, che riguardano soltanto rapporti di credito per i quali si sono verificati inadempimenti;

2) informazioni creditizie di tipo positivo e negativo, che attengono a richieste/rapporti di credito a prescindere dalla sussistenza di inadempimenti registrati nel sistema al momento del loro verificarsi;

d) «gestore»: il soggetto privato titolare del trattamento dei dati personali registrati in un sistema di informazioni creditizie e

che gestisce tale sistema stabilendone le modalita' di funzionamento e di utilizzazione;

e) «partecipante»: il soggetto privato titolare del trattamento dei dati personali raccolti in relazione a richieste/rapporti di credito, che in virtu' di contratto o accordo con il gestore partecipa al relativo sistema di informazioni creditizie e puo' utilizzare i dati presenti nel sistema, obbligandosi a comunicare al gestore i predetti dati personali relativi a richieste/rapporti di credito in modo sistematico, in un quadro di reciprocita' nello scambio di dati con gli altri partecipanti. Fatta eccezione di soggetti che esercitano attivita' di recupero crediti, il partecipante puo' essere:

1) una banca;

2) un intermediario finanziario;

3) un altro soggetto privato che, nell'esercizio di un'attivita' commerciale o professionale, concede una dilazione di pagamento del corrispettivo per la fornitura di beni o servizi;

f) «consumatore»: la persona fisica che, in relazione ad una richiesta/rapporto di credito, agisce per scopi non riferibili all'attivita' imprenditoriale o professionale eventualmente svolta;

g) «tempo di conservazione dei dati»: il periodo nel quale i dati personali relativi a richieste/rapporti di credito rimangono registrati in un sistema di informazioni creditizie ed utilizzabili dai partecipanti per le finalita' di cui al presente codice;

h) «tecniche o sistemi automatizzati di credit scoring»: le modalita' di organizzazione, aggregazione, raffronto od elaborazione di dati personali relativi a richieste/rapporti di credito, consistenti nell'impiego di sistemi automatizzati basati sull'applicazione di metodi o modelli statistici per valutare il rischio creditizio, e i cui risultati sono espressi in forma di giudizi sintetici, indicatori numerici o punteggi, associati all'interessato, diretti a fornire una rappresentazione, in termini predittivi o probabilistici, del suo profilo di rischio, affidabilita' o puntualita' nei pagamenti)).

Art. 2.

((Finalita' del trattamento))

((1. Il trattamento dei dati personali contenuti in un sistema di informazioni creditizie e' effettuato dal gestore e dai partecipanti esclusivamente per finalita' correlate alla tutela del credito e al contenimento dei relativi rischi e, in particolare, per valutare la situazione finanziaria e il merito creditizio degli interessati o, comunque, la loro affidabilita' e puntualita' nei pagamenti.

2. Non puo' essere perseguito alcun altro scopo, specie se relativo a ricerche di mercato e promozione, pubblicita' o vendita diretta di prodotti o servizi)).

Art. 3.

((Requisiti e categorie dei dati))

((1. Il trattamento effettuato nell'ambito di un sistema di informazioni creditizie riguarda solo dati riferiti al soggetto che chiede di instaurare o e' parte di un rapporto di credito con un partecipante e al soggetto coobbligato, anche in solido, la cui posizione e' chiaramente distinta da quella del debitore principale.

2. Il trattamento non puo' riguardare i dati sensibili e quelli giudiziari, e concerne dati personali di tipo obiettivo, strettamente pertinenti e non eccedenti rispetto alle finalita' perseguite, relativi ad una richiesta/rapporto di credito, e concernenti anche ogni vicenda intervenuta a qualsiasi titolo o causa fino alla regolarizzazione degli inadempimenti, nel rispetto dei tempi di conservazione stabiliti dall'art. 6.

3. Per ogni richiesta/rapporto di credito segnalato ad un sistema di informazioni creditizie possono essere trattate le seguenti categorie di dati, che il gestore indica in un elenco reso agevolmente disponibile su un proprio sito della rete di comunicazione, nonche' comunica analiticamente agli interessati su loro richiesta:

a) dati anagrafici, codice fiscale o partita IVA;

b) dati relativi alla richiesta/rapporto di credito, descrittivi, in particolare, della tipologia di contratto, dell'importo del credito, delle modalita' di rimborso e dello stato della richiesta o dell'esecuzione del contratto;

c) dati di tipo contabile relativi ai pagamenti, al loro andamento periodico, all'esposizione debitoria anche residua e alla sintesi dello stato contabile del rapporto;

d) dati relativi ad attivita' di recupero del credito o contenziose, alla cessione del credito o a eccezionali vicende che incidono sulla situazione soggettiva o patrimoniale di imprese, persone giuridiche o altri enti.

4. Le codifiche ed i criteri eventualmente utilizzati per registrare dati in un sistema di informazioni creditizie e per facilitarne il trattamento sono diretti esclusivamente a fornire una rappresentazione oggettiva e corretta degli stessi dati, nonche' delle vicende del rapporto di credito segnalato. L'utilizzo di tali codifiche e criteri e' accompagnato da precise indicazioni circa il loro significato, fornite dal gestore, osservate dai partecipanti e rese agevolmente disponibili da entrambi, anche a richiesta degli interessati.

5. Nel sistema di informazioni creditizie sono registrati gli estremi identificativi del partecipante che ha comunicato i dati personali relativi alla richiesta/rapporto di credito. Tali estremi sono accessibili al gestore o agli interessati e non anche intermediari partecipanti)).

Art. 4.

((Modalita' di raccolta e registrazione dei dati))

((1. Salvo quanto previsto dal comma 5, il gestore acquisisce esclusivamente dai partecipanti i dati personali da registrare nel sistema di informazioni creditizie.

2. Il partecipante adotta idonee procedure di verifica per garantire la lecita utilizzabilita' nel sistema, la correttezza e l'esattezza dei dati comunicati al gestore.

3. All'atto del ricevimento dei dati, il gestore verifica la loro congruita' attraverso controlli di carattere formale e logico e, se i dati risultano incompleti od incongrui, li ritrasmette al partecipante che li ha comunicati, ai fini delle necessarie integrazioni e correzioni. All'esito dei controlli e delle eventuali integrazioni e correzioni, i dati sono registrati nel sistema di informazioni creditizie e resi disponibili a tutti i partecipanti.

4. Il partecipante verifica con cura i dati da esso trattati e risponde tempestivamente alle richieste di verifica del gestore, anche a seguito dell'esercizio di un diritto da parte dell'interessato.

5. Eventuali operazioni di eliminazione, integrazione o modificazione dei dati registrati in un sistema di informazioni creditizie sono disposte direttamente dal partecipante che li ha comunicati, ove tecnicamente possibile, ovvero dal gestore su richiesta del medesimo partecipante o d'intesa con esso, anche a seguito dell'esercizio di un diritto da parte dell'interessato, oppure in attuazione di un provvedimento dell'autorita' giudiziaria o del Garante.

6. I dati relativi al primo ritardo nei pagamenti in un rapporto di credito sono utilizzati e resi accessibili agli altri partecipanti nel rispetto dei seguenti termini:

a) nei sistemi di informazioni creditizie di tipo negativo, dopo almeno centoventi giorni dalla data di scadenza del pagamento o in caso di mancato pagamento di almeno quattro rate mensili non regolarizzate;

b) nei sistemi di informazioni creditizie di tipo positivo e negativo:

1) qualora l'interessato sia un consumatore, decorsi sessanta giorni dall'aggiornamento mensile di cui al successivo comma 8, oppure in caso di mancato pagamento di almeno due rate mensili consecutive, oppure quando il ritardo si riferisce ad una delle due ultime scadenze di pagamento. Nel secondo caso i dati sono resi accessibili dopo l'aggiornamento mensile relativo alla seconda rata consecutivamente non pagata;

2) negli altri casi, dopo almeno trenta giorni dall'aggiornamento mensile di cui al successivo comma 8 o in caso di mancato pagamento di una rata.

7. Al verificarsi di ritardi nei pagamenti, il partecipante, anche unitamente all'invio di solleciti o di altre comunicazioni, avverte l'interessato circa l'imminente registrazione dei dati in uno o piu' sistemi di informazioni creditizie. I dati relativi al primo ritardo di cui al comma 6 possono essere resi accessibili ai partecipanti solo decorsi almeno quindici giorni dalla spedizione del preavviso all'interessato.

8. Fermo restando quanto previsto dal comma 6, i dati registrati in un sistema di informazioni creditizie sono aggiornati periodicamente, con cadenza mensile, a cura del partecipante che li ha comunicati).

Art. 5.

((Informativa))

((1. Al momento della raccolta dei dati personali relativi a richieste/rapporti di credito, il partecipante informa l'interessato ai sensi dell'art. 13 del Codice anche con riguardo al trattamento dei dati personali effettuato nell'ambito di un sistema di informazioni creditizie.

2. L'informativa di cui al comma 1 reca in modo chiaro e preciso, nell'ambito della descrizione delle finalita' e delle modalita' del trattamento, nonche' degli altri elementi di cui all'art. 13 del Codice, le seguenti indicazioni:

a) estremi identificativi dei sistemi di informazioni creditizie cui sono comunicati i dati personali e dei rispettivi gestori;

b) categorie di partecipanti che vi accedono;

c) tempi di conservazione dei dati nei sistemi di informazioni creditizie cui sono comunicati;

d) modalita' di organizzazione, raffronto ed elaborazione dei dati, nonche' eventuale uso di tecniche o sistemi automatizzati di credit scoring;

e) modalita' per l'esercizio da parte degli interessati dei diritti previsti dall'art. 7 del Codice.

3. L'informativa di cui al comma 2 e' fornita agli interessati per iscritto secondo il modello allegato alla deliberazione che verifica la conformita' del presente codice e, se inserita in un modulo utilizzato dal partecipante, e' adeguatamente evidenziata e collocata in modo autonomo ed unitario, in parti o riquadri distinti da quelli relativi ad eventuali altre finalita' del trattamento effettuato dal medesimo partecipante.

4. L'informativa dovuta per effetto di eventuali aggiornamenti o modifiche relativi alle indicazioni rese ai sensi del comma 2, anche in caso di cambiamento della denominazione e della sede del gestore, e' fornita attraverso comunicazioni periodiche, nonche' su uno o piu' siti Internet e a richiesta degli interessati.

5. Ad integrazione dell'informativa resa dai partecipanti singolarmente ad ogni interessato, il gestore fornisce un'informativa piu' dettagliata attraverso modalita' ulteriori di diffusione delle informazioni al pubblico, anche mediante strumenti telematici.

6. Quando la richiesta di credito non e' accolta, il partecipante comunica all'interessato se, per istruire la richiesta di credito, ha consultato dati personali relativi ad informazioni creditizie di tipo negativo in uno o piu' sistemi, indicandogli gli estremi identificativi del sistema da cui sono state rilevate tali informazioni e del relativo gestore.

7. Il partecipante fornisce all'interessato le altre notizie di cui agli articoli 9, comma 1, lettera d), e 10, comma 1, lettera c)).

Art. 6.

((Conservazione e aggiornamento dei dati))

((1. I dati personali riferiti a richieste di credito, comunicati dai partecipanti, possono essere conservati in un sistema di informazioni creditizie per il tempo necessario alla relativa istruttoria e comunque non oltre centottanta giorni dalla data di presentazione delle richieste medesime. Se la richiesta di credito non e' accolta o e' oggetto di rinuncia il partecipante ne da' notizia al gestore con l'aggiornamento mensile di cui all'art. 4, comma 8. In tal caso, i dati personali relativi alla richiesta cui l'interessato ha rinunciato o che non e' stata accolta possono essere conservati nel sistema non oltre trenta giorni dalla data del loro aggiornamento.

2. Le informazioni creditizie di tipo negativo relative a ritardi nei pagamenti, successivamente regolarizzati, possono essere conservate in un sistema di informazioni creditizie fino a:

a) dodici mesi dalla data di registrazione dei dati relativi alla regolarizzazione di ritardi non superiori a due rate o mesi;

b) ventiquattro mesi dalla data di registrazione dei dati relativi alla regolarizzazione di ritardi superiori a due rate o mesi.

3. Decorsi i periodi di cui al comma 2, i dati sono eliminati dal sistema di informazioni creditizie se nel corso dei medesimi intervalli di tempo non sono registrati dati relativi ad ulteriori ritardi o inadempimenti.

4. Il partecipante ed il gestore aggiornano senza ritardo i dati relativi alla regolarizzazione di inadempimenti di cui abbiano conoscenza, avvenuta dopo la cessione del credito da parte del partecipante ad un soggetto che non partecipa al sistema, anche a seguito di richiesta dell'interessato munita di dichiarazione del soggetto cessionario del credito o di altra idonea documentazione.

5. Le informazioni creditizie di tipo negativo relative a

inadempimenti non successivamente regolarizzati possono essere conservate nel sistema di informazioni creditizie non oltre trentasei mesi dalla data di scadenza contrattuale del rapporto oppure, in caso di altre vicende rilevanti in relazione al pagamento, dalla data in cui e' risultato necessario il loro ultimo aggiornamento, o comunque dalla data di cessazione del rapporto.

6. Le informazioni creditizie di tipo positivo relative ad un rapporto che si e' esaurito con estinzione di ogni obbligazione pecuniaria, possono essere conservate nel sistema non oltre ventiquattro mesi dalla data di cessazione del rapporto o di scadenza del relativo contratto, ovvero dal primo aggiornamento effettuato nel mese successivo a tali date. Tenendo conto del requisito della completezza dei dati in rapporto alle finalita' perseguite (art. 11, comma 1, lettera d) del Codice), le predette informazioni di tipo positivo possono essere conservate ulteriormente nel sistema qualora in quest'ultimo risultino presenti, in relazione ad altri rapporti di credito riferiti al medesimo interessato, informazioni creditizie di tipo negativo concernenti ritardi od inadempimenti non regolarizzati. In tal caso, le informazioni creditizie di tipo positivo sono eliminate dal sistema allo scadere del termine previsto dal comma 5 per la conservazione delle informazioni di tipo negativo registrate nel sistema in riferimento agli altri rapporti di credito con l'interessato.

7. Qualora il consumatore interessato comunichi al partecipante la revoca del consenso al trattamento delle informazioni di tipo positivo, nell'ambito del sistema di informazioni creditizie, il partecipante ne da' notizia al gestore con l'aggiornamento mensile di cui all'art. 4, comma 8. In tal caso, e in quello in cui la revoca gli sia stata comunicata direttamente dall'interessato, il gestore registra la notizia nel sistema ed elimina le informazioni non oltre novanta giorni dall'aggiornamento o dalla comunicazione.

8. Prima dell'eliminazione dei dati dal sistema di informazioni creditizie nei termini indicati ai precedenti commi, il gestore puo' trasporre i dati su altro supporto, ai fini della limitata conservazione per il tempo necessario, esclusivamente in relazione ad esigenze di difesa di un proprio diritto in sede giudiziaria, nonche' della loro eventuale elaborazione statistica in forma anonima.

9. Le disposizioni del presente art. non riguardano la conservazione ad uso interno, da parte del partecipante, della documentazione contrattuale o contabile contenente i dati personali relativi alla richiesta/rapporto di credito)).

Art. 7.

((Utilizzazione dei dati))

((1. Il partecipante puo' accedere al sistema di informazioni creditizie anche mediante consultazione di copia della relativa banca

dati, rispetto a dati per i quali sussiste un suo giustificato interesse, riguardanti esclusivamente:

a) consumatori che chiedono di instaurare o sono parte di un rapporto di credito con il medesimo partecipante e soggetti coobbligati, anche in solido;

b) soggetti che agiscono nell'ambito della loro attivita' imprenditoriale o professionale per i quali sia stata avviata un'istruttoria per l'instaurazione di un rapporto di credito o comunque per l'assunzione di un rischio di credito, oppure che siano gia' parte di un rapporto di credito con il medesimo partecipante;

c) soggetti aventi un collegamento di tipo giuridico con quelli di cui alla lettera b), in particolare in quanto obbligati in solido o appartenenti a gruppi di imprese, sempre che i dati personali cui il partecipante intende accedere risultino oggettivamente necessari per valutare la situazione finanziaria e il merito creditizio dei soggetti di cui alla stessa lettera b).

2. Il sistema di informazioni creditizie e' accessibile dal partecipante e dal gestore solo da un numero limitato, rispetto all'intera organizzazione del titolare, di responsabili ed incaricati del trattamento designati per iscritto, con esclusivo riferimento ai dati strettamente necessari, pertinenti e non eccedenti in rapporto alle finalita' indicate nell'art. 2, in relazione alle specifiche esigenze derivanti dall'istruttoria di una richiesta di credito o dalla gestione di un rapporto, concretamente verificabili sulla base degli elementi in possesso dei partecipanti medesimi. Nei soli limiti e con le medesime modalita' appena indicate, il sistema e' accessibile anche da banche ed intermediari finanziari appartenenti al gruppo bancario del partecipante all'esclusivo fine di curare l'istruttoria per l'instaurazione del rapporto di credito con l'interessato o comunque per l'assunzione del relativo rischio.

3. I partecipanti accedono al sistema di informazioni creditizie attraverso le modalita' e gli strumenti anche telematici individuati per iscritto con il gestore, nel rispetto della normativa sulla protezione dei dati personali. I dati personali relativi a richieste/rapporti di credito registrati in un sistema di informazioni creditizie sono consultabili con modalita' di accesso graduale e selettivo, attraverso uno o piu' livelli di consultazione di informazioni sintetiche o riepilogative dei dati riferiti all'interessato, prima della loro visione in dettaglio e con riferimento anche ad eventuali dati riferiti a soggetti coobbligati o collegati ai sensi del comma 1. Sono, in ogni caso, precluse, anche tecnicamente, modalita' di accesso che permettano interrogazioni di massa o acquisizioni di elenchi di dati concernenti richieste/rapporti di credito relativi a soggetti diversi da quelli che hanno chiesto di instaurare o sono parte di un rapporto di credito con il partecipante.

4. Non e' inoltre consentito l'accesso ad un sistema di informazioni creditizie da parte di terzi, fatte salve le richieste

da parte di organi giudiziari e di polizia giudiziaria per ragioni di giustizia, oppure da parte di altre istituzioni, autorità, amministrazioni o enti pubblici nei soli casi previsti da leggi, regolamenti o normative comunitarie e con l'osservanza delle norme che regolano la materia)).

Art. 8.

((Accesso ed esercizio di altri diritti degli interessati))

((1. In relazione ai dati personali registrati in un sistema di informazioni creditizie, gli interessati possono esercitare i propri diritti secondo le modalità stabilite dal Codice, sia presso il gestore, sia presso i partecipanti che li hanno comunicati. Tali soggetti garantiscono, anche attraverso idonee misure organizzative e tecniche, un riscontro tempestivo e completo alle richieste avanzate.

2. Nella richiesta con la quale esercita i propri diritti, l'interessato indica anche, ove possibile, il codice fiscale e/o la partita IVA, al fine di agevolare la ricerca dei dati che lo riguardano nel sistema di informazioni creditizie.

3. Il terzo al quale l'interessato conferisce, per iscritto, delega o procura per l'esercizio dei propri diritti, può trattare i dati personali acquisiti presso un sistema di informazioni creditizie esclusivamente per finalità di tutela dei diritti dell'interessato, con esclusione di ogni altro scopo perseguito dal terzo medesimo o da soggetti ad esso collegati.

4. Il partecipante, al quale è rivolta una richiesta con cui è esercitato taluno dei diritti di cui all'art. 7 del Codice relativamente alle informazioni creditizie registrate in un sistema, fornisce direttamente riscontro nei termini previsti dall'art. 146, commi 2 e 3 del Codice e dispone le eventuali modifiche ai dati ai sensi dell'art. 4, comma 5. Se la richiesta è rivolta al gestore, quest'ultimo provvede anch'esso direttamente nei medesimi termini, consultando ove necessario il partecipante.

5. Qualora sia necessario svolgere ulteriori o particolari verifiche con il partecipante, il gestore informa l'interessato di tale circostanza entro il termine di quindici giorni previsto dal codice ed indica un altro termine per la risposta, che non può essere superiore ad ulteriori quindici giorni. Durante il periodo necessario ad effettuare le ulteriori verifiche con il partecipante, il gestore:

a) nell'arco dei primi quindici giorni, mantiene nel sistema di informazioni creditizie l'indicazione relativa allo svolgimento delle verifiche, tramite specifica codifica o apposito messaggio da apporre in corrispondenza dei dati oggetto delle richieste dell'interessato;

b) negli ulteriori quindici giorni, sospende la visualizzazione nel sistema di informazioni creditizie dei dati oggetto delle verifiche.

6. In caso di richieste di cui al comma 4 riguardanti effettive contestazioni relative ad inadempimenti del venditore/fornitore dei beni o servizi oggetto del contratto sottostante al rapporto di credito, il gestore annota senza ritardo nel sistema di informazioni creditizie, su richiesta dell'interessato, del partecipante o informando quest'ultimo, la notizia relativa all'esistenza di tali contestazioni, tramite l'inserimento di una specifica codifica da apporre in corrispondenza dei dati relativi al rapporto di credito)).

Art. 9.

((Uso di tecniche o sistemi automatizzati di credit scoring))

((1. Nei casi in cui i dati personali contenuti in un sistema di informazioni creditizie siano trattati anche mediante l'impiego di tecniche o sistemi automatizzati di credit scoring, il gestore e i partecipanti assicurano il rispetto dei seguenti principi:

a) le tecniche o i sistemi, messi a disposizione dal gestore o impiegati per conto dei partecipanti, possono essere utilizzati solo per l'istruttoria di una richiesta di credito o per la gestione dei rapporti di credito instaurati;

b) i dati relativi a giudizi, indicatori o punteggi associati ad un interessato sono elaborati e comunicati dal gestore al solo partecipante che ha ricevuto la richiesta di credito dall'interessato o che ha precedentemente comunicato dati riguardanti il relativo rapporto di credito e, comunque, non sono conservati nel sistema di informazioni creditizie ai sensi dell'art. 6 del presente codice, ne' resi accessibili agli altri partecipanti;

c) i modelli o i fattori di analisi statistica, nonche' gli algoritmi di calcolo dei giudizi, indicatori o punteggi sono verificati periodicamente con cadenza almeno annuale ed aggiornati in funzione delle risultanze di tali verifiche;

d) quando la richiesta di credito non e' accolta, il partecipante comunica all'interessato se, per istruire la richiesta di credito, ha consultato dati relativi a giudizi, indicatori o punteggi di tipo negativo ottenuti mediante l'uso di tecniche o sistemi automatizzati di credit scoring e, su sua richiesta, gli fornisce tali dati, nonche' una spiegazione delle logiche di funzionamento dei sistemi utilizzati e delle principali tipologie di fattori tenuti in considerazione nell'elaborazione)).

Art. 10.

((Trattamento di dati provenienti da fonti pubbliche))

((1. Nei casi in cui il gestore di un sistema di informazioni creditizie, direttamente o per il tramite di societa' collegate o controllate, effettua in ogni forma di dati personali provenienti da

pubblici registri, elenchi, atti o documenti conoscibili da chiunque o comunque fornisce ai partecipanti servizi per accedere ai dati provenienti da tali fonti, fermi restando i limiti e le modalita' che le leggi stabiliscono per la loro conoscibilita' e pubblicita', nonche' le disposizioni di cui all'art. 61, comma 1, del Codice, il gestore e i partecipanti assicurano il rispetto dei seguenti principi:

a) i dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, se registrati, devono figurare in banche di dati personali separate dal sistema di informazioni creditizie e non interconnesse a tale sistema;

b) nel caso di accesso del partecipante a dati personali contenuti sia in un sistema di informazioni creditizie, sia in una delle banche di dati di cui alla lettera a), il gestore adotta le adeguate misure tecniche ed organizzative al fine di assicurare la separazione e la distinguibilita' dei dati provenienti dal sistema di informazioni creditizie rispetto a quelli provenienti da altre banche dati, anche attraverso l'inserimento di idonee indicazioni, eliminando ogni possibilita' di equivoco circa la diversa natura ed origine dei dati oggetto dell'accesso;

c) quando la richiesta di credito non e' accolta, il partecipante comunica all'interessato se, per istruire la richiesta di credito, ha consultato anche dati personali di tipo negativo nelle banche di dati di cui alla lettera a) e, su sua richiesta, specifica la fonte pubblica da cui provengono i dati medesimi).

Art. 11.

((Misure di sicurezza dei dati))

((1. I dati personali oggetto di trattamento nell'ambito di un sistema di informazioni creditizie hanno carattere riservato e non possono essere divulgati a terzi, al di fuori dei casi previsti dal Codice e nei precedenti articoli.

2. Le persone fisiche che, in qualita' di responsabili o di incaricati del trattamento designati dal gestore o dai partecipanti, hanno accesso al sistema di informazioni creditizie, mantengono il segreto sui dati personali acquisiti e rispondono della violazione degli obblighi di riservatezza derivanti da un'utilizzazione dei dati o una divulgazione a terzi per finalita' diverse o incompatibili con le finalita' di cui all'art. 2 del presente codice o comunque non consentite.

3. Il gestore e i partecipanti adottano le misure tecniche, logiche, informatiche, procedurali, fisiche ed organizzative idonee ad assicurare la sicurezza, l'integrita' e la riservatezza dei dati personali e delle comunicazioni elettroniche in conformita' alla disciplina in materia di protezione dei dati personali.

4. Il gestore adotta adeguate misure di sicurezza al fine di

garantire il corretto e regolare funzionamento del sistema di informazioni creditizie, nonché il controllo degli accessi. Questi ultimi sono registrati e memorizzati nel sistema informativo del gestore medesimo o di ogni partecipante presso cui risiede copia della stessa banca dati.

5. In relazione al rispetto degli obblighi di sicurezza, riservatezza e segretezza di cui al presente articolo, il gestore e i partecipanti impartiscono specifiche istruzioni per iscritto ai rispettivi responsabili ed incaricati del trattamento e vigilano sulla loro puntuale osservanza, anche attraverso verifiche da parte di idonei organismi di controllo).

Art. 12.

((Misure sanzionatorie))

((1. Ferme restando le sanzioni amministrative, civili e penali previste dalla normativa vigente, i gestori e i partecipanti prevedono d'intesa tra di loro, anche per il tramite delle associazioni che sottoscrivono il presente codice, idonei meccanismi per l'applicazione, in particolare da parte delle associazioni di categoria che sottoscrivono il presente codice o dell'organismo di cui all'art. 13, comma 7, previa informativa al Garante, di misure sanzionatorie graduate a seconda della gravità della violazione. Le misure comprendono il richiamo formale, la sospensione o la revoca dell'autorizzazione ad accedere al sistema di informazioni creditizie e, nei casi più gravi, anche la pubblicazione della notizia della violazione su uno o più quotidiani o periodici nazionali, a spese del contravventore)).

Art. 13.

((Disposizioni transitorie e finali))

((1. Le misure necessarie per l'applicazione del presente codice di deontologia e di buona condotta sono adottate dai soggetti tenuti a rispettarlo al più tardi entro il 30 aprile 2005.

2. Entro il termine di cui al comma 1, il gestore del sistema centralizzato di rilevazione dei rischi di importo contenuto, istituito con deliberazione Cibr del 3 maggio 1999 (pubblicata nella Gazzetta Ufficiale 8 luglio 1999, n. 158), nonché i relativi partecipanti, adottano le misure necessarie per l'applicazione degli articoli 5 e 8, commi 1, 2, 3, 4 e 5, primo periodo, del presente codice in tema di informativa agli interessati e di esercizio dei diritti, ad integrazione di quanto previsto nel punto 3 delle istruzioni della Banca d'Italia (pubblicate nella Gazzetta Ufficiale 21 novembre 2000, n. 272).

3. I partecipanti forniscono entro i tre mesi successivi al

termine di cui al comma 1, nell'ambito delle comunicazioni periodiche inviate alla clientela, le informazioni di cui all'art. 5, commi 1 e 2, del presente codice eventualmente non comprese nelle informative precedentemente rese agli interessati i cui dati personali risultino già registrati in un sistema di informazioni creditizie.

4. In sede di prima applicazione delle disposizioni di cui all'art. 6, comma 6, i gestori riducono entro il 30 giugno 2005, ad un termine non superiore a trentasei mesi, i tempi di conservazione dei dati personali relativi ad informazioni creditizie di tipo positivo. Entro il 31 dicembre 2005 l'organismo di cui al comma 7 valuta, con atto motivato, se l'esperienza maturata e l'incidenza delle misure previste dal presente codice sui diritti degli interessati, tenuto anche conto dell'efficienza dei sistemi di informazioni creditizie, giustifichino il mantenimento del predetto termine di trentasei mesi. Il medesimo termine si intende mantenuto qualora il Garante, su richiesta del predetto organismo o di propria iniziativa, non disponga diversamente. Entro il 31 gennaio 2006 il Garante dispone la pubblicazione sulla Gazzetta Ufficiale del proprio provvedimento o di un avviso indicante il termine da osservare.

5. Al fine di consentire il controllo sulla corretta attuazione delle disposizioni del presente codice, ogni gestore comunica al Garante, non oltre due mesi dal termine di cui al comma 1 e secondo le modalità indicate da quest'ultimo:

a) oltre ai propri estremi identificativi e recapiti, una descrizione generale delle modalità di funzionamento del sistema di informazioni creditizie e di accesso da parte dei partecipanti, che permetta di valutare l'adeguatezza delle misure, anche tecniche ed organizzative, adottate per l'applicazione del presente codice;

b) in relazione alle parti aventi riflessi in materia di protezione dei dati personali e di applicazione del presente codice, i modelli di contratti, accordi, convenzioni, regolamenti o istruzioni che disciplinano le modalità di partecipazione ed accesso dei partecipanti al sistema di informazioni creditizie, nonché la documentazione circa le misure adottate in tema di sicurezza, riservatezza e segretezza dei dati;

c) i documenti di cui agli articoli 3, commi 3 e 4, 5, commi 4 e 5, e di cui al successivo comma 7.

6. Le comunicazioni di cui al comma 5 sono inviate al Garante, anche successivamente al predetto termine, da qualsiasi titolare che, in qualità di gestore di un sistema di informazioni creditizie, intenda procedere ad un trattamento di dati personali soggetto all'ambito di applicazione del presente codice. I gestori trasmettono al Garante eventuali variazioni delle comunicazioni e dei documenti precedentemente inviati, non oltre la fine dell'anno in cui sono avvenute le variazioni.

7. Il gestore effettua verifiche periodiche, con cadenza almeno annuale, sulla liceità e correttezza del trattamento, controllando l'esattezza e completezza dei dati riferiti ad un congruo numero di

richieste/rapporti di credito, estratti a campione. Il controllo e' eseguito da un organismo composto da almeno un rappresentante del gestore, un rappresentante dei partecipanti designato a rotazione e un rappresentante delle associazioni dei consumatori designato dal Consiglio nazionale dei consumatori ed utenti. Il verbale dei controlli e' trasmesso al Garante.

8. Allo scopo di vigilare sulla puntuale osservanza delle disposizioni contenute nel presente codice e fermi restando i poteri previsti dal Codice in materia di accertamenti e controlli, il Garante puo' concordare con il gestore l'esecuzione di altre verifiche periodiche presso i luoghi ove si svolge il trattamento dei dati personali, con eventuali accessi, anche a campione, al sistema di informazioni creditizie. Il Garante puo' eseguire analoghi controlli concordati sugli accessi effettuati da parte dei partecipanti.

9. Le associazioni di categoria che sottoscrivono il presente codice e i gestori avviano forme di collaborazione con le associazioni dei consumatori e con il Garante, al fine di individuare sia soluzioni operative per il rispetto del presente codice, sia sistemi alternativi di risoluzione delle controversie derivanti dall'applicazione del presente codice.

10. Il Garante, anche su richiesta delle associazioni di categoria che sottoscrivono il presente codice, promuove il periodico riesame e l'eventuale adeguamento alla luce del progresso tecnologico, dell'esperienza acquisita nella sua applicazione o di novita' normative)).

Art. 14.

((Entrata in vigore))

((1. Il presente codice si applica a decorrere dal 1° gennaio 2005)).

((CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I SISTEMI INFORMATIVI GESTITI DA SOGGETTI PRIVATI IN TEMA DI CREDITI AL CONSUMO, AFFIDABILITA' E PUNTUALITA' NEI PAGAMENTI (ART. 117 DEL DECRETO LEGISLATIVO N. 196/2003)

Sottoscritto da:

AISReC - Associazione italiana delle societa' di referenza creditizia;

ABI - Associazione bancaria italiana;

FEDERCASSE - Federazione italiana delle banche di credito cooperativo;

ASSOFIN - Associazione italiana del credito al consumo e

immobiliare;

ASSILEA - Associazione italiana leasing;

CTC - Consorzio per la tutela del credito;

ADICONSUM - Associazione difesa consumatori e ambiente;

ADOC - Associazione per la difesa e l'orientamento dei consumatori;

ADUSBEF - Associazione difesa utenti servizi bancari finanziari assicurativi e postali;

CODACONS - Coordinamento delle associazioni per la difesa dell'ambiente e la tutela dei diritti di utenti e di consumatori;

FEDERCONSUMATORI - Federazione nazionale consumatori e utenti.

[Parte di provvedimento in formato grafico\)\)](#)

ALLEGATO A.6

REGOLE DEONTOLOGICHE RELATIVE AI TRATTAMENTI DI DATI PERSONALI EFFETTUATI PER SVOLGERE INVESTIGAZIONI DIFENSIVE O PER FARE VALERE O DIFENDERE UN DIRITTO IN SEDE

GIUDIZIARIA

CAPO I

PRINCIPI GENERALI

(Delibera del Garante n. 512 del 19 dicembre 2018, in G.U. 15 gennaio 2019, n. 12)

((IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il [regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati che abroga la [direttiva 95/46/CE](#) (di

seguito, «Regolamento»);

Visto il [Codice in materia di protezione dei dati personali](#), recante disposizioni per l'adeguamento dell'ordinamento nazionale al [regolamento \(UE\) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016](#), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la [direttiva 95/46/CE \(decreto legislativo 30 giugno 2003, n. 196](#), come modificato dal [decreto legislativo 10 agosto 2018, n. 101](#), di seguito «Codice»);

Visto l'[art. 20, comma 4, del decreto legislativo n. 101/2018](#) che demanda al Garante il compito di effettuare, nel termine di novanta giorni dall'entrata in vigore del decreto stesso, una verifica della conformità al Regolamento delle disposizioni contenute in alcuni codici deontologici ivi indicati, tra i quali quelle contenute nel «Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive», adottato il 6 novembre 2008, attualmente inserito nel Codice in materia di protezione come allegato A.6 ed applicabile sino al completamento della menzionata procedura;

Rilevato che, sempre secondo quanto previsto dal citato [art. 20, comma 4, del decreto legislativo n. 101/2018](#), al termine della suddetta procedura di verifica, le «disposizioni ritenute compatibili, ridenominate regole deontologiche, sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono successivamente riportate nell'allegato A del Codice»;

Ritenuto che la valutazione di compatibilità di dette disposizioni con il regolamento non possa prescindere da una loro lettura che tenga integralmente conto del mutato quadro normativo di riferimento;

Ritenuto, per tale ragione, che:

i richiami al [decreto legislativo n. 196/2003](#) contenuti in alcune disposizioni del codice deontologico, nonché la terminologia utilizzata, sono stati opportunamente aggiornati ai sensi delle corrispondenti disposizioni del Regolamento e del medesimo [decreto legislativo n. 196/2003](#), come modificato dal [decreto legislativo n. 101/2018](#);

e' opportuno espungere il preambolo del codice di deontologia, dovendosi, in base al richiamato [art. 20 del decreto legislativo 101/2018](#), ridenominare solo le disposizioni dello stesso; il preambolo, invece, nel sintetizzare le condizioni di liceità del trattamento, evidenziava, altresì, i presupposti della sottoscrizione del codice di deontologia, nel rispetto del principio di rappresentatività, che, comunque, rimane alla base delle presenti regole;

e' stata eliminata la previsione riguardante il monitoraggio periodico del codice di deontologia e di buona condotta;

Ritenuto che tali elementi, relativi all'aggiornamento della disciplina in materia, debbano essere recepiti nelle «Regole

deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive» in ragione di quanto disposto dall'[art. 20, comma 4, del decreto legislativo n. 101/2018](#);

Ritenuto, all'esito della verifica della conformita' al regolamento delle disposizioni previste nel «Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria», che le medesime, riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante, debbano essere pubblicate ai sensi dell'[art. 20, comma 4, del decreto legislativo n. 101/2018](#) come «Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria»;

Considerato che le predette «Regole deontologiche» sono volte a disciplinare i trattamenti in questione in attesa di un auspicabile aggiornamento delle stesse ai sensi degli articoli 2-quater del Codice;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

Relatore il dott. Antonello Soro;

Tutto cio' premesso il Garante:

Ai sensi dell'[art. 20, comma 4, del decreto legislativo n. 101/2018](#), verificata la conformita' al regolamento delle disposizioni del «Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria», dispone che le medesime, riportate nell'allegato 1 al presente provvedimento e che ne forma parte integrante, siano pubblicate come «relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria» e ne dispone, altresì, la trasmissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'Allegato A) al Codice.

Roma, 19 dicembre 2018

Il presidente: Soro

Il relatore: Soro

Il segretario generale: Busia

Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria))

Art. 1.

((Ambito di applicazione))

((1. Le presenti regole deontologiche devono essere rispettate nel trattamento di dati personali per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria, sia nel corso di un procedimento, anche in sede amministrativa, di arbitrato o di conciliazione, sia nella fase propedeutica all'instaurazione di un eventuale giudizio, sia nella fase successiva alla sua definizione, da parte di:

a) avvocati o praticanti avvocati iscritti ad albi territoriali o ai relativi registri, sezioni ed elenchi, i quali esercitano l'attività in forma individuale, associata o societaria svolgendo, anche su mandato, un'attività in sede giurisdizionale o di consulenza o di assistenza stragiudiziale, anche avvalendosi di collaboratori, dipendenti o ausiliari, nonché da avvocati stranieri esercenti legalmente la professione sul territorio dello Stato;

b) soggetti che, sulla base di uno specifico incarico anche da parte di un difensore, svolgano in conformità alla legge attività di investigazione privata ([art. 134 regio decreto 18 giugno 1931, n. 773](#); art. 222 norme di coordinamento del [c.p.p.](#)).

2. Le presenti regole deontologiche si applicano, altresì, a chiunque tratti dati personali per le finalità di cui al comma 1, in particolare a altri liberi professionisti o soggetti che in conformità alla legge prestino, su mandato, attività di assistenza o consulenza per le medesime finalità)).

CAPO II

TRATTAMENTI DA PARTE DI AVVOCATI

Art. 2.

((Modalita' di trattamento))

((1. L'avvocato organizza il trattamento anche non automatizzato dei dati personali secondo le modalita' che risultino piu' adeguate, caso per caso, a favorire in concreto l'effettivo rispetto dei diritti, delle liberta' e della dignita' degli interessati, applicando i principi di finalita', proporzionalita' e minimizzazione dei dati sulla base di un'attenta valutazione sostanziale e non formalistica delle garanzie previste, nonche' di un'analisi della quantita' e qualita' delle informazioni che utilizza e dei possibili rischi.

2. Le decisioni relativamente a quanto previsto dal comma 1 sono adottate dal titolare del trattamento il quale resta individuato, a seconda dei casi, in:

a) un singolo professionista;

b) una pluralita' di professionisti, codifensori della medesima parte assistita o che, anche al di fuori del mandato di difesa, siano stati comunque interessati a concorrere all'opera professionale quali consulenti o domiciliatari;

c) un'associazione tra professionisti o una societa' di professionisti.

3. Nel quadro delle adeguate istruzioni da impartire per iscritto alle persone autorizzate ad al trattamento dei dati, sono formulate concrete indicazioni in ordine alle modalita' che tali soggetti devono osservare, a seconda del loro ruolo di sostituto processuale, di praticante avvocato con o senza abilitazione al patrocinio, di consulente tecnico di parte, perito, investigatore privato o altro ausiliario che non rivesta la qualita' di autonomo titolare del trattamento, nonche' di tirocinante, stagista o di persona addetta a compiti di collaborazione amministrativa.

4. Specifica attenzione e' prestata all'adozione di idonee cautele per prevenire l'ingiustificata raccolta, utilizzazione o conoscenza di dati in caso di:

a) acquisizione anche informale di notizie, dati e documenti connotati da un alto grado di confidenzialita' o che possono comportare, comunque, rischi specifici per gli interessati;

b) scambio di corrispondenza, specie per via telematica;

c) esercizio contiguo di attivita' autonome all'interno di uno studio;

d) utilizzo di dati di cui e' dubbio l'impiego lecito, anche per effetto del ricorso a tecniche invasive;

e) utilizzo e distruzione di dati riportati su particolari dispositivi o supporti, specie elettronici (ivi comprese registrazioni audio/video), o documenti (tabulati di flussi telefonici e informatici, consulenze tecniche e perizie, relazioni redatte da investigatori privati);

f) custodia di materiale documentato, ma non utilizzato in un procedimento e ricerche su banche dati a uso interno, specie se

consultabili anche telematicamente da uffici dello stesso titolare del trattamento situati altrove;

g) acquisizione di dati e documenti da terzi, verificando che si abbia titolo per ottenerli;

h) conservazione di atti relativi ad affari definiti.

5. Se i dati sono trattati per esercitare il diritto di difesa in sede giurisdizionale, cio' puo' avvenire anche prima della pendenza di un procedimento, sempreche' i dati medesimi risultino strettamente funzionali all'esercizio del diritto di difesa, in conformita' ai principi di liceita', proporzionalita' e minimizzazione dei dati rispetto alle finalita' difensive ([art. 5 del regolamento UE 2016/679](#)).

6. Sono utilizzati lecitamente e secondo correttezza secondo i medesimi principi di cui all'[art. 5 del regolamento \(UE\) 2016/679](#):

a) i dati personali contenuti in pubblici registri, elenchi, albi, atti o documenti conoscibili da chiunque, nonche' in banche di dati, archivi ed elenchi, ivi compresi gli atti dello stato civile, dai quali possono essere estratte lecitamente informazioni personali riportate in certificazioni e attestazioni utilizzabili a fini difensivi;

b) atti, annotazioni, dichiarazioni e informazioni acquisite nell'ambito di indagini difensive, in particolare ai sensi degli [articoli 391-bis, 391-ter e 391-quater del codice di procedura penale](#), evitando l'ingiustificato rilascio di copie eventualmente richieste. Se per effetto di un conferimento accidentale, anche in sede di acquisizione di dichiarazioni e informazioni ai sensi dei medesimi articoli 391-bis, 391-ter e 391-quater, sono raccolti dati eccedenti e non pertinenti rispetto alle finalita' difensive, tali dati, qualora non possano essere estrapolati o distrutti, formano un unico contesto, unitariamente agli altri dati raccolti).

Art. 3.

((Informativa unica))

((1. L'avvocato puo' fornire in un unico contesto, anche mediante affissione nei locali dello Studio e, se ne dispone, pubblicazione sul proprio sito Internet, anche utilizzando formule sintetiche e colloquiali, l'informativa sul trattamento dei dati personali (art. 13 del Regolamento) e le notizie che deve indicare ai sensi della disciplina sulle indagini difensive)).

Art. 4.

((Conservazione e cancellazione dei dati))

((1. Fermo restando quanto previsto dall'[art. 5, par. 1, lettera e\), del regolamento \(UE\) 2016/679](#), la definizione di un grado di

giudizio o la cessazione dello svolgimento di un incarico non comportano un'automatica dismissione dei dati. Una volta estinto il procedimento o il relativo rapporto di mandato, atti e documenti attinenti all'oggetto della difesa o delle investigazioni difensive possono essere conservati, in originale o in copia e anche in formato elettronico, qualora risulti necessario in relazione a ipotizzabili altre esigenze difensive della parte assistita o del titolare del trattamento, ferma restando la loro utilizzazione in forma anonima per finalita' scientifiche. La valutazione e' effettuata tenendo conto della tipologia dei dati. Se e' prevista una conservazione per adempiere a un obbligo normativo, anche in materia fiscale e di contrasto della criminalita', sono custoditi i soli dati personali effettivamente necessari per adempiere al medesimo obbligo.

2. Fermo restando quanto previsto dal codice deontologico forense in ordine alla restituzione al cliente dell'originale degli atti da questi ricevuti, e salvo quanto diversamente stabilito dalla legge, e' consentito, previa comunicazione alla parte assistita, distruggere, cancellare o consegnare all'avente diritto o ai suoi eredi o aventi causa la documentazione integrale dei fascicoli degli affari trattati e le relative copie.

3. In caso di revoca o di rinuncia al mandato fiduciario o del patrocinio, la documentazione acquisita e' rimessa, in originale ove detenuta in tale forma, al difensore che subentra formalmente nella difesa.

4. La titolarita' del trattamento non cessa per il solo fatto della sospensione o cessazione dell'esercizio della professione. In caso di cessazione anche per sopravvenuta incapacita' e qualora manchi un altro difensore anche succeduto nella difesa o nella cura dell'affare, la documentazione dei fascicoli degli affari trattati, decorso un congruo termine dalla comunicazione all'assistito, e' consegnata al Consiglio dell'ordine di appartenenza ai fini della conservazione per finalita' difensive)).

Art. 5.

((Comunicazione e diffusione di dati))

((1. Nei rapporti con i terzi e con la stampa possono essere rilasciate informazioni non coperte da segreto qualora sia necessario per finalita' di tutela dell'assistito, ancorche' non concordato con l'assistito medesimo, nel rispetto dei principi di liceita', trasparenza, correttezza, e minimizzazione dei dati di cui al [Regolamento \(UE\) 2016/679 \(art. 5\)](#), nonche' dei diritti e della dignita' dell'interessato e di terzi, di eventuali divieti di legge e del codice deontologico forense)).

Art. 6.

((Accertamenti riguardanti documentazione detenuta dal difensore))

((1. In occasione di accertamenti ispettivi che lo riguardano l'avvocato ha diritto ai sensi dell'[art. 159, comma 3, del decreto legislativo n. 196/2003](#) che vi assista il presidente del competente Consiglio dell'ordine forense o un consigliere da questo delegato. Allo stesso, se interviene e ne fa richiesta, e' consegnata copia del provvedimento.

2. In sede di istanza di accesso o richiesta di comunicazione dei dati di traffico relativi a comunicazioni telefoniche in entrata, si applica quanto previsto dall'[art. 132, comma 3, del decreto legislativo n. 196/2003](#))).

CAPO III

TRATTAMENTI DA PARTE DI ALTRI LIBERI PROFESSIONISTI E ULTERIORI SOGGETTI

Art. 7.

((Applicazione di disposizioni riguardanti gli avvocati))

((1. Le disposizioni di cui agli articoli 2 e 5 si applicano, salvo quanto applicabile per legge unicamente all'avvocato:

a) a liberi professionisti che prestino o su mandato dell'avvocato o unitamente a esso o, comunque, nei casi e nella misura consentita dalla legge, attivita' di consulenza e assistenza per far valere o difendere un diritto in sede giudiziaria o per lo svolgimento delle investigazioni difensive;

b) agli altri soggetti, di cui all'art. 1, comma 2, salvo quanto risulti obiettivamente incompatibile in relazione alla figura soggettiva o alla funzione svolta)).

CAPO IV

TRATTAMENTI DA PARTE DI INVESTIGATORI PRIVATI

Art. 8.

((Modalita' di trattamento))

((1. L'investigatore privato organizza il trattamento anche non automatizzato dei dati personali secondo le modalita' di cui all'art. 2, comma 1.

2. L'investigatore privato non puo' intraprendere di propria iniziativa investigazioni, ricerche o altre forme di raccolta dei dati. Tali attivita' possono essere eseguite esclusivamente sulla base di apposito incarico conferito per iscritto e solo per le finalita' di cui alle presenti regole.

3. L'atto d'incarico deve menzionare in maniera specifica il diritto che si intende esercitare in sede giudiziaria, ovvero il procedimento penale al quale l'investigazione e' collegata, nonche' i principali elementi di fatto che giustificano l'investigazione e il termine ragionevole entro cui questa deve essere conclusa.

4. L'investigatore privato deve eseguire personalmente l'incarico ricevuto e puo' avvalersi solo di altri investigatori privati indicati nominativamente all'atto del conferimento dell'incarico, oppure successivamente in calce a esso qualora tale possibilita' sia stata prevista nell'atto di incarico. Restano ferme le prescrizioni predisposte ai sensi dell'[art. 2-septies del decreto legislativo n. 196/2003](#) e [art. 21 del decreto legislativo n. 101/2018](#) relative al trattamento delle particolari categorie di dati personali di cui all'[art. 9, par. 1, del Regolamento \(UE\) 2016/679](#).

5. Nel caso in cui si avvalga di persone autorizzate al trattamento dei dati per suo conto, l'investigatore privato rende specifiche istruzioni in ordine alle modalita' da osservare e vigila, con cadenza almeno settimanale, sulla puntuale osservanza delle norme di legge e delle istruzioni impartite. Tali soggetti possono avere accesso ai soli dati strettamente pertinenti alla collaborazione a essi richiesta.

6. Il difensore o il soggetto che ha conferito l'incarico devono essere informati periodicamente dell'andamento dell'investigazione, anche al fine di permettere loro una valutazione tempestiva circa le determinazioni da adottare riguardo all'esercizio del diritto in sede giudiziaria o al diritto alla prova)).

Art. 9.

((Altre regole di comportamento))

((1. L'investigatore privato si astiene dal porre in essere prassi elusive di obblighi e di limiti di legge e, in particolare, conforma ai principi di liceità, trasparenza e correttezza del trattamento sanciti dal [Regolamento \(UE\) 2016/679](#) e dal [decreto legislativo n. 196/2003](#):

a) l'acquisizione di dati personali presso altri titolari del trattamento, anche mediante mera consultazione, verificando che si abbia titolo per ottenerli;

b) il ricorso ad attività lecite di rilevamento, specie a distanza, e di audio/videoripresa;

c) la raccolta di dati biometrici.

2. L'investigatore privato rispetta nel trattamento dei dati le disposizioni di cui all'art. 2, commi 4, 5 e 6 delle presenti regole)).

Art. 10.

((Conservazione e cancellazione dei dati))

((1. Nel rispetto dell'[art. 5 del regolamento \(UE\) 2016/679](#), i dati personali trattati dall'investigatore privato possono essere conservati per un periodo non superiore a quello strettamente necessario per eseguire l'incarico ricevuto. A tal fine deve essere verificata costantemente, anche mediante controlli periodici, la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto alle finalità perseguite e all'incarico conferito.

2. Una volta conclusa la specifica attività investigativa, il trattamento deve cessare in ogni sua forma, fatta eccezione per l'immediata comunicazione al difensore o al soggetto che ha conferito l'incarico, i quali possono consentire, anche in sede di mandato, l'eventuale conservazione temporanea di materiale strettamente personale dei soggetti che hanno curato l'attività svolta, a i soli fini dell'eventuale dimostrazione della liceità, trasparenza e correttezza del proprio operato. Se è stato contestato il trattamento il difensore o il soggetto che ha conferito l'incarico possono anche fornire all'investigatore il materiale necessario per dimostrare la liceità, trasparenza e correttezza del proprio operato, per il tempo a ciò strettamente necessario.

3. La sola pendenza del procedimento al quale l'investigazione è collegata, ovvero il passaggio ad altre fasi di giudizio in attesa della formazione del giudicato, non costituiscono, di per se stessi, una giustificazione valida per la conservazione dei dati da parte dell'investigatore privato)).

Art. 11.

((Informativa))

((1. L'investigatore privato puo' fornire l'informativa in un unico contesto ai sensi dell'art. 3 delle presenti regole, ponendo in particolare evidenza l'identita' e la qualita' professionale dell'investigatore, nonche' la natura facoltativa del conferimento dei dati, fermo restando quanto disposto dall'art. 14 del regolamento, nel caso in cui i dati personali non siano stati ottenuti presso l'interessato)).

Art. 12.

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 26/3/2019, N. 72)))

Art. 13.

((ARTICOLO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 26/3/2019, N. 72)))

Allegato

((ALLEGATO NON PIU' PREVISTO DAL DECRETO 15 MARZO 2019 (IN G.U. 26/3/2019, N. 72)))

((ALLEGATO A.7

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER IL TRATTAMENTO DEI DATI PERSONALI EFFETTUATO A FINI DI INFORMAZIONE COMMERCIALE))

(Provvedimento del Garante n. 479 del 17 settembre 2015, in G.U. 13 ottobre 2015, n. 238)

((IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

Visto il [Codice in materia di protezione dei dati personali](#) ([d.lgs.](#)

30 giugno 2003, n. 196, di seguito "Codice");

Visto l'art. 27 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visti gli artt. 12 e 154, comma 1, lett. e), del Codice, i quali attribuiscono al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto l'art. 118 del Codice con il quale è stato demandato al Garante il compito di promuovere la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale, prevedendo anche, in correlazione con quanto previsto dall'art. 13, comma 5, modalità semplificate per l'informativa all'interessato e idonei meccanismi per favorire la qualità e l'esattezza dei dati raccolti e comunicati;

Visto il regolamento n. 2/2006 recante le procedure per la sottoscrizione dei codici deontologici e di buona condotta, adottato dal Garante il 20 luglio 2006 (G.U. n. 183 dell'8 agosto 2006);

Considerato che il Collegio del Garante in data 19 febbraio 2015, all'esito della complessa attività di stesura dell'articolato, ha analizzato lo schema preliminare del codice di deontologia e di buona condotta predisposto dai partecipanti al tavolo di lavoro, ritenendolo conforme alle leggi ed ai regolamenti anche in relazione a quanto previsto dall'art. 12 del Codice e ha disposto l'avvio della consultazione pubblica su tale testo, pubblicato sul sito internet del Garante;

Rilevato che la consultazione pubblica si è svolta nel periodo compreso tra il 17 marzo ed il 27 aprile u.s.;

Visto il verbale dell'incontro tenutosi il 9 giugno 2015 presso gli uffici del Garante nel corso del quale i soggetti rappresentativi, esaminate le osservazioni ricevute nel corso della consultazione pubblica, hanno definito lo schema finale del codice di deontologia e di buona condotta rimettendolo al Garante per il prosieguo dell'iter di adozione;

Visto il provvedimento n. 434 del 23 luglio 2015 con il quale il Garante, nell'esaminare lo schema finale del Codice, lo ha ritenuto conforme alle norme di legge e di regolamento, invitando i soggetti rappresentativi e quelli interessati a sottoscriverlo;

Visto il verbale redatto il 3 settembre 2015 dal quale risulta che in tale data il testo del Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale (riportato in allegato alla presente deliberazione) e' stato sottoscritto, in qualita' di soggetti rappresentativi, da ANCIC (Associazione nazionale tra le imprese di informazione commerciale e di gestione del Credito), FEDERPOL (Federazione italiana degli istituti privati per le investigazioni, per le informazioni e per la sicurezza) ed ABI (Associazione bancaria italiana), nonche', in qualita' di soggetti interessati che hanno manifestato la loro adesione ai principi del Codice, da CONFCOMMERCIO (Confederazione Generale Italiana delle Imprese, delle Attivita' Professionali e del Lavoro Autonomo) CONFESERCENTI (Confederazione degli Esercenti attivita' Commerciali e Turistiche), CODACONS (Coordinamento delle Associazioni per la Difesa dell'Ambiente e dei Diritti degli Utenti e dei Consumatori), ASSOUTENTI (Associazione nazionale a difesa dei consumatori nei confronti di burocrazia, commercio, assicurazioni, banche e telecomunicazioni), ADICONSUM (Associazione italiana difesa consumatori e ambiente);

Rilevato che le sottoscrizioni e le adesioni fino ad oggi manifestate rappresentano un adeguato spettro delle realta' che trattano professionalmente informazioni commerciali, che le utilizzano nello svolgimento della propria attivita' economica e professionale nonche' della platea degli interessati i cui dati sono oggetto di trattamento da parte dei c.d. "informatori commerciali";

Considerato che, in conformita' all'art. 8, comma 3, del citato [reg. 2/2006](#), il Garante esaminerà le eventuali richieste di altri soggetti rappresentativi o interessati volte ad apporre le sottoscrizioni o le adesioni in epoca successiva all'adozione del codice di deontologia e buona condotta;

Rilevato che il rispetto delle disposizioni contenute nel codice di deontologia e di buona condotta costituisce condizione essenziale per la liceita' e la correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici (art. 12, comma 3, del Codice);

Considerato che, ai sensi dell'art. 12, comma 2, del Codice e dell'art. 9 del menzionato [regolamento n. 2/2006](#), il codice di deontologia e di buona condotta deve essere pubblicato a cura del Garante nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, riportato nell'Allegato A) al medesimo Codice;

Vista la documentazione in atti;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'[art. 15 del regolamento n. 1/2000](#);

Relatore la dott.ssa Augusta Iannini;

Tutto cio' premesso il Garante:

preso atto della conclusione dell'iter procedurale di redazione e sottoscrizione del codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale, che figura in allegato, quale parte integrante della presente deliberazione, ai sensi dell'[art. 9 del regolamento n. 2/2006](#), ne dispone la trasmissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana, nonche' al Ministero della giustizia per essere riportato nell'Allegato A) al Codice.

Roma, 17 settembre 2015

Il presidente: Soro

Il relatore: Iannini

Il segretario generale: Busia

Allegato

Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale

PREAMBOLO

I sotto indicati soggetti privati sottoscrivono il presente Codice deontologico, adottato sulla base di quanto previsto dall'[art. 118 del decreto legislativo 30 giugno 2003, n. 196](#), e successive modificazioni ed integrazioni, recante il [Codice in materia di protezione dei dati personali](#) (di seguito denominato "Codice"), sulla base delle seguenti premesse:

1) i soggetti operanti nel settore relativo alle attivita' di informazione commerciale si impegnano al rispetto dei diritti, delle liberta' fondamentali e della dignita' delle persone interessate, in particolare del diritto alla protezione dei dati personali, del diritto alla riservatezza e del diritto all'identita' personale;

2) nel presente Codice deontologico sono individuate le adeguate garanzie e modalita' di trattamento dei dati personali a tutela dei diritti degli interessati da porre in essere nel perseguire le finalita' di informazione commerciale per garantire, da un lato, la certezza e la trasparenza nei rapporti commerciali nonche' l'adeguata conoscenza e circolazione delle informazioni commerciali ed economiche e, dall'altro lato, la qualita', la pertinenza, l'esattezza e l'aggiornamento dei dati personali trattati;

3) le disposizioni del presente Codice deontologico si applicano alle sole informazioni commerciali riferite a persone fisiche (rientranti nel concetto di interessato di cui all'art. 4, comma 1, lettera i), del Codice) ed, in particolare, al trattamento dei dati personali provenienti da pubblici registri, elenchi, atti o documenti

conoscibili da chiunque o pubblicamente accessibili da chiunque (c.d. fonti pubbliche), nonche' al trattamento avente ad oggetto i dati personali forniti direttamente dagli interessati, effettuato dai soggetti che prestano a terzi servizi, per finalita' di informazione commerciale, nel rispetto dei limiti e delle modalita' che le normative vigenti stabiliscono per la conoscibilita', utilizzabilita' e pubblicita' di tali dati; e' escluso dall'ambito di applicazione del presente Codice deontologico il trattamento avente ad oggetto i dati personali raccolti presso soggetti privati diversi dall'interessato, che rimane disciplinato dalle disposizioni del Codice oltre che da eventuali provvedimenti specifici adottati dal Garante, al fine di disciplinare compiutamente questo particolare tipo di trattamento;

4) non rientra nell'ambito di applicazione del presente Codice deontologico il trattamento dei dati personali effettuato nell'ambito di sistemi informativi creditizi (c.d. SIC). Per il trattamento di tali dati, resta fermo, pertanto, quanto previsto dal relativo Codice deontologico (v. Allegato 5 al Codice);

5) sono destinatari del presente Codice deontologico tutti i soggetti che prestano a terzi servizi di informazione commerciale, ai sensi dell'[art. 134 del R.D. n. 773/1931](#), e successive modificazioni ed integrazioni, recante il [Testo Unico delle Leggi di Pubblica Sicurezza](#) (di seguito indicato come "[T.U.L.P.S.](#)") e relativi Regolamenti di attuazione).

Art. 1.

((Definizioni))

((1. Ai fini del presente Codice deontologico, si applicano le definizioni previste dall'art. 4 del d.lg. 30 giugno 2003, n. 196.

2. Ai medesimi fini, si intende per:

a) "informazione commerciale": il dato relativo ad aspetti patrimoniali, economici, finanziari, creditizi, industriali e produttivi di un soggetto;

b) "attivita' di informazione commerciale": l'attivita' consistente nella fornitura di servizi informativi e/o valutativi che comportano la ricerca, la raccolta, l'elaborazione, l'analisi, anche mediante stime e giudizi, e la comunicazione di informazioni commerciali;

c) "finalita' di informazione commerciale": la finalita' di fornire informazioni ai committenti sulla situazione economica, finanziaria e patrimoniale delle persone fisiche, nonche' sulla solidita', solvibilita' ed affidabilita' delle predette, in relazione ad esigenze connesse all'instaurazione e gestione di rapporti commerciali, anche precontrattuali, di natura economica e finanziaria e alla tutela dei relativi diritti da parte dei committenti;

d) "servizio di informazione commerciale": il servizio

concernente l'esecuzione, per conto dei committenti, di operazioni di raccolta, analisi, valutazione, elaborazione e comunicazione delle informazioni provenienti da fonti pubbliche, da fonti pubblicamente e generalmente accessibili da chiunque o acquisite direttamente dall'interessato, tali da fornire un valore di conoscenza aggiuntiva ai terzi;

e) "committente": il soggetto privato o pubblico che richiede al fornitore il servizio di informazione commerciale;

f) "fornitore": il soggetto privato che fornisce al committente il servizio di informazione commerciale;

g) "soggetto censito": il soggetto cui si riferiscono il servizio di informazione commerciale o il rapporto informativo richiesti dal committente;

h) "rapporto informativo": il documento cartaceo od elettronico (dossier o report) che, ove richiesto, puo' essere elaborato dal fornitore per il committente e che contiene la rappresentazione complessiva, anche in forma unitaria, aggregata o sintetica, delle informazioni commerciali raccolte in relazione al soggetto censito;

i) "elaborazione di informazioni valutative": attivita' volta alla formulazione di un giudizio, espresso anche in termini predittivi o probabilistici ed in forma di indicatori alfanumerici, codici o simboli, sulla solidita', solvibilita' ed affidabilita' del soggetto censito, risultante da un processo statistico o, comunque, da un modello prestabilito, automatizzato e impersonale di elaborazione delle informazioni, oppure emesso sulla base di analisi e valutazioni effettuate da esperti analisti, anche sulla base di una classificazione in categorie o classi predefinite).

Art. 2.

((Individuazione dei requisiti dell'informazione commerciale))

((1. Il trattamento dei dati personali effettuato nello svolgimento dell'attivita' di informazione commerciale si svolge nel rispetto dei principi di cui all'art. 11 del Codice.

2. Il trattamento non puo' riguardare i dati sensibili ed i dati giudiziari, fatto salvo quanto previsto al successivo art. 3, comma 5, per il trattamento dei soli dati giudiziari provenienti da fonti pubbliche o da quelle pubblicamente e generalmente accessibili da chiunque ivi indicate, nel rispetto dei limiti e delle modalita' stabiliti dalla legge in ordine alla loro conoscibilita', utilizzabilita' e pubblicita'.

3. I dati personali raccolti e trattati dal fornitore ai fini dell'erogazione del servizio di informazione commerciale possono riguardare sia l'interessato quale soggetto censito, sia le persone fisiche od altri interessati legati sul piano giuridico e/o economico al soggetto censito, anche se diverso dalla persona fisica (come, ad es., nel caso di una societa').

4. Ai fini del presente Codice deontologico, deve ritenersi che sussista un legame sul piano giuridico e/o economico tra due o piu' persone fisiche e tra un interessato ed un soggetto (es: societa') diverso dalla persona fisica, quando ricorra una o piu' delle seguenti situazioni:

a) partecipazione dell'interessato ad un'impresa o ad una societa' attraverso il possesso o controllo diretto od indiretto di una percentuale di quote o azioni, oppure di diritti di voto, pari o superiore alle soglie individuate al successivo art. 7;

b) esercizio, tramite la carica o qualifica ricoperta dall'interessato, di effettivi poteri di amministrazione, direzione, gestione e controllo di una impresa o societa'.

5. Al successivo art. 7 del presente Codice deontologico sono individuati i limiti, anche temporali, per associare i dati personali relativi al soggetto censito ed a quelli ad esso legati sul piano giuridico e/o economico, nei casi in cui tali dati riguardino eventi negativi quali, ad esempio, fallimenti o procedure concorsuali, ipoteche o pignoramenti, protesti).

Art. 3.

((Fonti di provenienza e modalita' di trattamento delle informazioni commerciali))

((1. Il fornitore raccoglie le informazioni commerciali presso il soggetto censito, presso fonti pubbliche, fonti pubblicamente e generalmente accessibili da chiunque o presso altri soggetti autorizzati dalla legge alla distribuzione e fornitura delle informazioni.

2. Sono fonti utilizzabili dal fornitore:

a) Le fonti pubbliche ossia i pubblici registri, gli elenchi, gli atti o i documenti conoscibili da chiunque in base alla vigente normativa di riferimento, nei limiti e con le modalita' che in essa sono stabiliti per la conoscibilita', l'utilizzabilita' e la pubblicita' dei dati ivi contenuti, tra cui rientrano, in via esemplificativa e non esaustiva:

1) registro delle imprese, bilanci ed elenchi dei soci, visure e/o atti camerali, atti ed eventi relativi a fallimenti o altre procedure concorsuali nonche' il registro informatico dei protesti presso le camere di commercio e la relativa societa' consortile InfoCamere;

2) atti immobiliari, atti pregiudizievoli ed ipocatastali (come, ad es., iscrizioni o cancellazioni di ipoteche, trascrizioni e cancellazioni di pignoramenti, decreti ingiuntivi o atti giudiziari, e relativi annotamenti) conservati nei registri gestiti dall'Agenzia delle Entrate (tra i quali rientrano le ex Conservatorie dei registri immobiliari e l'Ufficio del Catasto), nel Pubblico Registro Automobilistico e presso l'Anagrafe della popolazione residente.

b) Le fonti pubblicamente e generalmente accessibili da chiunque, sono costituite da:

1) quotidiani e testate giornalistiche in formato cartaceo, che risultino regolarmente registrate;

2) elenchi c.d. categorici ed elenchi telefonici;

3) siti Internet appartenenti a:

3.1. soggetti censiti ed altri soggetti a loro connessi ai sensi del successivo art. 7;

3.2. enti pubblici, governativi, territoriali e locali, agenzie pubbliche, nonche' autorita' di vigilanza e controllo, relativamente ad elenchi, registri, atti e documenti ivi diffusi e contenenti informazioni relative allo svolgimento di attivita' economiche;

3.3. associazioni di categoria ed ordini professionali, relativamente ad elenchi od albi di operatori economici e imprenditoriali, diffusi sui propri siti;

3.4. quotidiani e testate giornalistiche on-line nel numero minimo di tre, che confermino le informazioni oggetto di comunicazione e che risultino regolarmente registrati. Sono escluse dal conteggio le testate giornalistiche on-line, per le quali sia gia' stata computata la corrispondente testata cartacea, nonche' gli articoli che rappresentino una mera ripubblicazione dello stesso testo sotto diverse testate;

3.5. servizi on-line di elenchi telefonici e categorici.

3. Il fornitore raccoglie i dati personali provenienti dalle suddette fonti pubbliche o pubblicamente e generalmente accessibili da chiunque anche mediante l'ausilio di strumenti elettronici e per via telematica, in forma sia diretta che mediata, presso soggetti pubblici o presso altri fornitori privati, sulla base di appositi accordi con questi ultimi e, comunque, nel rispetto delle forme e dei limiti stabiliti dalle disposizioni normative che disciplinano la conoscibilita', utilizzabilita' e pubblicita' degli atti e dei dati in essi contenuti.

4. Nell'acquisire e registrare i dati personali provenienti da fonti pubbliche o da fonti pubblicamente e generalmente accessibili da chiunque, il fornitore adotta idonee e preventive misure per assicurare che:

a) l'informazione estratta sia esatta e pertinente rispetto al fine perseguito e i relativi dati personali vengano trattati in conformita' al principio di proporzionalita';

b) sia annotata la specifica fonte di provenienza dei dati;

c) sia effettuato l'aggiornamento dei medesimi dati nei propri rapporti informativi.

5. Ai fini dell'erogazione del servizio di informazione commerciale e' ammesso il trattamento anche di dati giudiziari provenienti dalle fonti pubbliche; per quanto riguarda, invece, le fonti pubblicamente e generalmente accessibili, e' consentito il trattamento dei soli dati giudiziari diffusi negli ultimi sei mesi, a partire dalla data di ricezione della richiesta del servizio da parte

del committente, e senza alcuna possibilita' per il fornitore di apportare modifiche al contenuto di tali informazioni - salvo l'eventuale loro aggiornamento - e di utilizzarle a fini dell'elaborazione di informazioni valutative)).

Art. 4.

((Informativa agli interessati))

((1. Per il trattamento delle informazioni provenienti dalle fonti di cui al precedente art. 3, considerato il rilevante numero di interessati e la peculiare natura delle stesse informazioni, tale da comportare un impiego di mezzi da ritenersi manifestamente sproporzionato rispetto al diritto tutelato, il fornitore rende l'informativa all'interessato, in forma non individuale, attraverso modalita' semplificate rispetto a quelle ordinarie previste dall'art. 13, comma 5), lett. c), del Codice e, in particolare, attraverso un'informativa predisposta in apposite comunicazioni sul portale Internet costituito, anche a tal fine, dai fornitori di informazioni commerciali.

2. L'informativa di cui al precedente comma contiene gli elementi previsti dall'art. 13, comma 1, del Codice, indicati mediante una descrizione sintetica delle principali caratteristiche del trattamento effettuato dai fornitori, autonomi titolari, e deve recare obbligatoriamente:

a) l'indicazione dei responsabili del trattamento, qualora designati, e/o l'elenco degli stessi, anche al fine di ottenere il riscontro in caso di esercizio dei diritti di cui all'art. 7 del Codice (art. 13, comma 1, lett. f), del Codice);

b) l'indicazione dei siti Internet o altre sedi dove sia agevolmente e gratuitamente consultabile la specifica e dettagliata informativa di ciascun fornitore;

c) l'indicazione delle modalita' attraverso le quali e' possibile esercitare i diritti di cui all'art. 7 del Codice.

3. I fornitori aventi un fatturato annuale per servizi di informazione commerciale non superiore a € 300.000,00 (trecentomila), possono rendere l'informativa solo attraverso la relativa comunicazione sul proprio sito Internet)).

Art. 5.

((Presupposti di liceita' del trattamento))

((1. Ai sensi dell'art. 24, comma 1, lett. c) e d), del Codice, il trattamento per finalita' di informazione commerciale di dati personali provenienti dalle fonti di cui al precedente art. 3 non richiede il consenso dell'interessato medesimo)).

Art. 6.

((Comunicazione delle informazioni))

((1. Le informazioni provenienti da fonti pubbliche, di cui al precedente art. 3, e trattate ai fini dell'erogazione dei servizi di informazione commerciale, sono comunicate dal fornitore, anche per via telematica, ai committenti secondo quanto previsto dalla normativa vigente in materia di pubblica sicurezza ([T.U.L.P.S.](#)))).

Art. 7.**((Associazione e utilizzazione delle informazioni commerciali))**

((1. Ai fini dell'erogazione dei servizi di informazione commerciale, qualora le informazioni provenienti da fonti pubbliche siano riferite ad eventi negativi (quali, ad es., fallimenti o procedure concorsuali, pregiudizievoli, ipoteche o pignoramenti, protesti), il fornitore:

a) utilizza le informazioni di cui sopra che riguardano direttamente l'interessato, quale soggetto censito;

b) utilizza - qualora il soggetto censito sia una persona fisica che non svolga o abbia svolto alcuna attivita' d'impresa, non ricopra od abbia ricoperto cariche sociali, o non detenga o abbia detenuto partecipazioni rilevanti in un'impresa o societa' nei termini indicati ai successivi commi - soltanto le informazioni relative a protesti ed atti pregiudizievoli che lo riguardano direttamente, nonche' le informazioni giudiziarie cosi' come indicate e disciplinate dall'art. 3, comma 5;

c) indica, nel contesto del rapporto informativo, la sola circostanza dell'esistenza di altre informazioni e/o rapporti informativi relativi ad ulteriori interessati legati sul piano giuridico e/o economico al soggetto censito, senza che tali informazioni provenienti da fonti pubbliche e riguardanti eventi negativi, possano essere, in alcun modo, direttamente associate all'interessato quale soggetto censito, ne' tanto meno utilizzate per l'elaborazione di informazioni valutative riferite a quest'ultimo, fatto salvo quanto previsto dai successivi commi.

2. Con riferimento a quanto indicato al precedente comma 1, lett. c), viene fatta salva la facolta' per il fornitore qualora il soggetto censito sia una persona fisica, ai fini dell'erogazione dei servizi di informazione commerciale di associare direttamente all'interessato quale soggetto censito ed utilizzare per l'elaborazione di informazioni valutative riferite a quest'ultimo le informazioni provenienti da fonti pubbliche che si riferiscono ad eventi negativi relativi ad imprese o societa' nelle quali lo stesso interessato (soggetto censito) rivesta o abbia rivestito, fino ad un anno prima, le cariche o qualifiche qui sotto indicate:

a) titolare di ditta individuale;

b) socio di societa' semplice e di societa' in nome collettivo;
c) socio accomandatario di societa' in accomandita semplice e socio accomandante con partecipazioni pari o superiori alla soglia del 25% o detentore della quota di maggioranza del capitale sociale, fatte salve, nel caso di societa' in accomandita semplice, le quote di controllo e partecipazioni del 10% in caso di quote paritarie tra i soci;

d) nelle societa' di capitali:

1) socio con partecipazioni pari o superiori alla soglia del 25% o in possesso del pacchetto di maggioranza del capitale sociale, fatte salve le partecipazioni del 10% in caso di quote paritarie tra i soci;

2) presidente o vice presidente del consiglio di amministrazione, consigliere od amministratore delegato, consigliere, amministratore, consigliere od amministratore con deleghe, amministratore unico o socio unico di societa' a responsabilita' limitata e socio unico di societa' per azioni;

3) sindaco, revisore, institore, presidente del patto di sindacato, organi delle procedure concorsuali e soggetti con qualifica di procuratori e direttori, soltanto se il soggetto censito che ricopra tali ultime cariche o qualifiche abbia:

3.1. amministrato l'impresa o la societa':

3.2. avuto fino ad un anno prima partecipazioni pari o superiori alla soglia del 25% o la quota di maggioranza del capitale sociale, fatte salve le quote di controllo e le partecipazioni con quote paritarie, per le quali i soci rilevano tutti, anche al di sotto della soglia predetta, con il limite della soglia minima del 10%.

3. Sempre con riferimento a quanto indicato al precedente comma 1, lett. c), viene inoltre fatta salva la facolta' per il fornitore, qualora il soggetto censito sia un soggetto diverso dalla persona fisica (come nel caso, ad es., di una societa'), ai fini dell'erogazione dei servizi di informazione commerciale, di associare direttamente al soggetto censito ed utilizzare per l'elaborazione di informazioni valutative riferite a quest'ultimo, le informazioni provenienti da fonti pubbliche che si riferiscono ad eventi negativi riguardanti:

a) le persone fisiche che, nell'ambito del soggetto censito, ricoprono le cariche o qualifiche di cui al precedente comma 2, ivi incluse quelle relative ad imprese o societa' connesse a tali persone fisiche secondo quanto previsto al medesimo comma 2;

b) le persone fisiche, che detengano partecipazioni al capitale del soggetto censito nella misura di cui al precedente comma 2, ivi incluse quelle su dati negativi relative ad imprese o societa' connesse a tali persone fisiche secondo quanto previsto al medesimo comma 2.

4. Fatti salvi i termini piu' restrittivi previsti da specifiche norme di legge, le informazioni provenienti da fonti pubbliche ed attinenti ad eventi negativi oggetto di trattamento nei termini di

cui ai precedenti commi 2 e 3, sono conservate dal fornitore, ai fini dell'erogazione dei servizi di informazione commerciale, nel rispetto dei seguenti limiti temporali:

a) le informazioni relative a fallimenti o procedure concorsuali per un periodo di tempo non superiore a 10 anni dalla data di apertura della procedura del fallimento; decorso tale periodo, le predette informazioni potranno essere ulteriormente utilizzate dal fornitore, solo quando risultino presenti altre informazioni relative ad un successivo fallimento o risulti avviata una nuova procedura fallimentare o concorsuale riferita al soggetto censito o ad altro soggetto connesso, nel qual caso, il trattamento puo' protrarsi per un periodo massimo di 10 anni dalle loro rispettive aperture;

b) le informazioni relative ad atti pregiudizievoli ed ipocatastali (ipoteche e pignoramenti) per un periodo di tempo non superiore a 10 anni dalla data della loro trascrizione o iscrizione, salva l'eventuale loro cancellazione prima di tale termine, nel qual caso verra' conservata per un periodo di 2 anni l'annotazione dell'avvenuta cancellazione)).

Art. 8.

((Conservazione delle informazioni))

((1. Fatto salvo quanto stabilito all'art. 7, comma 4, lett. a) e b), i dati personali provenienti dalle fonti di cui all'art. 3 possono essere conservati dal fornitore ai fini dell'erogazione ai committenti dei servizi di informazione commerciale per il periodo di tempo in cui rimangono conoscibili e/o pubblicati nelle fonti pubbliche da cui provengono, in conformita' a quanto previsto dalle rispettive normative di riferimento.

2. Resta fermo l'obbligo del fornitore di adottare idonee misure per garantire l'aggiornamento delle informazioni commerciali erogate rispetto ai dati personali riportati nelle fonti pubbliche da cui sono state raccolte, nei limiti e con le modalita' stabiliti dalle predette normative di riferimento per la conoscibilita', l'utilizzabilita' e la pubblicita' dei dati ivi contenuti e dei relativi aggiornamenti)).

Art. 9.

((Esercizio dei diritti da parte degli interessati))

((1. I fornitori adottano idonee misure organizzative e tecniche atte a garantire un riscontro telematico, tempestivo e completo alle richieste avanzate dagli interessati di esercizio dei diritti previsti dall'art. 7 del Codice.

2. Gli interessati possono esercitare i predetti diritti anche tramite il portale telematico costituito per tali finalita', le cui

regole di gestione ed accesso sono rimesse ad un distinto documento tecnico da adottarsi successivamente alla sottoscrizione del presente Codice.

3. Nella presentazione della richiesta di esercizio dei propri diritti l'interessato indica anche il codice fiscale e/o la partita Iva al fine di agevolare la ricerca dei dati che lo riguardano da parte del fornitore.

4. Il terzo, al quale l'interessato conferisce per iscritto delega o procura, puo' trattare i dati personali acquisiti presso un fornitore esclusivamente per finalita' di tutela dei diritti dell'interessato, con esclusione di ogni altra finalita' perseguite dal terzo medesimo.

5. Restano fermi i limiti previsti dal Codice per l'esercizio da parte dell'interessato dei diritti di rettificazione od integrazione nei confronti di dati personali di tipo valutativo, elaborati dal fornitore).

Art. 10.

((Sicurezza delle informazioni))

((1. I fornitori adottano le misure tecniche, logiche, informatiche, procedurali, fisiche ed organizzative idonee ad assicurare la sicurezza, l'integrita' e la riservatezza delle informazioni commerciali oggetto di trattamento conformemente agli obblighi previsti dagli artt. 31 e ss. del Codice e dell'Allegato "B" al Codice.

2. Ogni fornitore individua gli eventuali responsabili, anche esterni, e gli incaricati autorizzati a trattare le informazioni commerciali, conformemente agli artt. 29 e ss. del Codice)).

Art. 11.

((Verifiche sul rispetto del Codice deontologico))

((1. Le associazioni di categoria dei fornitori che sottoscrivono il presente Codice deontologico, anche attraverso organi a cio' legittimati in base ai rispettivi ordinamenti statutari o comitati appositamente costituiti, promuovono il rispetto da parte dei rispettivi associati delle regole di condotta previste dal presente Codice. A tal fine, esse adottano apposite procedure per:

a) la soluzione di eventuali problemi relativi all'applicazione delle predette regole;

b) la verifica dell'osservanza delle predette regole da parte dei rispettivi associati nei casi di eventuali controversie insorte tra fornitori, committenti e/o interessati.

2. Le stesse associazioni si impegnano inoltre a valutare, anche con le associazioni di categoria ed organismi rappresentativi degli

altri soggetti firmatari del presente Codice, forme o sistemi alternativi di risoluzione di eventuali controversie insorte tra fornitori, committenti e/o interessati, nonché specifiche misure sanzionatorie, secondo i rispettivi ordinamenti statutari, delle eventuali violazioni delle suddette regole da parte degli aderenti alle associazioni di categoria dei fornitori che sottoscrivono il presente Codice deontologico.

3. Ove siano adottate misure sanzionatorie per le violazioni delle regole del presente Codice deontologico, l'associazione od organismo che le applica deve darne tempestiva informativa anche al Garante)).

Art. 12.

((Disposizioni transitorie e finali))

((1. Le misure necessarie per l'applicazione del presente Codice deontologico sono adottate dai soggetti tenuti a rispettarlo entro il termine di cui al successivo articolo 13.

2. Il Garante, anche su richiesta delle associazioni di categoria che sottoscrivono il presente Codice, promuove il riesame e l'eventuale adeguamento del suddetto Codice alla luce di novità normative, del progresso tecnologico o dell'esperienza acquisita nella sua applicazione)).

Art. 13.

((Entrata in vigore))

((Il presente Codice si applica a decorrere dal 1 ottobre 2016)).

Allegato

((Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato ai fini di informazione commerciale [\(art. 118 del d.lgs. 196/2003 - Codice in materia di protezione dei dati personali\)](#)))

Elenco sottoscrittori:

- ANIC (Associazione nazionale tra le imprese di informazioni commerciali e di gestione del credito) -**
- Federpol (Federazione italiana degli istituti privati per le investigazioni, per le informazioni e per la sicurezza)**
- Abi (Associazione bancaria italiana)**
- Confcommercio**
- Confesercenti**
- Codacons (Coordinamento di associazioni per la tutela dell'ambiente e dei diritti di utenti e consumatori)**

- **Assoutenti (Associazione degli utenti dei servizi pubblici)**
- **Adiconsum (Associazione difesa consumatori e ambiente))).**

ALLEGATO B

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

ALLEGATO B

((ALLEGATO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

ALLEGATO C

TRATTAMENTI NON OCCASIONALI EFFETTUATI IN AMBITO GIUDIZIARIO O PER FINI DI POLIZIA

ALLEGATO C)

((ALLEGATO ABROGATO DAL [D.LGS. 10 AGOSTO 2018, N. 101](#)))

I

(Atti legislativi)

REGOLAMENTI

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo ⁽¹⁾,

visto il parere del Comitato delle regioni ⁽²⁾,

deliberando secondo la procedura legislativa ordinaria ⁽³⁾,

considerando quanto segue:

- (1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
- (2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.
- (3) La direttiva 95/46/CE del Parlamento europeo e del Consiglio ⁽⁴⁾ ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

⁽¹⁾ GU C 229 del 31.7.2012, pag. 90.

⁽²⁾ GU C 391 del 18.12.2012, pag. 127.

⁽³⁾ Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura dell'8 aprile 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 14 aprile 2016.

⁽⁴⁾ Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

- (4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va temperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.
- (5) L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro.
- (6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.
- (7) Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.
- (8) Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale.
- (9) Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE.
- (10) Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

- (11) Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri.
- (12) L'articolo 16, paragrafo 2, TFUE conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati.
- (13) Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni. Inoltre, le istituzioni e gli organi dell'Unione e gli Stati membri e le loro autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese nell'applicare il presente regolamento. La nozione di micro, piccola e media impresa dovrebbe ispirarsi all'articolo 2 dell'allegato della raccomandazione 2003/361/CE della Commissione ⁽¹⁾.
- (14) È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.
- (15) Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.
- (16) Il presente regolamento non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale. Il presente regolamento non si applica al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione.
- (17) Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ⁽²⁾ si applica al trattamento di dati personali effettuato da istituzioni, organi, uffici e agenzie dell'Unione. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali dovrebbero essere adeguati ai principi e alle norme stabiliti dal presente regolamento e applicati alla luce dello stesso. Per offrire un quadro di protezione dei dati solido e coerente nell'Unione, si dovrebbe procedere, successivamente all'adozione del presente regolamento, ai necessari adeguamenti del regolamento (CE) n. 45/2001, al fine di consentirne l'applicazione contemporaneamente al presente regolamento.
- (18) Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la

⁽¹⁾ Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (C(2003) 1422) (GU L 124 del 20.5.2003, pag. 36).

⁽²⁾ Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

- (19) La protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati sono oggetto di uno specifico atto dell'Unione. Il presente regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per tali finalità. I dati personali trattati dalle autorità pubbliche in forza del presente regolamento, quando utilizzati per tali finalità, dovrebbero invece essere disciplinati da un più specifico atto dell'Unione, segnatamente la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ⁽¹⁾. Gli Stati membri possono conferire alle autorità competenti ai sensi della direttiva (UE) 2016/680 altri compiti che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, affinché il trattamento di dati personali per tali altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientri nell'ambito di applicazione del presente regolamento.

Con riguardo al trattamento dei dati personali da parte di tali autorità competenti per finalità rientranti nell'ambito di applicazione del presente regolamento, gli Stati membri dovrebbero poter mantenere o introdurre disposizioni più specifiche per adattare l'applicazione delle disposizioni del presente regolamento. Tali disposizioni possono determinare con maggiore precisione requisiti specifici per il trattamento di dati personali da parte di dette autorità competenti per tali altre finalità, tenuto conto della struttura costituzionale, organizzativa e amministrativa dei rispettivi Stati membri. Quando il trattamento dei dati personali effettuato da organismi privati rientra nell'ambito di applicazione del presente regolamento, è opportuno che lo stesso preveda la facoltà per gli Stati membri, a determinate condizioni, di adottare disposizioni legislative intese a limitare determinati obblighi e diritti, qualora tale limitazione costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia di importanti interessi specifici, comprese la sicurezza pubblica e le attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica. Ciò riveste particolare importanza ad esempio nel quadro del riciclaggio o di attività di medicina legale.

- (20) Sebbene il presente regolamento si applichi, tra l'altro, anche alle attività delle autorità giurisdizionali e di altre autorità giudiziarie, il diritto dell'Unione o degli Stati membri potrebbe specificare le operazioni e le procedure di trattamento relativamente al trattamento dei dati personali effettuato da autorità giurisdizionali e da altre autorità giudiziarie. Non è opportuno che rientri nella competenza delle autorità di controllo il trattamento di dati personali effettuato dalle autorità giurisdizionali nell'adempimento delle loro funzioni giurisdizionali, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento dei suoi compiti giurisdizionali, compreso il processo decisionale. Si dovrebbe poter affidare il controllo su tali trattamenti di dati ad organismi specifici all'interno del sistema giudiziario dello Stato membro, che dovrebbero in particolare assicurare la conformità alle norme del presente regolamento, rafforzare la consapevolezza della magistratura con riguardo agli obblighi che alla stessa derivano dal presente regolamento ed esaminare i reclami in relazione a tali operazioni di trattamento dei dati.
- (21) Il presente regolamento non pregiudica l'applicazione della direttiva 2000/31/CE del Parlamento europeo e del Consiglio ⁽²⁾, in particolare delle norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva. Detta direttiva mira a contribuire al buon funzionamento del mercato interno garantendo la libera circolazione dei servizi della società dell'informazione tra Stati membri.
- (22) Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o responsabile del trattamento nel territorio dell'Unione dovrebbe essere conforme al presente regolamento, indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica.

⁽¹⁾ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Cfr. pagina 89 della presente Gazzetta ufficiale).

⁽²⁾ Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico») (GUL 178 del 17.7.2000, pag. 1).

- (23) Onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al presente regolamento, è opportuno che questo disciplini il trattamento dei dati personali degli interessati che si trovano nell'Unione effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono connesse all'offerta di beni o servizi a detti interessati indipendentemente dal fatto che vi sia un pagamento correlato. Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione.
- (24) È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al monitoraggio del comportamento di detti interessati, nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.
- (25) Laddove vige il diritto di uno Stato membro in virtù del diritto internazionale pubblico, ad esempio nella rappresentanza diplomatica o consolare di uno Stato membro, il presente regolamento dovrebbe applicarsi anche a un titolare del trattamento non stabilito nell'Unione.
- (26) È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.
- (27) Il presente regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute.
- (28) L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati.
- (29) Al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all'interno dello stesso titolare del trattamento.

- (30) Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle.
- (31) Le autorità pubbliche a cui i dati personali sono comunicati conformemente a un obbligo legale ai fini dell'esercizio della loro missione istituzionale, quali autorità fiscali e doganali, unità di indagine finanziaria, autorità amministrative indipendenti o autorità dei mercati finanziari, responsabili della regolamentazione e della vigilanza dei mercati dei valori mobiliari, non dovrebbero essere considerate destinatari qualora ricevano dati personali che sono necessari per svolgere una specifica indagine nell'interesse generale, conformemente al diritto dell'Unione o degli Stati membri. Le richieste di comunicazione inviate dalle autorità pubbliche dovrebbero sempre essere scritte, motivate e occasionali e non dovrebbero riguardare un intero archivio o condurre all'interconnessione di archivi. Il trattamento di tali dati personali da parte delle autorità pubbliche dovrebbe essere conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento.
- (32) Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.
- (33) In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista.
- (34) È opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti.
- (35) Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio ⁽¹⁾; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.
- (36) Lo stabilimento principale di un titolare del trattamento nell'Unione dovrebbe essere il luogo in cui ha sede la sua amministrazione centrale nell'Unione, a meno che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione, nel qual caso tale altro stabilimento dovrebbe essere considerato lo stabilimento principale. Lo stabilimento principale di un titolare del

⁽¹⁾ Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

trattamento nell'Unione dovrebbe essere determinato in base a criteri obiettivi e implicare l'effettivo e reale svolgimento di attività di gestione finalizzate alle principali decisioni sulle finalità e sui mezzi del trattamento nel quadro di un'organizzazione stabile. Tale criterio non dovrebbe dipendere dal fatto che i dati personali siano trattati in quella sede. La presenza o l'uso di mezzi tecnici e tecnologie di trattamento di dati personali o di attività di trattamento non costituiscono di per sé lo stabilimento principale né sono quindi criteri determinanti della sua esistenza. Per quanto riguarda il responsabile del trattamento, per «stabilimento principale» dovrebbe intendersi il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se non dispone di un'amministrazione centrale nell'Unione, il luogo in cui sono condotte le principali attività di trattamento nell'Unione. In caso di coinvolgimento sia del titolare del trattamento sia del responsabile del trattamento, l'autorità di controllo competente capofila dovrebbe continuare a essere l'autorità di controllo dello Stato membro in cui il titolare del trattamento ha lo stabilimento principale, ma l'autorità di controllo del responsabile del trattamento dovrebbe essere considerata autorità di controllo interessata e tale autorità di controllo dovrebbe partecipare alla procedura di cooperazione prevista dal presente regolamento. In ogni caso, le autorità di controllo dello Stato membro o degli Stati membri in cui il responsabile del trattamento ha uno o più stabilimenti non dovrebbero essere considerate autorità di controllo interessate quando il progetto di decisione riguarda soltanto il titolare del trattamento. Se il trattamento è effettuato da un gruppo imprenditoriale, lo stabilimento principale dell'impresa controllante dovrebbe essere considerato lo stabilimento principale del gruppo di imprese, tranne nei casi in cui le finalità e i mezzi del trattamento sono stabiliti da un'altra impresa.

- (37) Un gruppo imprenditoriale dovrebbe costituirsi di un'impresa controllante e delle sue controllate, là dove l'impresa controllante dovrebbe essere quella che può esercitare un'influenza dominante sulle controllate in forza, ad esempio, della proprietà, della partecipazione finanziaria o delle norme societarie o del potere di fare applicare le norme in materia di protezione dei dati personali. Un'impresa che controlla il trattamento dei dati personali in imprese a essa collegate dovrebbe essere considerata, unitamente a tali imprese, quale «gruppo imprenditoriale».
- (38) I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.
- (39) Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.
- (40) Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri, come indicato

nel presente regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.

- (41) Qualora il presente regolamento faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato. Tuttavia, tale base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea (la «Corte di giustizia») e della Corte europea dei diritti dell'uomo.
- (42) Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di esprimere un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio ⁽¹⁾ è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.
- (43) Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.
- (44) Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.
- (45) È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri sia basato sul diritto dell'Unione o di uno Stato membro. Il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo legale cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento. Inoltre, tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale.
- (46) Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato

⁽¹⁾ Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori (GU L 95 del 21.4.1993, pag. 29).

sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

- (47) I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.
- (48) I titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti. Sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in un paese terzo.
- (49) Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi impreveduti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.
- (50) Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali. Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione o degli Stati membri può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in

particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

Ove l'interessato abbia prestato il suo consenso o il trattamento si basi sul diritto dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democratica per salvaguardare, in particolare, importanti obiettivi di interesse pubblico generale, il titolare del trattamento dovrebbe poter sottoporre i dati personali a ulteriore trattamento a prescindere dalla compatibilità delle finalità. In ogni caso, dovrebbe essere garantita l'applicazione dei principi stabiliti dal presente regolamento, in particolare l'obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi. L'indicazione da parte del titolare del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati personali pertinenti a un'autorità competente in singoli casi o in più casi riguardanti lo stesso reato o la stessa minaccia alla sicurezza pubblica dovrebbero essere considerate nell'interesse legittimo perseguito dal titolare del trattamento. Tuttavia, tale trasmissione nell'interesse legittimo del titolare del trattamento o l'ulteriore trattamento dei dati personali dovrebbero essere vietati se il trattamento non è compatibile con un obbligo vincolante di segretezza, di natura giuridica, professionale o di altro genere.

- (51) Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini «origine razziale» nel presente regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte. Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.
- (52) La deroga al divieto di trattare categorie particolari di dati personali dovrebbe essere consentita anche quando è prevista dal diritto dell'Unione o degli Stati membri, fatte salve adeguate garanzie, per proteggere i dati personali e altri diritti fondamentali, laddove ciò avvenga nell'interesse pubblico, in particolare il trattamento dei dati personali nel settore del diritto del lavoro e della protezione sociale, comprese le pensioni, e per finalità di sicurezza sanitaria, controllo e allerta, la prevenzione o il controllo di malattie trasmissibili e altre minacce gravi alla salute. Tale deroga può avere luogo per finalità inerenti alla salute, compresa la sanità pubblica e la gestione dei servizi di assistenza sanitaria, soprattutto al fine di assicurare la qualità e l'economicità delle procedure per soddisfare le richieste di prestazioni e servizi nell'ambito del regime di assicurazione sanitaria, o a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici. La deroga dovrebbe anche consentire di trattare tali dati personali se necessario per accertare, esercitare o difendere un diritto, che sia in sede giudiziale, amministrativa o stragiudiziale.
- (53) Le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o a fini di archiviazione nel

pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica. Pertanto il presente regolamento dovrebbe prevedere condizioni armonizzate per il trattamento di categorie particolari di dati personali relativi alla salute in relazione a esigenze specifiche, in particolare qualora il trattamento di tali dati sia svolto da persone vincolate dal segreto professionale per talune finalità connesse alla salute. Il diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali delle persone fisiche. Gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi.

- (54) Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche. In tale contesto, la nozione di «sanità pubblica» dovrebbe essere interpretata secondo la definizione del regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio⁽¹⁾: tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito.
- (55) Inoltre, è effettuato per motivi di interesse pubblico il trattamento di dati personali a cura di autorità pubbliche allo scopo di realizzare fini, previsti dal diritto costituzionale o dal diritto internazionale pubblico, di associazioni religiose ufficialmente riconosciute.
- (56) Se, nel corso di attività elettorali, il funzionamento del sistema democratico presuppone, in uno Stato membro, che i partiti politici raccolgano dati personali sulle opinioni politiche delle persone, può esserne consentito il trattamento di tali dati per motivi di interesse pubblico, purché siano predisposte garanzie adeguate.
- (57) Se i dati personali che tratta non gli consentono di identificare una persona fisica, il titolare del trattamento non dovrebbe essere obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione del presente regolamento. Tuttavia, il titolare del trattamento non dovrebbe rifiutare le ulteriori informazioni fornite dall'interessato al fine di sostenere l'esercizio dei suoi diritti. L'identificazione dovrebbe includere l'identificazione digitale di un interessato, ad esempio mediante un meccanismo di autenticazione quali le stesse credenziali, utilizzate dall'interessato per l'accesso (log in) al servizio on line offerto dal titolare del trattamento.
- (58) Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.
- (59) È opportuno prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici. Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

⁽¹⁾ Regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativo alle statistiche comunitarie in materia di sanità pubblica e di salute e sicurezza sul luogo di lavoro (GU L 354 del 31.12.2008, pag. 70).

- (60) I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e del contesto specifici in cui i dati personali sono trattati. Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa. In caso di dati personali raccolti direttamente presso l'interessato, questi dovrebbe inoltre essere informato dell'eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli. Tali informazioni possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico.
- (61) L'interessato dovrebbe ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso. Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali. Il titolare del trattamento, qualora intenda trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie. Qualora non sia possibile comunicare all'interessato l'origine dei dati personali, perché sono state utilizzate varie fonti, dovrebbe essere fornita un'informazione di carattere generale.
- (62) Per contro, non è necessario imporre l'obbligo di fornire l'informazione se l'interessato dispone già dell'informazione, se la registrazione o la comunicazione dei dati personali sono previste per legge o se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato. Quest'ultima eventualità potrebbe verificarsi, ad esempio, nei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi si può tener conto del numero di interessati, dell'antichità dei dati e di eventuali garanzie adeguate in essere.
- (63) Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce.
- (64) Il titolare del trattamento dovrebbe adottare tutte le misure ragionevoli per verificare l'identità di un interessato che chieda l'accesso, in particolare nel contesto di servizi online e di identificativi online. Il titolare del trattamento non dovrebbe conservare dati personali al solo scopo di poter rispondere a potenziali richieste.
- (65) Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che la riguardano e il «diritto all'oblio» se la conservazione di tali dati viola il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole

successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

- (66) Per rafforzare il «diritto all'oblio» nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.
- (67) Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.
- (68) Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati. Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente regolamento. Inoltre tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto. Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro.
- (69) Qualora i dati personali possano essere lecitamente trattati, essendo il trattamento necessario per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ovvero per i legittimi interessi di un titolare del trattamento o di terzi, l'interessato dovrebbe comunque avere il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. È opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato.
- (70) Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento, sia con riguardo a quello iniziale o ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto dovrebbe essere esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione.

- (71) L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore.

Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca tra l'altro effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni.

- (72) La profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali le basi giuridiche del trattamento o i principi di protezione dei dati. Il comitato europeo per la protezione dei dati istituito dal presente regolamento («comitato») dovrebbe poter emanare orientamenti in tale contesto.
- (73) Il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti di informazione, accesso, rettifica e cancellazione di dati, al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione, nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento, ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica, ivi comprese la tutela della vita umana, in particolare in risposta a catastrofi di origine naturale o umana, le attività di prevenzione, indagini e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, o di violazioni della deontologia professionale, per la tutela di altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, tra cui un interesse economico o finanziario rilevante dell'Unione o di uno Stato membro, per la tenuta di registri pubblici per ragioni di interesse pubblico generale, per l'ulteriore trattamento di dati personali archiviati al fine di fornire informazioni specifiche connesse al comportamento politico sotto precedenti regimi statali totalitari o per la tutela dell'interessato o dei diritti e delle libertà altrui, compresi la protezione sociale, la sanità pubblica e gli scopi umanitari. Tali limitazioni dovrebbero essere conformi alla Carta e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.
- (74) È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

- (75) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.
- (76) La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.
- (77) Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio.
- (78) La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.
- (79) La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.
- (80) Quando un titolare del trattamento o un responsabile del trattamento non stabilito nell'Unione tratta dati personali di interessati che si trovano nell'Unione e le sue attività di trattamento sono connesse all'offerta di beni o alla prestazione di servizi a tali interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, o al controllo del loro comportamento, nella misura in cui tale comportamento ha luogo all'interno dell'Unione, è opportuno che tale titolare del trattamento o responsabile del trattamento designi un rappresentante, tranne se il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati personali o il trattamento di dati personali relativi alle condanne penali e ai reati, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento, o se il titolare del trattamento è un'autorità

pubblica o un organismo pubblico. Il rappresentante dovrebbe agire per conto del titolare del trattamento o del responsabile del trattamento e può essere interpellato da qualsiasi autorità di controllo. Il rappresentante dovrebbe essere esplicitamente designato mediante mandato scritto del titolare del trattamento o del responsabile del trattamento ad agire per conto di questi ultimi con riguardo agli obblighi che a questi derivano dal presente regolamento. La designazione di tale rappresentante non incide sulla responsabilità generale del titolare del trattamento o del responsabile del trattamento ai sensi del presente regolamento. Tale rappresentante dovrebbe svolgere i suoi compiti nel rispetto del mandato conferitogli dal titolare del trattamento o dal responsabile del trattamento, anche per quanto riguarda la cooperazione con le autorità di controllo competenti per qualsiasi misura adottata al fine di garantire il rispetto del presente regolamento. Il rappresentante designato dovrebbe essere oggetto di misure attuative in caso di inadempienza da parte del titolare del trattamento o del responsabile del trattamento.

- (81) Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento. L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato. Il titolare del trattamento e il responsabile del trattamento possono scegliere di usare un contratto individuale o clausole contrattuali tipo che sono adottate direttamente dalla Commissione oppure da un'autorità di controllo in conformità del meccanismo di coerenza e successivamente dalla Commissione. Dopo il completamento del trattamento per conto del titolare del trattamento, il responsabile del trattamento dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali.
- (82) Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per monitorare detti trattamenti.
- (83) Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.
- (84) Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.
- (85) Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifrazione non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica

interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

- (86) Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.
- (87) È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.
- (88) Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.
- (89) La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.
- (90) In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento.
- (91) Ciò dovrebbe applicarsi in particolare ai trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali

sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza. Una valutazione d'impatto sulla protezione dei dati è altresì richiesta per la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala. Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati.

- (92) Vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata.
- (93) In vista dell'adozione della legge degli Stati membri che disciplina i compiti dell'autorità pubblica o dell'organismo pubblico e lo specifico trattamento o insieme di trattamenti, gli Stati membri possono ritenere necessario effettuare tale valutazione prima di procedere alle attività di trattamento.
- (94) Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il titolare del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno consultare l'autorità di controllo prima dell'inizio delle attività di trattamento. Tale rischio elevato potrebbe scaturire da certi tipi di trattamento e dall'estensione e frequenza del trattamento, da cui potrebbe derivare altresì un danno o un'interferenza con i diritti e le libertà della persona fisica. L'autorità di controllo che riceve una richiesta di consultazione dovrebbe darvi seguito entro un termine determinato. Tuttavia, la mancanza di reazione dell'autorità di controllo entro tale termine dovrebbe far salvo ogni intervento della stessa nell'ambito dei suoi compiti e poteri previsti dal presente regolamento, compreso il potere di vietare i trattamenti. Nell'ambito di tale processo di consultazione, può essere presentato all'autorità di controllo il risultato di una valutazione d'impatto sulla protezione dei dati effettuata riguardo al trattamento in questione, in particolare le misure previste per attenuare il rischio per i diritti e le libertà delle persone fisiche.
- (95) Il responsabile del trattamento, se necessario e su richiesta, dovrebbe assistere il titolare del trattamento nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una valutazione d'impatto sulla protezione dei dati e dalla previa consultazione dell'autorità di controllo.
- (96) L'autorità di controllo dovrebbe essere altresì consultata durante l'elaborazione di una misura legislativa o regolamentare che prevede il trattamento di dati personali al fine di garantire che il trattamento previsto rispetti il presente regolamento e, in particolare, che si attui il rischio per l'interessato.
- (97) Per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere

determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente.

- (98) Le associazioni o altre organizzazioni rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento dovrebbero essere incoraggiate a elaborare codici di condotta, nei limiti del presente regolamento, in modo da facilitarne l'effettiva applicazione, tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese. In particolare, tali codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento e dei responsabili del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche.
- (99) Nell'elaborare un codice di condotta, o nel modificare o prorogare tale codice, le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento dovrebbero consultare le parti interessate pertinenti, compresi, quando possibile, gli interessati, e tener conto delle osservazioni ricevute e delle opinioni espresse in riscontro a tali consultazioni.
- (100) Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi.
- (101) I flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali potrebbero essere effettuati soltanto nel pieno rispetto del presente regolamento. Il trasferimento potrebbe aver luogo soltanto se, fatte salve le altre disposizioni del presente regolamento, il titolare del trattamento o il responsabile del trattamento rispetta le condizioni stabilite dalle disposizioni del presente regolamento in relazione al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.
- (102) Il presente regolamento lascia impregiudicate le disposizioni degli accordi internazionali conclusi tra l'Unione e i paesi terzi che disciplinano il trasferimento di dati personali, comprese adeguate garanzie per gli interessati. Gli Stati membri possono concludere accordi internazionali che implicano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, purché tali accordi non incidano sul presente regolamento o su qualsiasi altra disposizione del diritto dell'Unione e includano un adeguato livello di protezione per i diritti fondamentali degli interessati.
- (103) La Commissione può decidere, con effetto nell'intera Unione, che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale offrono un livello adeguato di protezione dei dati, garantendo in tal modo la certezza del diritto e l'uniformità in tutta l'Unione nei confronti del paese terzo o dell'organizzazione internazionale che si ritiene offra tale livello di protezione. In tali casi, i trasferimenti di dati personali verso tale paese terzo od organizzazione internazionale possono avere luogo senza ulteriori autorizzazioni. La Commissione può inoltre decidere, dopo aver fornito una dichiarazione completa che illustra le motivazioni al paese terzo o all'organizzazione internazionale, di revocare una tale decisione.
- (104) In linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo, è opportuno che la Commissione, nella sua valutazione del paese terzo, o di un territorio o di un settore specifico all'interno di un paese terzo, tenga conto del modo in cui tale paese rispetta lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in materia di diritti dell'uomo, nonché la legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure l'ordine pubblico e il diritto penale. L'adozione di una decisione di adeguatezza nei confronti di un territorio o di un settore specifico all'interno di un paese terzo dovrebbe prendere in considerazione criteri chiari e obiettivi come specifiche attività di trattamento e l'ambito di applicazione delle norme giuridiche e degli atti legislativi applicabili

in vigore nel paese terzo. Il paese terzo dovrebbe offrire garanzie di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione, segnatamente quando i dati personali sono trattati in uno o più settori specifici. In particolare, il paese terzo dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri e agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziale.

- (105) Al di là degli impegni internazionali che il paese terzo o l'organizzazione internazionale hanno assunto, la Commissione dovrebbe tenere in considerazione gli obblighi derivanti dalla partecipazione del paese terzo o dell'organizzazione internazionale a sistemi multilaterali o regionali, soprattutto in relazione alla protezione dei dati personali, nonché all'attuazione di tali obblighi. In particolare si dovrebbe tenere in considerazione l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e relativo protocollo addizionale. La Commissione, nel valutare l'adeguatezza del livello di protezione nei paesi terzi o nelle organizzazioni internazionali, dovrebbe consultare il comitato.
- (106) È opportuno che la Commissione controlli il funzionamento delle decisioni sul livello di protezione in un paese terzo, in un territorio o settore specifico all'interno di un paese terzo, o un'organizzazione internazionale, e monitorare il funzionamento delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, o dell'articolo 26, paragrafo 4, della direttiva 95/46/CE. Nella sua decisione di adeguatezza, la Commissione dovrebbe prevedere un meccanismo di riesame periodico del loro funzionamento. Tale riesame periodico dovrebbe essere effettuato in consultazione con il paese terzo o l'organizzazione internazionale in questione e tenere conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. Ai fini del controllo e dello svolgimento dei riesami periodici, la Commissione dovrebbe tener conto delle posizioni e delle conclusioni del Parlamento europeo e del Consiglio, nonché di altri organismi e fonti pertinenti. La Commissione dovrebbe valutare, entro un termine ragionevole, il funzionamento di tali ultime decisioni e riferire eventuali riscontri pertinenti al comitato ai sensi del regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ⁽¹⁾, come stabilito a norma del presente regolamento, al Parlamento europeo e al Consiglio.
- (107) La Commissione può riconoscere che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello adeguato di protezione dei dati. Di conseguenza il trasferimento di dati personali verso tale paese terzo od organizzazione internazionale dovrebbe essere vietato, a meno che non siano soddisfatti i requisiti di cui al presente regolamento relativamente ai trasferimenti sottoposti a garanzie adeguate, comprese norme vincolanti d'impresa, e a deroghe per situazioni particolari. In tal caso è opportuno prevedere consultazioni tra la Commissione e detti paesi terzi o organizzazioni internazionali. La Commissione dovrebbe informare tempestivamente il paese terzo o l'organizzazione internazionale dei motivi e avviare consultazioni con questi al fine di risolvere la situazione.
- (108) In mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento dovrebbe provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato. Tali adeguate garanzie possono consistere nell'applicazione di norme vincolanti d'impresa, clausole tipo di protezione dei dati adottate dalla Commissione, clausole tipo di protezione dei dati adottate da un'autorità di controllo o clausole contrattuali autorizzate da un'autorità di controllo. Tali garanzie dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi, fra cui il ricorso effettivo in sede amministrativa o giudiziale e la richiesta di risarcimento, nell'Unione o in un paese terzo. Esse dovrebbero riguardare, in particolare, la conformità rispetto ai principi generali in materia di trattamento dei dati personali e ai principi di protezione dei dati fin dalla progettazione e di protezione dei dati di default. I trasferimenti possono essere effettuati anche da autorità pubbliche o organismi pubblici ad autorità pubbliche o organismi pubblici di paesi terzi, o organizzazioni internazionali con analoghi compiti o funzioni, anche sulla base di disposizioni da inserire in accordi amministrativi, quali un memorandum d'intesa, che prevedano per gli interessati diritti effettivi e azionabili. L'autorizzazione dell'autorità di controllo competente dovrebbe essere ottenuta quando le garanzie sono offerte nell'ambito di accordi amministrativi giuridicamente non vincolanti.
- (109) La possibilità che il titolare del trattamento o il responsabile del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo non dovrebbe precludere ai titolari del trattamento o ai responsabili del trattamento la possibilità di includere tali clausole tipo in un contratto più

⁽¹⁾ Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GUL 55 del 28.2.2011, pag. 13).

ampio, anche in un contratto tra il responsabile del trattamento e un altro responsabile del trattamento, né di aggiungere altre clausole o garanzie supplementari, purché non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate dalla Commissione o da un'autorità di controllo o ledano i diritti o le libertà fondamentali degli interessati. I titolari del trattamento e i responsabili del trattamento dovrebbero essere incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le clausole tipo di protezione.

- (110) Un gruppo imprenditoriale o un gruppo di imprese che svolge un'attività economica comune dovrebbe poter applicare le norme vincolanti d'impresa approvate per i trasferimenti internazionali dall'Unione agli organismi dello stesso gruppo imprenditoriale o gruppo d'impresa che svolge un'attività economica comune, purché tali norme contemplino tutti i principi fondamentali e diritti azionabili che costituiscano adeguate garanzie per i trasferimenti o categorie di trasferimenti di dati personali.
- (111) È opportuno prevedere la possibilità di trasferire dati in alcune circostanze se l'interessato ha esplicitamente acconsentito, se il trasferimento è occasionale e necessario in relazione a un contratto o un'azione legale, che sia in sede giudiziale, amministrativa o stragiudiziale, compresi i procedimenti dinanzi alle autorità di regolamentazione. È altresì opportuno prevedere la possibilità di trasferire dati se sussistono motivi di rilevante interesse pubblico previsti dal diritto dell'Unione o degli Stati membri o se i dati sono trasferiti da un registro stabilito per legge e destinato a essere consultato dal pubblico o dalle persone aventi un legittimo interesse. In quest'ultimo caso, il trasferimento non dovrebbe riguardare la totalità dei dati personali o delle categorie di dati contenuti nel registro; inoltre, quando il registro è destinato a essere consultato dalle persone aventi un legittimo interesse, i dati possono essere trasferiti soltanto se tali persone lo richiedono o ne sono destinatarie, tenendo pienamente conto degli interessi e dei diritti fondamentali dell'interessato.
- (112) Tali deroghe dovrebbero in particolare valere per i trasferimenti di dati richiesti e necessari per importanti motivi di interesse pubblico, ad esempio nel caso di scambio internazionale di dati tra autorità garanti della concorrenza, amministrazioni fiscali o doganali, autorità di controllo finanziario, servizi competenti in materia di sicurezza sociale o sanità pubblica, ad esempio in caso di ricerca di contatti per malattie contagiose o al fine di ridurre e/o eliminare il doping nello sport. Il trasferimento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per salvaguardare un interesse che è essenziale per gli interessi vitali dell'interessato o di un'altra persona, comprese la vita o l'integrità fisica, qualora l'interessato si trovi nell'incapacità di prestare il proprio consenso. In mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri dovrebbero notificare tali disposizioni alla Commissione. Qualunque trasferimento a un'organizzazione internazionale umanitaria di dati personali di un interessato che si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso ai fini dell'esecuzione di un compito derivante dalle convenzioni di Ginevra o al fine di rispettare il diritto internazionale umanitario applicabile nei conflitti armati potrebbe essere considerato necessario per importanti motivi di interesse pubblico o nell'interesse vitale dell'interessato.
- (113) Potrebbero altresì essere autorizzati i trasferimenti qualificabili come non ripetitivi e riguardanti soltanto un numero limitato di interessati ai fini del perseguimento degli interessi legittimi cogenti del titolare del trattamento, a meno che non prevalgano gli interessi o i diritti e le libertà dell'interessato e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento. Il titolare del trattamento dovrebbe considerare con particolare attenzione la natura dei dati personali, la finalità e la durata del trattamento o dei trattamenti proposti, nonché la situazione nel paese d'origine, nel paese terzo e nel paese di destinazione finale, e dovrebbe offrire garanzie adeguate per la tutela dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali. Tali trasferimenti dovrebbero essere ammessi soltanto nei casi residui in cui nessuno degli altri presupposti per il trasferimento è applicabile. Per finalità di ricerca scientifica o storica o a fini statistici, è opportuno tener conto delle legittime aspettative della società nei confronti di un miglioramento delle conoscenze. Il titolare del trattamento dovrebbe informare l'autorità di controllo e l'interessato in merito al trasferimento.
- (114) In ogni caso, se la Commissione non ha adottato alcuna decisione circa il livello adeguato di protezione dei dati di un paese terzo, il titolare del trattamento o il responsabile del trattamento dovrebbe ricorrere a soluzioni che diano all'interessato diritti effettivi e azionabili in relazione al trattamento dei suoi dati personali nell'Unione, dopo il trasferimento, così da continuare a beneficiare dei diritti fondamentali e delle garanzie.

- (115) Alcuni paesi terzi adottano leggi, regolamenti e altri atti normativi finalizzati a disciplinare direttamente le attività di trattamento di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. Essi possono includere le sentenze di autorità giurisdizionali o le decisioni di autorità amministrative di paesi terzi che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento e non sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria. L'applicazione extraterritoriale di tali leggi, regolamenti e altri atti normativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della protezione delle persone fisiche assicurata nell'Unione con il presente regolamento. I trasferimenti dovrebbero quindi essere consentiti solo se ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi. Ciò vale, tra l'altro, quando la comunicazione è necessaria per un rilevante motivo di interesse pubblico riconosciuto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento.
- (116) Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati dall'insufficienza di poteri per prevenire e correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. Pertanto vi è la necessità di promuovere una più stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni e condurre indagini di concerto con le loro controparti internazionali. Al fine di sviluppare meccanismi di cooperazione internazionale per agevolare e prestare mutua assistenza a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, la Commissione e le autorità di controllo dovrebbero scambiare informazioni e cooperare, nell'ambito di attività connesse con l'esercizio dei loro poteri, con le autorità competenti in paesi terzi, sulla base della reciprocità e in conformità del presente regolamento.
- (117) L'istituzione di autorità di controllo a cui è conferito il potere di eseguire i loro compiti ed esercitare i loro poteri in totale indipendenza in ciascuno Stato membro è un elemento essenziale della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali. Gli Stati membri dovrebbero poter istituire più di una autorità di controllo, al fine di rispecchiare la loro struttura costituzionale, organizzativa e amministrativa.
- (118) L'indipendenza delle autorità di controllo non dovrebbe significare che tali autorità non possano essere assoggettate a meccanismi di controllo o monitoraggio con riguardo alle loro spese o a controllo giurisdizionale.
- (119) Laddove siano istituite più autorità di controllo, lo Stato membro dovrebbe stabilire per legge meccanismi atti ad assicurare la partecipazione effettiva di dette autorità al meccanismo di coerenza. Lo Stato membro dovrebbe in particolare designare l'autorità di controllo che funge da punto di contatto unico per l'effettiva partecipazione di tutte le autorità al meccanismo, onde garantire la rapida e agevole cooperazione con altre autorità di controllo, il comitato e la Commissione.
- (120) Ciascuna autorità di controllo dovrebbe disporre delle risorse umane e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei propri compiti, compresi quelli di assistenza reciproca e cooperazione con altre autorità di controllo in tutta l'Unione. Ciascuna autorità di controllo dovrebbe disporre di un bilancio annuale, separato e pubblico, che può far parte del bilancio generale statale o nazionale.
- (121) Le condizioni generali applicabili al membro o ai membri dell'autorità di controllo dovrebbero essere stabilite per legge da ciascuno Stato membro e dovrebbero in particolare prevedere che tali membri devono essere nominati, attraverso una procedura trasparente, dal parlamento, dal governo o dal capo di Stato dello Stato membro, sulla base di una proposta del governo, di un membro del governo, del parlamento o di una sua camera, o da un organismo indipendente incaricato ai sensi del diritto degli Stati membri. Al fine di assicurare l'indipendenza dell'autorità di controllo, è opportuno che il membro o i membri di tale autorità agiscano con integrità, si astengano da qualunque azione incompatibile con le loro funzioni e, per tutta la durata del mandato, non esercitino alcuna altra attività incompatibile, remunerata o meno. L'autorità di controllo dovrebbe disporre di proprio personale, scelto dalla stessa autorità di controllo o da un organismo indipendente istituito ai sensi del diritto degli Stati membri, che dovrebbe essere soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo.
- (122) Ogni autorità di controllo dovrebbe avere la competenza, nel territorio del proprio Stato membro, a esercitare i poteri e ad assolvere i compiti a essa attribuiti a norma del presente regolamento. Ciò dovrebbe comprendere in

particolare il trattamento nell'ambito delle attività di uno stabilimento del titolare del trattamento o del responsabile del trattamento sul territorio del proprio Stato membro, il trattamento di dati personali effettuato dalle pubbliche autorità o dagli organismi privati che agiscono nel pubblico interesse, il trattamento riguardante gli interessati nel suo territorio o il trattamento effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione europea riguardante interessati non residenti nel suo territorio. Ciò dovrebbe includere l'esame dei reclami proposti dall'interessato, lo svolgimento di indagini sull'applicazione del regolamento e la promozione della sensibilizzazione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali.

- (123) Le autorità di controllo dovrebbero controllare l'applicazione delle disposizioni del presente regolamento e contribuire alla sua coerente applicazione in tutta l'Unione, così da tutelare le persone fisiche in relazione al trattamento dei loro dati personali e facilitare la libera circolazione di tali dati nel mercato interno. A tal fine, le autorità di controllo dovrebbero cooperare tra loro e con la Commissione, senza che siano necessari accordi tra gli Stati membri sulla mutua assistenza o su tale tipo di cooperazione.
- (124) Qualora il trattamento dei dati personali abbia luogo nell'ambito delle attività di uno stabilimento di un titolare del trattamento o di un responsabile del trattamento nell'Unione e il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro o qualora il trattamento effettuato nell'ambito delle attività dello stabilimento unico di un titolare del trattamento o responsabile del trattamento nell'Unione incida o possa verosimilmente incidere in modo sostanziale su interessati in più di uno Stato membro, l'autorità di controllo dello stabilimento principale del titolare del trattamento o del responsabile del trattamento o dello stabilimento unico del titolare del trattamento o del responsabile del trattamento dovrebbe fungere da autorità capofila. Essa dovrebbe cooperare con le altre autorità interessate perché il titolare del trattamento o il responsabile del trattamento ha uno stabilimento nel territorio dei loro Stati membri, perché il trattamento incide in modo sostanziale sugli interessati residenti nel loro territorio o perché è stato proposto loro un reclamo. Anche in caso di reclamo proposto da un interessato non residente in tale Stato membro, l'autorità di controllo cui è stato proposto detto reclamo dovrebbe essere considerata un'autorità di controllo interessata. Nell'ambito del suo compito di rilascio di linee guida su qualsiasi questione relativa all'applicazione del presente regolamento, il comitato dovrebbe essere in grado di pubblicare linee guida in particolare sui criteri da prendere in considerazione per accertare se il trattamento in questione incida in modo sostanziale su interessati in più di uno Stato membro e su cosa costituisca obiezione pertinente e motivata.
- (125) L'autorità capofila dovrebbe essere competente per l'adozione di decisioni vincolanti riguardanti misure di applicazione dei poteri di cui gode a norma del presente regolamento. Nella sua qualità di autorità capofila, l'autorità di controllo dovrebbe coinvolgere e coordinare strettamente le autorità di controllo interessate nel processo decisionale. In caso di decisione di rigetto del reclamo dell'interessato, in tutto o in parte, tale decisione dovrebbe essere adottata dall'autorità di controllo a cui il reclamo è stato proposto.
- (126) La decisione dovrebbe essere adottata congiuntamente dall'autorità di controllo capofila e dalle autorità di controllo interessate e dovrebbe essere rivolta allo stabilimento principale o unico del titolare del trattamento o del responsabile del trattamento ed essere vincolante per il titolare del trattamento e il responsabile del trattamento. Il titolare del trattamento o il responsabile del trattamento dovrebbe adottare le misure necessarie per garantire la conformità al presente regolamento e l'attuazione della decisione notificata dall'autorità di controllo capofila allo stabilimento principale del titolare del trattamento o del responsabile del trattamento per quanto riguarda le attività di trattamento nell'Unione.
- (127) Ogni autorità di controllo che non agisce in qualità di autorità di controllo capofila dovrebbe essere competente a trattare casi locali qualora il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro, ma l'oggetto dello specifico trattamento riguardi unicamente il trattamento effettuato in un singolo Stato membro e coinvolga soltanto interessati in tale singolo Stato membro, ad esempio quando l'oggetto riguarda il trattamento di dati personali di dipendenti nell'ambito di specifici rapporti di lavoro in uno Stato membro. In tali casi, l'autorità di controllo dovrebbe informare senza indugio l'autorità di controllo capofila sulla questione. Dopo essere stata informata, l'autorità di controllo capofila dovrebbe decidere se intende trattare il caso a norma della disposizione sulla cooperazione tra l'autorità di controllo capofila e altre autorità di controllo interessate («meccanismo dello sportello unico»), ovvero se l'autorità di controllo che l'ha informata debba trattarlo a livello locale. Al momento di decidere se intende trattare il caso, l'autorità di controllo capofila dovrebbe tenere conto dell'eventuale esistenza, nello Stato membro dell'autorità di controllo che l'ha informata, di uno stabilimento del titolare del trattamento o del responsabile del trattamento, al fine di garantire l'effettiva applicazione di una decisione nei confronti del titolare del trattamento o del responsabile del trattamento. Qualora l'autorità di controllo capofila decida di trattare il caso, l'autorità di controllo che l'ha informata

dovrebbe avere la possibilità di presentare un progetto di decisione, che l'autorità di controllo capofila dovrebbe tenere nella massima considerazione nella preparazione del proprio progetto di decisione nell'ambito di tale meccanismo di sportello unico.

- (128) Le norme sull'autorità di controllo capofila e sul meccanismo di sportello unico non dovrebbero applicarsi quando il trattamento è effettuato da autorità pubbliche o da organismi privati nell'interesse pubblico. In tali casi l'unica autorità di controllo competente a esercitare i poteri a essa conferiti a norma del presente regolamento dovrebbe essere l'autorità di controllo dello Stato membro in cui l'autorità pubblica o l'organismo privato sono stabiliti.
- (129) Al fine di garantire un monitoraggio e un'applicazione coerenti del presente regolamento in tutta l'Unione, le autorità di controllo dovrebbero avere in ciascuno Stato membro gli stessi compiti e poteri effettivi, fra cui poteri di indagine, poteri correttivi e sanzionatori, e poteri autorizzativi e consultivi, segnatamente in caso di reclamo proposto da persone fisiche, e fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale ai sensi del diritto degli Stati membri, il potere di intentare un'azione e di agire in sede giudiziale o stragiudiziale in caso di violazione del presente regolamento. Tali poteri dovrebbero includere anche il potere di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento. Gli Stati membri possono precisare altri compiti connessi alla protezione dei dati personali ai sensi del presente regolamento. È opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e degli Stati membri, in modo imparziale ed equo ed entro un termine ragionevole. In particolare ogni misura dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità al presente regolamento, tenuto conto delle circostanze di ciascun singolo caso, rispettare il diritto di ogni persona di essere ascoltata prima che nei suoi confronti sia adottato un provvedimento individuale che le rechi pregiudizio ed evitare costi superflui ed eccessivi disagi per le persone interessate. I poteri di indagine per quanto riguarda l'accesso ai locali dovrebbero essere esercitati nel rispetto dei requisiti specifici previsti dal diritto processuale degli Stati membri, quale l'obbligo di ottenere un'autorizzazione giudiziaria preliminare. Ogni misura giuridicamente vincolante dell'autorità di controllo dovrebbe avere forma scritta, essere chiara e univoca, riportare l'autorità di controllo che ha adottato la misura e la relativa data di adozione, recare la firma del responsabile o di un membro dell'autorità di controllo da lui autorizzata, precisare i motivi della misura e fare riferimento al diritto a un ricorso effettivo. Ciò non dovrebbe precludere requisiti supplementari ai sensi del diritto processuale degli Stati membri. L'adozione di una decisione giuridicamente vincolante implica che essa può essere soggetta a controllo giurisdizionale nello Stato membro dell'autorità di controllo che ha adottato la decisione.
- (130) Qualora l'autorità di controllo cui sia stato proposto il reclamo non sia l'autorità di controllo capofila, l'autorità di controllo capofila dovrebbe cooperare strettamente con l'autorità di controllo cui è stato proposto il reclamo in conformità delle disposizioni sulla cooperazione e la coerenza previste dal presente regolamento. In tali casi, l'autorità di controllo capofila, nell'adottare le misure intese a produrre effetti giuridici, compresa l'imposizione di sanzioni amministrative pecuniarie, dovrebbe tenere nella massima considerazione il parere dell'autorità di controllo cui è stato proposto il reclamo e che dovrebbe rimanere competente per svolgere indagini nel territorio del proprio Stato membro in collegamento con l'autorità di controllo capofila.
- (131) Qualora un'altra autorità di controllo agisca in qualità di autorità di controllo capofila per le attività di trattamento del titolare del trattamento o del responsabile del trattamento, ma il concreto oggetto di un reclamo o la possibile violazione riguardi solo attività di trattamento del titolare del trattamento o del responsabile del trattamento nello Stato membro di presentazione del reclamo o di accertamento della possibile violazione e la questione non incida in modo sostanziale o è improbabile che incida in modo sostanziale su interessati in altri Stati membri, l'autorità di controllo che riceva un reclamo o che accerti o sia altrimenti informata di situazioni che implicano possibili violazioni del regolamento dovrebbe tentare una composizione amichevole con il titolare del trattamento e, qualora ciò non abbia esito, esercitare l'intera sua gamma di poteri. Ciò dovrebbe includere: il trattamento specifico effettuato nel territorio dello Stato membro dell'autorità di controllo o con riguardo agli interessati nel territorio di tale Stato membro; il trattamento effettuato nell'ambito di un'offerta di beni o prestazione di servizi specificamente riguardante gli interessati nel territorio dello Stato membro dell'autorità di controllo; o il trattamento che deve essere oggetto di valutazione tenuto conto dei pertinenti obblighi giuridici ai sensi della legislazione degli Stati membri.
- (132) Le attività di sensibilizzazione delle autorità di controllo nei confronti del pubblico dovrebbero comprendere misure specifiche per i titolari del trattamento e i responsabili del trattamento, comprese le micro, piccole e medie imprese, e le persone fisiche in particolare nel contesto educativo.

- (133) Le autorità di controllo dovrebbero prestarsi assistenza reciproca nell'adempimento dei loro compiti, in modo da garantire la coerente applicazione e attuazione del presente regolamento nel mercato interno. L'autorità di controllo che chiede assistenza reciproca può adottare una misura provvisoria in caso di mancato riscontro a una richiesta di assistenza reciproca entro un mese dal ricevimento di tale richiesta da parte dell'altra autorità di controllo.
- (134) Ciascuna autorità di controllo dovrebbe, se del caso, partecipare alle operazioni congiunte con altre autorità di controllo. L'autorità di controllo che riceve una richiesta dovrebbe darvi seguito entro un termine determinato.
- (135) È opportuno istituire un meccanismo di coerenza per la cooperazione tra le autorità di controllo, al fine di assicurare un'applicazione coerente del presente regolamento in tutta l'Unione. Tale meccanismo dovrebbe applicarsi in particolare quando un'autorità di controllo intenda adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di trattamento che incidono in modo sostanziale su un numero significativo di interessati in vari Stati membri. È opportuno che il meccanismo si attivi anche quando un'autorità di controllo interessata o la Commissione chiede che tale questione sia trattata nell'ambito del meccanismo di coerenza. Tale meccanismo non dovrebbe pregiudicare le misure che la Commissione può adottare nell'esercizio dei suoi poteri a norma dei trattati.
- (136) In applicazione del meccanismo di coerenza il comitato dovrebbe emettere un parere entro un termine determinato, se i suoi membri lo decidono a maggioranza o se a richiederlo è un'autorità di controllo interessata o la Commissione. Il comitato dovrebbe altresì avere il potere di adottare decisioni giuridicamente vincolanti qualora insorgano controversie tra autorità di controllo. A tal fine, dovrebbe adottare, in linea di principio a maggioranza dei due terzi dei suoi membri, decisioni giuridicamente vincolanti in casi chiaramente determinati in cui vi siano pareri divergenti tra le autorità di controllo segnatamente nell'ambito del meccanismo di cooperazione tra l'autorità di controllo capofila e le autorità di controllo interessate sul merito del caso, in particolare sulla sussistenza di una violazione del presente regolamento.
- (137) Potrebbe essere necessario intervenire urgentemente per tutelare i diritti e le libertà degli interessati, in particolare quando sussiste il pericolo che l'esercizio di un diritto possa essere gravemente ostacolato. Un'autorità di controllo potrebbe pertanto essere in grado di adottare misure provvisorie debitamente giustificate nel proprio territorio, con un periodo di validità determinato che non dovrebbe superare tre mesi.
- (138) L'applicazione di tale meccanismo dovrebbe essere un presupposto di liceità di una misura intesa a produrre effetti giuridici adottata dall'autorità di controllo nei casi in cui la sua applicazione è obbligatoria. In altri casi di rilevanza transfrontaliera, si dovrebbe applicare il meccanismo di cooperazione tra autorità di controllo capofila e autorità di controllo interessate e le autorità di controllo interessate potrebbero prestarsi assistenza reciproca ed effettuare operazioni congiunte, su base bilaterale o multilaterale, senza attivare il meccanismo di coerenza.
- (139) Per promuovere l'applicazione coerente del presente regolamento, il comitato dovrebbe essere istituito come un organismo indipendente dell'Unione. Per conseguire i suoi obiettivi, il comitato dovrebbe essere dotato di personalità giuridica. Il comitato dovrebbe essere rappresentato dal suo presidente. Esso dovrebbe sostituire il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito con direttiva 95/46/CE. Il comitato dovrebbe essere composto dalla figura di vertice dell'autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti. È opportuno che la Commissione partecipi alle attività del comitato senza diritto di voto e che il garante europeo della protezione dei dati abbia diritti di voto specifici. Il comitato dovrebbe contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, anche fornendo consulenza alla Commissione, in particolare sul livello di protezione garantito dai paesi terzi o dalle organizzazioni internazionali, e promuovendo la cooperazione delle autorità di controllo in tutta l'Unione. Esso dovrebbe assolvere i suoi compiti in piena indipendenza.
- (140) Il comitato dovrebbe essere assistito da un segretariato messo a disposizione dal garante europeo della protezione dei dati. Il personale del garante europeo della protezione dei dati impegnato nell'assolvimento dei compiti attribuiti al comitato dal presente regolamento dovrebbe svolgere i suoi compiti esclusivamente secondo le istruzioni del presidente del comitato e riferire a quest'ultimo.
- (141) Ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente, e il diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento

o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato. Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico. È opportuno che l'autorità di controllo informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato dovrebbe ricevere informazioni interlocutorie. Per agevolare la proposizione di reclami, ogni autorità di controllo dovrebbe adottare misure quali la messa a disposizione di un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.

- (142) Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento, dovrebbe avere il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto di uno Stato membro, con obiettivi statutari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto a un'autorità di controllo, esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati se quest'ultimo è previsto dal diritto degli Stati membri. Gli Stati membri possono prescrivere che tale organismo, organizzazione o associazione abbia il diritto di proporre reclamo in tale Stato membro, indipendentemente dall'eventuale mandato dell'interessato, e il diritto di proporre un ricorso giurisdizionale effettivo qualora abbia motivo di ritenere che i diritti di un interessato siano stati violati in conseguenza di un trattamento dei dati personali che violi il presente regolamento. tale organismo, organizzazione o associazione può non essere autorizzato a chiedere il risarcimento del danno per conto di un interessato indipendentemente dal mandato dell'interessato.
- (143) Qualsiasi persona fisica o giuridica ha diritto di proporre un ricorso per l'annullamento delle decisioni del comitato dinanzi alla Corte di giustizia, alle condizioni previste all'articolo 263 TFUE. In quanto destinatari di tali decisioni, le autorità di controllo interessate che intendono impugnarle, devono proporre ricorso entro due mesi dalla loro notifica, conformemente all'articolo 263 TFUE. Ove le decisioni del comitato si riferiscano direttamente e individualmente a un titolare del trattamento, a un responsabile del trattamento o al reclamante, quest'ultimo può proporre un ricorso per l'annullamento di tali decisioni e dovrebbe farlo entro due mesi dalla loro pubblicazione sul sito web del comitato, conformemente all'articolo 263 TFUE. Fatto salvo tale diritto ai sensi dell'articolo 263 TFUE, ogni persona fisica o giuridica dovrebbe poter proporre un ricorso giurisdizionale effettivo dinanzi alle competenti autorità giurisdizionali nazionali contro una decisione dell'autorità di controllo che produce effetti giuridici nei confronti di detta persona. Tale decisione riguarda in particolare l'esercizio di poteri di indagine, correttivi e autorizzativi da parte dell'autorità di controllo o l'archiviazione o il rigetto dei reclami. Tuttavia, tale diritto a un ricorso giurisdizionale effettivo non comprende altre misure adottate dalle autorità di controllo che non sono giuridicamente vincolanti, come pareri o consulenza forniti dall'autorità di controllo. Le azioni contro l'autorità di controllo dovrebbero essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita e dovrebbero essere effettuate in conformità del diritto processuale dello Stato membro in questione. Tali autorità giurisdizionali dovrebbero esercitare i loro pieni poteri giurisdizionali, ivi compreso quello di esaminare tutte le questioni di fatto e di diritto che abbiano rilevanza per la controversia dinanzi a esse pendente.

Se un reclamo è stato rigettato o archiviato da un'autorità di controllo, il reclamante può proporre ricorso giurisdizionale nello stesso Stato membro. Nell'ambito dei ricorsi giurisdizionali relativi all'applicazione del presente regolamento, le autorità giurisdizionali nazionali che ritengano necessario, ai fini di una sentenza, disporre di una decisione in merito, possono, o nel caso di cui all'articolo 267 TFUE, devono chiedere alla Corte di giustizia di pronunciarsi, in via pregiudiziale, sull'interpretazione del diritto dell'Unione, compreso il presente regolamento. Inoltre, se una decisione dell'autorità di controllo che attua una decisione del comitato è impugnata dinanzi a un'autorità giurisdizionale nazionale ed è in questione la validità della decisione del comitato, tale autorità giurisdizionale nazionale non ha il potere di invalidare la decisione del comitato, ma deve deferire la questione di validità alla Corte di giustizia ai sensi dell'articolo 267 TFUE quale interpretato dalla Corte di giustizia, ove ritenga la decisione non valida. Tuttavia, un'autorità giurisdizionale nazionale non può deferire una questione relativa alla validità di una decisione del comitato su richiesta di una persona fisica o giuridica che ha avuto la possibilità di proporre un ricorso per l'annullamento di tale decisione, specialmente se direttamente e individualmente interessata da siffatta decisione, ma non ha agito in tal senso entro il termine stabilito dall'articolo 263 TFUE.

- (144) Qualora un'autorità giurisdizionale adita per un'azione contro una decisione di un'autorità di controllo abbia motivo di ritenere che le azioni riguardanti lo stesso trattamento, quale lo stesso oggetto relativamente al trattamento da parte dello stesso titolare del trattamento o dello stesso responsabile del trattamento, o lo stesso titolo, siano sottoposte a un'autorità giurisdizionale competente in un altro Stato membro, l'autorità giurisdizionale adita dovrebbe contattare tale autorità giurisdizionale al fine di confermare l'esistenza di tali azioni connesse. Se le azioni connesse sono pendenti dinanzi a un'autorità giurisdizionale in un altro Stato membro,

qualsiasi autorità giurisdizionale successivamente adita può sospendere l'azione proposta dinanzi a essa o, su richiesta di una delle parti, può dichiarare la propria incompetenza a favore della prima autorità giurisdizionale adita se tale autorità giurisdizionale è competente a conoscere delle azioni in questione e la sua legge consente la riunione delle azioni. Le azioni sono considerate connesse quando hanno tra loro un legame così stretto da rendere opportuno trattarle e decidere in merito contestualmente, per evitare il rischio di sentenze incompatibili risultanti da azioni separate.

- (145) Nelle azioni contro un titolare del trattamento o responsabile del trattamento, il ricorrente dovrebbe poter avviare un'azione legale dinanzi all'autorità giurisdizionale dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento o in cui risiede l'interessato, salvo che il titolare del trattamento sia un'autorità pubblica di uno Stato membro che agisce nell'esercizio dei suoi poteri pubblici.
- (146) Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento.
- (147) Qualora il presente regolamento preveda disposizioni specifiche in materia di giurisdizione, in particolare riguardo a procedimenti che prevedono il ricorso giurisdizionale, compreso quello per risarcimento, contro un titolare del trattamento o un responsabile del trattamento, disposizioni generali in materia di giurisdizione quali quelle di cui al regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio⁽¹⁾ non dovrebbero pregiudicare l'applicazione di dette disposizioni specifiche.
- (148) Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento. In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisca un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria. Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo.
- (149) Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del *ne bis in idem* quale interpretato dalla Corte di giustizia.
- (150) Al fine di rafforzare e armonizzare le sanzioni amministrative applicabili per violazione del presente regolamento, ogni autorità di controllo dovrebbe poter imporre sanzioni amministrative pecuniarie. Il presente regolamento

⁽¹⁾ Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU L 351 del 20.12.2012, pag. 1).

dovrebbe specificare le violazioni, indicare il limite massimo e i criteri per prevedere la relativa sanzione amministrativa pecuniaria, che dovrebbe essere stabilita dall'autorità di controllo competente in ogni singolo caso, tenuto conto di tutte le circostanze pertinenti della situazione specifica, in particolare della natura, gravità e durata dell'infrazione e delle relative conseguenze, nonché delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione. Se le sanzioni amministrative sono inflitte a imprese, le imprese dovrebbero essere intese quali definite agli articoli 101 e 102 TFUE a tali fini. Se le sanzioni amministrative sono inflitte a persone che non sono imprese, l'autorità di controllo dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Il meccanismo di coerenza può essere utilizzato anche per favorire un'applicazione coerente delle sanzioni amministrative pecuniarie. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie. Imporre una sanzione amministrativa pecuniaria o dare un avvertimento non incide sull'applicazione di altri poteri delle autorità di controllo o di altre sanzioni a norma del regolamento.

- (151) I sistemi giudiziari di Danimarca ed Estonia non consentono l'irrogazione di sanzioni amministrative pecuniarie come previsto dal presente regolamento. Le norme relative alle sanzioni amministrative pecuniarie possono essere applicate in maniera tale che in Danimarca la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali quale sanzione penale e in Estonia la sanzione pecuniaria sia imposta dall'autorità di controllo nel quadro di una procedura d'infrazione, purché l'applicazione di tali norme in detti Stati membri abbia effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. Le competenti autorità giurisdizionali nazionali dovrebbero pertanto tener conto della raccomandazione dell'autorità di controllo che avvia l'azione sanzionatoria. In ogni caso, le sanzioni pecuniarie irrogate dovrebbero essere effettive, proporzionate e dissuasive.
- (152) Se il presente regolamento non armonizza le sanzioni amministrative o se necessario in altri casi, ad esempio in caso di gravi violazioni del regolamento, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive. La natura di tali sanzioni, penali o amministrative, dovrebbe essere determinata dal diritto degli Stati membri.
- (153) Il diritto degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali ai sensi del presente regolamento. Il trattamento dei dati personali effettuato unicamente a scopi giornalistici o di espressione accademica, artistica o letteraria dovrebbe essere soggetto a deroghe o esenzioni rispetto ad alcune disposizioni del presente regolamento se necessario per conciliare il diritto alla protezione dei dati personali e il diritto alla libertà d'espressione e di informazione sancito nell'articolo 11 della Carta. Ciò dovrebbe applicarsi in particolare al trattamento dei dati personali nel settore audiovisivo, negli archivi stampa e nelle emeroteche. È pertanto opportuno che gli Stati adottino misure legislative che prevedano le deroghe e le esenzioni necessarie ai fini di un equilibrio tra tali diritti fondamentali. Gli Stati membri dovrebbero adottare tali esenzioni e deroghe con riferimento alle disposizioni riguardanti i principi generali, i diritti dell'interessato, il titolare del trattamento e il responsabile del trattamento, il trasferimento di dati personali verso paesi terzi o a organizzazioni internazionali, le autorità di controllo indipendenti, la cooperazione e la coerenza nonché situazioni di trattamento dei dati specifiche. Qualora tali esenzioni o deroghe differiscano da uno Stato membro all'altro, dovrebbe applicarsi il diritto dello Stato membro cui è soggetto il titolare del trattamento. Per tenere conto dell'importanza del diritto alla libertà di espressione in tutte le società democratiche è necessario interpretare in modo esteso i concetti relativi a detta libertà, quali la nozione di giornalismo.
- (154) Il presente regolamento ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali. L'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico. I dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti. Tali disposizioni legislative dovrebbero conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali e possono quindi prevedere la necessaria conciliazione con il diritto alla protezione dei dati personali, in conformità del presente regolamento. Il riferimento alle autorità pubbliche e agli organismi pubblici dovrebbe comprendere, in tale contesto, tutte le autorità o altri organismi cui si applica il diritto degli Stati membri sull'accesso del pubblico ai documenti. La direttiva 2003/98/CE del Parlamento europeo e del Consiglio ⁽¹⁾ non pregiudica in alcun modo il livello di tutela

⁽¹⁾ Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico (GUL 345 del 31.12.2003, pag. 90).

delle persone fisiche con riguardo al trattamento dei dati personali ai sensi delle disposizioni di diritto dell'Unione e degli Stati membri e non modifica, in particolare, gli obblighi e i diritti previsti dal presente regolamento. Nello specifico, tale direttiva non dovrebbe applicarsi ai documenti il cui accesso è escluso o limitato in virtù dei regimi di accesso per motivi di protezione dei dati personali, e a parti di documenti accessibili in virtù di tali regimi che contengono dati personali il cui riutilizzo è stato previsto per legge come incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali.

- (155) Il diritto degli Stati membri o i contratti collettivi, ivi compresi gli «accordi aziendali», possono prevedere norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per quanto riguarda le condizioni alle quali i dati personali nei rapporti di lavoro possono essere trattati sulla base del consenso del dipendente, per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.
- (156) Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici dovrebbe essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie dovrebbero assicurare che siano state predisposte misure tecniche e organizzative al fine di garantire, in particolare, il principio della minimizzazione dei dati. L'ulteriore trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è da effettuarsi quando il titolare del trattamento ha valutato la fattibilità di conseguire tali finalità trattando dati personali che non consentono o non consentono più di identificare l'interessato, purché esistano garanzie adeguate (come ad esempio la pseudonimizzazione dei dati personali). Gli Stati membri dovrebbero prevedere garanzie adeguate per il trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche. Gli Stati membri dovrebbero essere autorizzati a fornire, a specifiche condizioni e fatte salve adeguate garanzie per gli interessati, specifiche e deroghe relative ai requisiti in materia di informazione e ai diritti alla rettifica, alla cancellazione, all'oblio, alla limitazione del trattamento, alla portabilità dei dati personali, nonché al diritto di opporsi in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche. Le condizioni e le garanzie in questione possono comprendere procedure specifiche per l'esercizio di tali diritti da parte degli interessati, qualora ciò sia appropriato alla luce delle finalità previste dallo specifico trattamento, oltre a misure tecniche e organizzative intese a ridurre al minimo il trattamento dei dati personali conformemente ai principi di proporzionalità e di necessità. Il trattamento dei dati personali per finalità scientifiche dovrebbe rispettare anche altre normative pertinenti, ad esempio quelle sulle sperimentazioni cliniche.
- (157) Combinando informazioni provenienti dai registri, i ricercatori possono ottenere nuove conoscenze di grande utilità relativamente a patologie diffuse come le malattie cardiovascolari, il cancro e la depressione. Avvalendosi dei registri, i risultati delle ricerche possono acquistare maggiore rilevanza, dal momento che si basano su una popolazione più ampia. Nell'ambito delle scienze sociali, la ricerca basata sui registri consente ai ricercatori di ottenere conoscenze essenziali sulla correlazione a lungo termine tra numerose condizioni sociali, quali la disoccupazione e il livello di istruzione, e altre condizioni di vita. I risultati delle ricerche ottenuti dai registri forniscono conoscenze solide e di alta qualità, che possono costituire la base per l'elaborazione e l'attuazione di politiche basate sulla conoscenza, migliorare la qualità della vita per molte persone, migliorare l'efficienza dei servizi sociali. Al fine di facilitare la ricerca scientifica, i dati personali possono essere trattati per finalità di ricerca scientifica fatte salve condizioni e garanzie adeguate previste dal diritto dell'Unione o degli Stati membri.
- (158) Qualora i dati personali siano trattati a fini di archiviazione, il presente regolamento dovrebbe applicarsi anche a tale tipo di trattamento, tenendo presente che non dovrebbe applicarsi ai dati delle persone decedute. Le autorità pubbliche o gli organismi pubblici o privati che tengono registri di interesse pubblico dovrebbero essere servizi che, in virtù del diritto dell'Unione o degli Stati membri, hanno l'obbligo legale di acquisire, conservare, valutare, organizzare, descrivere, comunicare, promuovere, diffondere e fornire accesso a registri con un valore a lungo termine per l'interesse pubblico generale. Gli Stati membri dovrebbero inoltre essere autorizzati a prevedere il trattamento ulteriore dei dati personali per finalità di archiviazione, per esempio al fine di fornire specifiche informazioni connesse al comportamento politico sotto precedenti regimi statali totalitari, a genocidi, crimini contro l'umanità, in particolare l'Olocausto, o crimini di guerra.

- (159) Qualora i dati personali siano trattati per finalità di ricerca scientifica, il presente regolamento dovrebbe applicarsi anche a tale trattamento. Nell'ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica. Per rispondere alle specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica. Se il risultato della ricerca scientifica, in particolare nel contesto sanitario, costituisce motivo per ulteriori misure nell'interesse dell'interessato, le norme generali del presente regolamento dovrebbero applicarsi in vista di tali misure.
- (160) Qualora i dati personali siano trattati a fini di ricerca storica, il presente regolamento dovrebbe applicarsi anche a tale trattamento. Ciò dovrebbe comprendere anche la ricerca storica e la ricerca a fini genealogici, tenendo conto del fatto che il presente regolamento non dovrebbe applicarsi ai dati delle persone decedute.
- (161) Ai fini del consenso alla partecipazione ad attività di ricerca scientifica nell'ambito di sperimentazioni cliniche dovrebbero applicarsi le pertinenti disposizioni del regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio ⁽¹⁾.
- (162) Qualora i dati personali siano trattati per finalità statistiche, il presente regolamento dovrebbe applicarsi a tale trattamento. Il diritto dell'Unione o degli Stati membri dovrebbe, entro i limiti del presente regolamento, determinare i contenuti statistici, il controllo dell'accesso, le specifiche per il trattamento dei dati personali per finalità statistiche e le misure adeguate per tutelare i diritti e le libertà dell'interessato e per garantire il segreto statistico. Per finalità statistiche si intende qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici. Tali risultati statistici possono essere ulteriormente usati per finalità diverse, anche per finalità di ricerca scientifica. La finalità statistica implica che il risultato del trattamento per finalità statistiche non siano dati personali, ma dati aggregati, e che tale risultato o i dati personali non siano utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche.
- (163) È opportuno proteggere le informazioni riservate raccolte dalle autorità statistiche nazionali e dell'Unione per la produzione di statistiche ufficiali europee e nazionali. Le statistiche europee dovrebbero essere sviluppate, prodotte e diffuse conformemente ai principi statistici di cui all'articolo 338, paragrafo 2, TFUE, mentre le statistiche nazionali dovrebbero essere conformi anche al diritto degli Stati membri. Il regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio ⁽²⁾ fornisce ulteriori specificazioni in merito al segreto statistico per quanto riguarda le statistiche europee.
- (164) Per quanto riguarda il potere delle autorità di controllo di ottenere, dal titolare del trattamento o dal responsabile del trattamento, accesso ai dati personali e accesso ai loro locali, gli Stati membri possono stabilire per legge, nei limiti del presente regolamento, norme specifiche per tutelare il segreto professionale o altri obblighi equivalenti di segretezza, qualora si rendano necessarie per conciliare il diritto alla protezione dei dati personali con il segreto professionale. Ciò non pregiudica gli obblighi esistenti degli Stati membri di adottare norme relative al segreto professionale laddove richiesto dal diritto dell'Unione.
- (165) Il presente regolamento rispetta e non pregiudica lo status di cui godono le chiese e le associazioni o comunità religiose negli Stati membri in virtù del diritto costituzionale vigente, in conformità dell'articolo 17 TFUE.
- (166) Al fine di conseguire gli obiettivi del regolamento, segnatamente tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire la libera circolazione di tali

⁽¹⁾ Regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE (GU L 158 del 27.5.2014, pag. 1).

⁽²⁾ Regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio, dell'11 marzo 2009, relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del Parlamento europeo e del Consiglio, relativo alla trasmissione all'Istituto statistico delle Comunità europee di dati statistici protetti dal segreto, il regolamento (CE) n. 322/97 del Consiglio, relativo alle statistiche comunitarie, e la decisione 89/382/CEE, Euratom del Consiglio, che istituisce un comitato del programma statistico delle Comunità europee (GU L 87 del 31.3.2009, pag. 164).

dati nell'Unione, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE. In particolare, dovrebbero essere adottati atti delegati riguardanti i criteri e i requisiti dei meccanismi di certificazione, le informazioni da presentare sotto forma di icone standardizzate e le procedure per fornire tali icone. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti. Nella preparazione e nell'elaborazione degli atti delegati, la Commissione dovrebbe provvedere alla contestuale, tempestiva e appropriata trasmissione dei documenti pertinenti al Parlamento europeo e al Consiglio.

- (167) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione ove previsto dal presente regolamento. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio. A tal fine, la Commissione dovrebbe contemplare misure specifiche per le micro, piccole e medie imprese.
- (168) È opportuno applicare la procedura d'esame per l'adozione di atti di esecuzione su: clausole contrattuali tipo tra i titolari del trattamento e i responsabili del trattamento e tra responsabili del trattamento, codici di condotta; norme tecniche e meccanismi di certificazione; adeguato livello di protezione offerto da un paese terzo, un territorio o settore specifico all'interno del paese terzo, o da un'organizzazione internazionale; clausole tipo di protezione dei dati; formati e procedure per lo scambio di informazioni per via elettronica tra i titolari del trattamento, i responsabili del trattamento e le autorità di controllo per norme vincolanti d'impresa; assistenza reciproca; e modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato.
- (169) È opportuno che la Commissione adotti atti di esecuzione immediatamente applicabili quando gli elementi a disposizione indicano che un paese terzo, un territorio o settore di specifico all'interno di tale paese terzo, o un'organizzazione internazionale non garantisce un livello di protezione adeguato e ciò è reso necessario da imperativi motivi di urgenza.
- (170) Poiché l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.
- (171) Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente regolamento entro un periodo di due anni dall'entrata in vigore del presente regolamento. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento. Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.
- (172) Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e ha espresso un parere il 7 marzo 2012 ⁽¹⁾.
- (173) È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio ⁽²⁾, compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche. Per chiarire il rapporto tra il presente regolamento e la direttiva 2002/58/CE, è opportuno modificare quest'ultima di conseguenza. Una volta adottato il presente regolamento, la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento,

⁽¹⁾ GU C 192 del 30.6.2012, pag. 7.

⁽²⁾ Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GUL 201 del 31.7.2002, pag. 37).

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

Disposizioni generali

Articolo 1

Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.
2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.
3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 2

Ambito di applicazione materiale

1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.
2. Il presente regolamento non si applica ai trattamenti di dati personali:
 - a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;
 - b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;
 - c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;
 - d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.
3. Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.
4. Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

Articolo 3

Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:

- a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
- b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Articolo 4

Definizioni

Ai fini del presente regolamento s'intende per:

- 1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- 2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- 3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- 4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- 5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- 6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- 7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- 8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- 9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati

membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- 10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- 11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- 12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- 13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- 14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- 15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- 16) «stabilimento principale»:
 - a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;
 - b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;
- 17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;
- 18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;
- 19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
- 20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;
- 21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

- 22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:
- il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;
 - gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
 - un reclamo è stato proposto a tale autorità di controllo;
- 23) «trattamento transfrontaliero»:
- trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure
 - trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;
- 24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;
- 25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ⁽¹⁾;
- 26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

CAPO II

Principi

Articolo 5

Principi applicabili al trattamento di dati personali

- I dati personali sono:
 - trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
 - raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
 - adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
 - esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

⁽¹⁾ Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

- e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
 - f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di provarlo («responsabilizzazione»).

Articolo 6

Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
- a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
 - b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
 - c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
 - d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
 - e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
 - f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita:

- a) dal diritto dell'Unione; o
- b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di

conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

- a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;
- c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;
- d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;
- e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 7

Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.
2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.
3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.
4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 8

Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

2. Il titolare del trattamento si adoperava in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.
3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

Articolo 9

Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
 - a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;
 - b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
 - c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
 - d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegue finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
 - e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
 - f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitano le loro funzioni giurisdizionali;
 - g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
 - h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;
 - i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Articolo 10

Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Articolo 11

Trattamento che non richiede l'identificazione

1. Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.

2. Qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione.

CAPO III

Diritti dell'interessato

Sezione 1

Trasparenza e modalità

Articolo 12

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

7. Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

Sezione 2

Informazione e accesso ai dati personali

Articolo 13

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
- a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- d) il diritto di proporre reclamo a un'autorità di controllo;
- e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.
4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 14

Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni:
- a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) le categorie di dati personali in questione;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.
2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:
- a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
 - b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
 - c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
 - d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;
 - e) il diritto di proporre reclamo a un'autorità di controllo;
 - f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;
 - g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:
- a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati;
 - b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure
 - c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.
4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.
5. I paragrafi da 1 a 4 non si applicano se e nella misura in cui:
- a) l'interessato dispone già delle informazioni;
 - b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;
 - c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure
 - d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

*Articolo 15***Diritto di accesso dell'interessato**

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- f) il diritto di proporre reclamo a un'autorità di controllo;
- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

*Sezione 3***Rettifica e cancellazione***Articolo 16***Diritto di rettifica**

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

*Articolo 17***Diritto alla cancellazione («diritto all'oblio»)**

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

- b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
- c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
- d) i dati personali sono stati trattati illecitamente;
- e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

- a) per l'esercizio del diritto alla libertà di espressione e di informazione;
- b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;
- d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o
- e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Articolo 18

Diritto di limitazione di trattamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

- a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

Articolo 19

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Articolo 20

Diritto alla portabilità dei dati

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
 - a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e
 - b) il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Sezione 4

Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

Articolo 21

Diritto di opposizione

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.
3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.
5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Articolo 22

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.
2. Il paragrafo 1 non si applica nel caso in cui la decisione:
 - a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
 - b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;
 - c) si basi sul consenso esplicito dell'interessato.
3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Sezione 5

Limitazioni

Articolo 23

Limitazioni

1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:
 - a) la sicurezza nazionale;
 - b) la difesa;
 - c) la sicurezza pubblica;

- d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
 - e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;
 - f) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;
 - g) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
 - h) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere da a), a e) e g);
 - i) la tutela dell'interessato o dei diritti e delle libertà altrui;
 - j) l'esecuzione delle azioni civili.
2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:
- a) le finalità del trattamento o le categorie di trattamento;
 - b) le categorie di dati personali;
 - c) la portata delle limitazioni introdotte;
 - d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;
 - e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;
 - f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento;
 - g) i rischi per i diritti e le libertà degli interessati; e
 - h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

CAPO IV

Titolare del trattamento e responsabile del trattamento

Sezione 1

Obblighi generali

Articolo 24

Responsabilità del titolare del trattamento

1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.
2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

*Articolo 25***Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.
2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

*Articolo 26***Contitolari del trattamento**

1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.
2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

*Articolo 27***Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione**

1. Ove si applichi l'articolo 3, paragrafo 2, il titolare del trattamento o il responsabile del trattamento designa per iscritto un rappresentante nell'Unione.
2. L'obbligo di cui al paragrafo 1 del presente articolo non si applica:
 - a) al trattamento se quest'ultimo è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento; oppure
 - b) alle autorità pubbliche o agli organismi pubblici.

3. Il rappresentante è stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato.
4. Ai fini della conformità con il presente regolamento, il rappresentante è incaricato dal titolare del trattamento o dal responsabile del trattamento a fungere da interlocutore, in aggiunta o in sostituzione del titolare del trattamento o del responsabile del trattamento, in particolare delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.
5. La designazione di un rappresentante a cura del titolare del trattamento o del responsabile del trattamento fa salve le azioni legali che potrebbero essere promosse contro lo stesso titolare del trattamento o responsabile del trattamento.

Articolo 28

Responsabile del trattamento

1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.
2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.
3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:
 - a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
 - b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
 - c) adottino tutte le misure richieste ai sensi dell'articolo 32;
 - d) rispettino le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;
 - e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;
 - f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
 - g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e
 - h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

Articolo 29

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 30

Registri delle attività di trattamento

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

- a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;

- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:
- a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.
3. I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico.
4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.
5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Articolo 31

Cooperazione con l'autorità di controllo

Il titolare del trattamento, il responsabile del trattamento e, ove applicabile, il loro rappresentante cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

Sezione 2

Sicurezza dei dati personali

Articolo 32

Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;

- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

- a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) descrivere le probabili conseguenze della violazione dei dati personali;
- d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34

Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
 - a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
 - b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
 - c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Sezione 3

Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Articolo 35

Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
 - a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
 - b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
 - c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:
- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
 - una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
 - una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
 - le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.
11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Articolo 36

Consultazione preventiva

- Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.
- Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.
- Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:
 - ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
 - le finalità e i mezzi del trattamento previsto;
 - le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
 - ove applicabile, i dati di contatto del titolare della protezione dei dati;

- e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35;
 - f) ogni altra informazione richiesta dall'autorità di controllo.
4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.
5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

Sezione 4

Responsabile della protezione dei dati

Articolo 37

Designazione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:
 - a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
 - b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
 - c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.
2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.
3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.
4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.
5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.
6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.
7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Articolo 38

Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.
4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.
5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39

Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:
 - a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
 - b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
 - c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
 - d) cooperare con l'autorità di controllo; e
 - e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Sezione 5

Codici di condotta e certificazione

Articolo 40

Codici di condotta

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.
2. Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:
 - a) il trattamento corretto e trasparente dei dati;

- b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
- c) la raccolta dei dati personali;
- d) la pseudonimizzazione dei dati personali;
- e) l'informazione fornita al pubblico e agli interessati;
- f) l'esercizio dei diritti degli interessati;
- g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;
- h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;
- i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;
- j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; o
- k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

3. Oltre all'adesione ai codici di condotta approvati ai sensi del paragrafo 5 del presente articolo e aventi validità generale a norma del paragrafo 9 del presente articolo da parte di titolari o responsabili soggetti al presente regolamento, possono aderire a tali codici di condotta anche i titolari del trattamento o i responsabili del trattamento che non sono soggetti al presente regolamento ai sensi dell'articolo 3, al fine di fornire adeguate garanzie nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera e). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

4. Il codice di condotta di cui al paragrafo 2 del presente articolo contiene i meccanismi che consentono all'organismo di cui all'articolo 41, paragrafo 1, di effettuare il controllo obbligatorio del rispetto delle norme del codice da parte dei titolari del trattamento o dei responsabili del trattamento che si impegnano ad applicarlo, fatti salvi i compiti e i poteri delle autorità di controllo competenti ai sensi degli articoli 55 o 56.

5. Le associazioni e gli altri organismi di cui al paragrafo 2 del presente articolo che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice, la modifica o la proroga all'autorità di controllo competente ai sensi dell'articolo 55. L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate.

6. Qualora il progetto di codice, la modifica o la proroga siano approvati ai sensi dell'articolo 55, e se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice.

7. Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvare il progetto, la modifica o la proroga, l'autorità di controllo che è competente ai sensi dell'articolo 55 lo sottopone, tramite la procedura di cui all'articolo 63, al comitato, il quale formula un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 del presente articolo, sulla previsione di adeguate garanzie.

8. Qualora il parere di cui al paragrafo 7 confermi che il progetto di codice di condotta, la modifica o la proroga è conforme al presente regolamento o, nel caso di cui al paragrafo 3, fornisce adeguate garanzie, il comitato trasmette il suo parere alla Commissione.

9. La Commissione può decidere, mediante atti di esecuzione, che il codice di condotta, la modifica o la proroga approvati, che le sono stati sottoposti ai sensi del paragrafo 8 del presente articolo, hanno validità generale all'interno dell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

10. La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 9.
11. Il comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

Articolo 41

Monitoraggio dei codici di condotta approvati

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente.
2. L'organismo di cui al paragrafo 1 può essere accreditato a monitorare l'osservanza di un codice di condotta se esso ha:
 - a) dimostrato in modo convincente all'autorità di controllo competente di essere indipendente e competente riguardo al contenuto del codice;
 - b) istituito procedure che gli consentono di valutare l'ammissibilità dei titolari del trattamento e dei responsabili del trattamento in questione ad applicare il codice, di controllare che detti titolari e responsabili ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento;
 - c) istituito procedure e strutture atte a gestire i reclami relativi a violazioni del codice o il modo in cui il codice è stato o è attuato da un titolare del trattamento o un responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e
 - d) dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da esso svolti non danno adito a conflitto di interessi.
3. L'autorità di controllo competente presenta al comitato il progetto di criteri per l'accreditamento dell'organismo di cui al paragrafo 1 del presente articolo, ai sensi del meccanismo di coerenza di cui all'articolo 63.
4. Fatti salvi i compiti e i poteri dell'autorità di controllo competente e le disposizioni del capo VIII, un organismo di cui al paragrafo 1 del presente articolo adotta, stanti garanzie appropriate, le opportune misure in caso di violazione del codice da parte di un titolare del trattamento o responsabile del trattamento, tra cui la sospensione o l'esclusione dal codice del titolare del trattamento o del responsabile del trattamento. Esso informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.
5. L'autorità di controllo competente revoca l'accreditamento dell'organismo di cui al paragrafo 1, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate dall'organismo violano il presente regolamento.
6. Il presente articolo non si applica al trattamento effettuato da autorità pubbliche e da organismi pubblici.

Articolo 42

Certificazione

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

2. Oltre all'adesione dei titolari del trattamento o dei responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo, possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.
3. La certificazione è volontaria e accessibile tramite una procedura trasparente.
4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56.
5. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.
6. Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione di cui all'articolo 43 o, ove applicabile, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.
7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.
8. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

Articolo 43

Organismi di certificazione

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:
 - a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56;
 - b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio⁽¹⁾ conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56.
2. Gli organismi di certificazione di cui al paragrafo 1 sono accreditati in conformità di tale paragrafo solo se:
 - a) hanno dimostrato in modo convincente all'autorità di controllo competente di essere indipendenti e competenti riguardo al contenuto della certificazione;

⁽¹⁾ Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

- b) si sono impegnati a rispettare i criteri di cui all'articolo 42, paragrafo 5, e approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63;
- c) hanno istituito procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati;
- d) hanno istituito procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal titolare del trattamento o dal responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e
- e) hanno dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da loro svolti non danno adito a conflitto di interessi.
3. L'accreditamento degli organi di certificazione di cui ai paragrafi 1 e 2 del presente articolo ha luogo in base ai criteri approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63. In caso di accreditamento ai sensi del paragrafo 1, lettera b), del presente articolo, tali requisiti integrano quelli previsti dal regolamento (CE) n. 765/2008 nonché le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione.
4. Gli organismi di certificazione di cui al paragrafo 1 sono responsabili della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione soddisfi i requisiti.
5. L'organismo di certificazione di cui al paragrafo 1 trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta.
6. I requisiti di cui al paragrafo 3 del presente articolo e i criteri di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in forma facilmente accessibile. Le autorità di controllo provvedono a trasmetterli anche al comitato. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.
7. Fatto salvo il capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento di un organismo di certificazione di cui al paragrafo 1 del presente articolo, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il presente regolamento.
8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati di cui all'articolo 42, paragrafo 1.
9. La Commissione può adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

CAPO V

Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

Articolo 44

Principio generale per il trasferimento

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Articolo 45

Trasferimento sulla base di una decisione di adeguatezza

1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

2. Nel valutare l'adeguatezza del livello di protezione, la Commissione prende in considerazione in particolare i seguenti elementi:

- a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento;
- b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e
- c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.

3. La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, ove applicabile, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

4. La Commissione controlla su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate a norma del paragrafo 3 del presente articolo e delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE.

5. Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 del presente articolo mediante atti di esecuzione senza effetto retroattivo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2, o, in casi di estrema urgenza, secondo la procedura di cui all'articolo 93, paragrafo 3.

Per imperativi motivi di urgenza debitamente giustificati, la Commissione adotta atti di esecuzione immediatamente applicabili secondo la procedura di cui all'articolo 93, paragrafo 3.

6. La Commissione avvia consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla situazione che ha motivato la decisione di cui al paragrafo 5.

7. Una decisione ai sensi del paragrafo 5 del presente articolo lascia impregiudicato il trasferimento di dati personali verso il paese terzo, il territorio o uno o più settori specifici all'interno del paese terzo, o verso l'organizzazione internazionale in questione, a norma degli articoli da 46 a 49.

8. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato.

9. Le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della direttiva 95/46/CE restano in vigore fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al paragrafo 3 o 5 del presente articolo.

Articolo 46

Trasferimento soggetto a garanzie adeguate

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

- a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;
- b) le norme vincolanti d'impresa in conformità dell'articolo 47;
- c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
- d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;
- e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o
- f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

3. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1:

- a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o
- b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

4. L'autorità di controllo applica il meccanismo di coerenza di cui all'articolo 63 nei casi di cui al paragrafo 3 del presente articolo.

5. Le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della direttiva 95/46/CE restano valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo. Le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata conformemente al paragrafo 2 del presente articolo.

Articolo 47

Norme vincolanti d'impresa

1. L'autorità di controllo competente approva le norme vincolanti d'impresa in conformità del meccanismo di coerenza di cui all'articolo 63, a condizione che queste:

- a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;

- b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali; e
 - c) soddisfino i requisiti di cui al paragrafo 2.
2. Le norme vincolanti d'impresa di cui al paragrafo 1 specificano almeno:
- a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;
 - b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;
 - c) la loro natura giuridicamente vincolante, a livello sia interno che esterno;
 - d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;
 - e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;
 - f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;
 - g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14;
 - h) i compiti di qualunque responsabile della protezione dei dati designato ai sensi dell'articolo 35 o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami;
 - i) le procedure di reclamo;
 - j) i meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;
 - k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;
 - l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j);
 - m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e
 - n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

3. La Commissione può specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa ai sensi del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Articolo 48

Trasferimento o comunicazione non autorizzati dal diritto dell'Unione

Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.

Articolo 49

Deroghe in specifiche situazioni

1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

- a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
- b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
- c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
- d) il trasferimento sia necessario per importanti motivi di interesse pubblico;
- e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri.

Se non è possibile basare il trasferimento su una disposizione dell'articolo 45 o 46, comprese le disposizioni sulle norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni a norma del primo comma del presente paragrafo è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale sia ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare del trattamento informa del trasferimento l'autorità di controllo. In aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14, il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

2. Il trasferimento di cui al paragrafo 1, primo comma, lettera g), non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro. Se il registro è destinato a essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari.

3. Il primo comma, lettere a), b) e c), e il secondo comma del paragrafo 1 non si applicano alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.
4. L'interesse pubblico di cui al paragrafo 1, primo comma, lettera d), è riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento.
5. In mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri notificano tali disposizioni alla Commissione.
6. Il titolare del trattamento o il responsabile del trattamento attesta nel registro di cui all'articolo 30 la valutazione e le garanzie adeguate di cui al paragrafo 1, secondo comma, del presente articolo.

Articolo 50

Cooperazione internazionale per la protezione dei dati personali

In relazione ai paesi terzi e alle organizzazioni internazionali, la Commissione e le autorità di controllo adottano misure appropriate per:

- a) sviluppare meccanismi di cooperazione internazionale per facilitare l'applicazione efficace della legislazione sulla protezione dei dati personali;
- b) prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, in particolare mediante notificazione, deferimento dei reclami, assistenza alle indagini e scambio di informazioni, fatte salve garanzie adeguate per la protezione dei dati personali e gli altri diritti e libertà fondamentali;
- c) coinvolgere le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali;
- d) promuovere lo scambio e la documentazione delle legislazioni e prassi in materia di protezione dei dati personali, compresi i conflitti di giurisdizione con paesi terzi.

CAPO VI

Autorità di controllo indipendenti

Sezione 1

Indipendenza

Articolo 51

Autorità di controllo

1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»).
2. Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII.
3. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63.
4. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

*Articolo 52***Indipendenza**

1. Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente regolamento.
2. Nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dal presente regolamento, il membro o i membri di ogni autorità di controllo non subiscono pressioni esterne, né dirette, né indirette, e non sollecitano né accettano istruzioni da alcuno.
3. Il membro o i membri dell'autorità di controllo si astengono da qualunque azione incompatibile con le loro funzioni e per tutta la durata del mandato non possono esercitare alcuna altra attività incompatibile, remunerata o meno.
4. Ogni Stato membro provvede affinché ogni autorità di controllo sia dotata delle risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, compresi quelli nell'ambito dell'assistenza reciproca, della cooperazione e della partecipazione al comitato.
5. Ogni Stato membro provvede affinché ogni autorità di controllo selezioni e disponga di proprio personale, soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo interessata.
6. Ogni Stato membro provvede affinché ogni autorità di controllo sia soggetta a un controllo finanziario che non ne pregiudichi l'indipendenza e disponga di bilanci annuali, separati e pubblici, che possono far parte del bilancio generale statale o nazionale.

*Articolo 53***Condizioni generali per i membri dell'autorità di controllo**

1. Gli Stati membri dispongono che ciascun membro delle rispettive autorità di controllo sia nominato attraverso una procedura trasparente:
 - dal rispettivo parlamento;
 - dal rispettivo governo;
 - dal rispettivo capo di Stato; oppure
 - da un organismo indipendente incaricato della nomina a norma del diritto dello Stato membro.
2. Ogni membro possiede le qualifiche, l'esperienza e le competenze, in particolare nel settore della protezione dei dati personali, richieste per l'esercizio delle sue funzioni e dei suoi poteri.
3. Il mandato dei membri cessa alla scadenza del termine o in caso di dimissioni volontarie o di provvedimento d'ufficio, a norma del diritto dello Stato membro interessato.
4. Un membro è rimosso solo in casi di colpa grave o se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni.

*Articolo 54***Norme sull'istituzione dell'autorità di controllo**

1. Ogni Stato membro prevede con legge tutte le condizioni seguenti:
 - a) l'istituzione di ogni autorità di controllo;

- b) le qualifiche e le condizioni di idoneità richieste per essere nominato membro di ogni autorità di controllo;
- c) le norme e le procedure per la nomina del membro o dei membri di ogni autorità di controllo;
- d) la durata del mandato del membro o dei membri di ogni autorità di controllo non inferiore a quattro anni, salvo per le prime nomine dopo 24 maggio 2016, alcune delle quali possono avere una durata inferiore qualora ciò sia necessario per tutelare l'indipendenza dell'autorità di controllo mediante una procedura di nomina scaglionata;
- e) l'eventuale rinnovabilità e, in caso positivo, il numero di rinnovi del mandato del membro o dei membri di ogni autorità di controllo;
- f) le condizioni che disciplinano gli obblighi del membro o dei membri e del personale di ogni autorità di controllo, i divieti relativi ad attività, professioni e benefici incompatibili con tali obblighi durante e dopo il mandato e le regole che disciplinano la cessazione del rapporto di lavoro.

2. Il membro o i membri e il personale di ogni autorità di controllo sono tenuti, in virtù del diritto dell'Unione o degli Stati membri, al segreto professionale in merito alle informazioni riservate cui hanno avuto accesso nell'esecuzione dei loro compiti o nell'esercizio dei loro poteri, sia durante che dopo il mandato. Per tutta la durata del loro mandato, tale obbligo del segreto professionale si applica in particolare alle segnalazioni da parte di persone fisiche di violazioni del presente regolamento.

Sezione 2

Competenza, compiti e poteri

Articolo 55

Competenza

1. Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro.
2. Se il trattamento è effettuato da autorità pubbliche o organismi privati che agiscono sulla base dell'articolo 6, paragrafo 1, lettera c) o e), è competente l'autorità di controllo dello Stato membro interessato. In tal caso, non si applica l'articolo 56.
3. Le autorità di controllo non sono competenti per il controllo dei trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali.

Articolo 56

Competenza dell'autorità di controllo capofila

1. Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60.
2. In deroga al paragrafo 1, ogni autorità di controllo è competente per la gestione dei reclami a essa proposti o di eventuali violazioni del presente regolamento se l'oggetto riguarda unicamente uno stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro.
3. Nei casi indicati al paragrafo 2 del presente articolo, l'autorità di controllo informa senza indugio l'autorità di controllo capofila in merito alla questione. Entro un termine di tre settimane da quando è stata informata, l'autorità di controllo capofila decide se intende o meno trattare il caso secondo la procedura di cui all'articolo 60, tenendo conto dell'esistenza o meno di uno stabilimento del titolare del trattamento o responsabile del trattamento nello Stato membro dell'autorità di controllo che l'ha informata.

4. Qualora l'autorità di controllo capofila decida di trattare il caso, si applica la procedura di cui all'articolo 60. L'autorità di controllo che ha informato l'autorità di controllo capofila può presentare a quest'ultima un progetto di decisione. L'autorità di controllo capofila tiene nella massima considerazione tale progetto nella predisposizione del progetto di decisione di cui all'articolo 60, paragrafo 3.
5. Nel caso in cui l'autorità di controllo capofila decida di non trattarlo, l'autorità di controllo che ha informato l'autorità di controllo capofila tratta il caso conformemente agli articoli 61 e 62.
6. L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare del trattamento o responsabile del trattamento.

Articolo 57

Compiti

1. Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo:
 - a) sorveglia e assicura l'applicazione del presente regolamento;
 - b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;
 - c) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;
 - d) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;
 - e) su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dal presente regolamento e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri;
 - f) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 80, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;
 - g) collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento;
 - h) svolge indagini sull'applicazione del presente regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;
 - i) sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali;
 - j) adotta le clausole contrattuali tipo di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);
 - k) redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;
 - l) offre consulenza sui trattamenti di cui all'articolo 36, paragrafo 2;
 - m) incoraggia l'elaborazione di codici di condotta ai sensi dell'articolo 40, paragrafo 1, e fornisce un parere su tali codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma dell'articolo 40, paragrafo 5;
 - n) incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5;
 - o) ove applicabile, effettua un riesame periodico delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;

- p) definisce e pubblica i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;
 - q) effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;
 - r) autorizza le clausole contrattuali e le altre disposizioni di cui all'articolo 46, paragrafo 3;
 - s) approva le norme vincolanti d'impresa ai sensi dell'articolo 47;
 - t) contribuisce alle attività del comitato;
 - u) tiene registri interni delle violazioni del presente regolamento e delle misure adottate in conformità dell'articolo 58, paragrafo 2; e
 - v) svolge qualsiasi altro compito legato alla protezione dei dati personali.
2. Ogni autorità di controllo agevola la proposizione di reclami di cui al paragrafo 1, lettera f), tramite misure quali un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.
3. Ogni autorità di controllo svolge i propri compiti senza spese né per l'interessato né, ove applicabile, per il responsabile della protezione dei dati.
4. Qualora le richieste siano manifestamente infondate o eccessive, in particolare per il carattere ripetitivo, l'autorità di controllo può addebitare un contributo spese ragionevole basato sui costi amministrativi o rifiutarsi di soddisfare la richiesta. Incombe all'autorità di controllo dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Articolo 58

Poteri

1. Ogni autorità di controllo ha tutti i poteri di indagine seguenti:
- a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessita per l'esecuzione dei suoi compiti;
 - b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati;
 - c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
 - d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;
 - e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e
 - f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.
2. Ogni autorità di controllo ha tutti i poteri correttivi seguenti:
- a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;
 - b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
 - c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;

- d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
 - e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
 - f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
 - g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
 - h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
 - i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e
 - j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.
3. Ogni autorità di controllo ha tutti i poteri autorizzativi e consultivi seguenti:
- a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36;
 - b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali;
 - c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare;
 - d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5;
 - e) accreditare gli organismi di certificazione a norma dell'articolo 43;
 - f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5;
 - g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);
 - h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a);
 - i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b);
 - j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47.
4. L'esercizio da parte di un'autorità di controllo dei poteri attribuiti dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e degli Stati membri conformemente alla Carta.
5. Ogni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso.
6. Ogni Stato membro può prevedere per legge che la sua autorità di controllo abbia ulteriori poteri rispetto a quelli di cui ai paragrafi 1, 2 e 3. L'esercizio di tali poteri non pregiudica l'operatività effettiva del capo VII.

Articolo 59

Relazioni di attività

Ogni autorità di controllo elabora una relazione annuale sulla propria attività, in cui può figurare un elenco delle tipologie di violazioni notificate e di misure adottate a norma dell'articolo 58, paragrafo 2. Tali relazioni sono trasmesse al parlamento nazionale, al governo e alle altre autorità designate dal diritto dello Stato membro. Esse sono messe a disposizione del pubblico, della Commissione e del comitato.

CAPO VII

Cooperazione e coerenza

Sezione 1

Cooperazione*Articolo 60***Cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate**

1. L'autorità di controllo capofila coopera con le altre autorità di controllo interessate conformemente al presente articolo nell'impegno per raggiungere un consenso. L'autorità di controllo capofila e le autorità di controllo interessate si scambiano tutte le informazioni utili.
2. L'autorità di controllo capofila può chiedere in qualunque momento alle altre autorità di controllo interessate di fornire assistenza reciproca a norma dell'articolo 61 e può condurre operazioni congiunte a norma dell'articolo 62, in particolare per lo svolgimento di indagini o il controllo dell'attuazione di una misura riguardante un titolare del trattamento o responsabile del trattamento stabilito in un altro Stato membro.
3. L'autorità di controllo capofila comunica senza indugio le informazioni utili sulla questione alle altre autorità di controllo interessate. Trasmette senza indugio alle altre autorità di controllo interessate un progetto di decisione per ottenere il loro parere e tiene debitamente conto delle loro opinioni.
4. Se una delle altre autorità di controllo interessate solleva un'obiezione pertinente e motivata al progetto di decisione entro un termine di quattro settimane dopo essere stata consultata conformemente al paragrafo 3 del presente articolo, l'autorità di controllo capofila, ove non dia seguito all'obiezione pertinente e motivata o ritenga l'obiezione non pertinente o non motivata, sottopone la questione al meccanismo di coerenza di cui all'articolo 63.
5. L'autorità di controllo capofila, qualora intenda dare seguito all'obiezione pertinente e motivata sollevata, trasmette un progetto di decisione riveduto alle altre autorità di controllo interessate per ottenere il loro parere. Tale progetto di decisione riveduto è soggetto alla procedura di cui al paragrafo 4 entro un termine di due settimane.
6. Se nessuna delle altre autorità di controllo interessate ha sollevato obiezioni al progetto di decisione trasmesso dall'autorità di controllo capofila entro il termine di cui ai paragrafi 4 e 5, si deve considerare che l'autorità di controllo capofila e le autorità di controllo interessate concordano su tale progetto di decisione e sono da esso vincolate.
7. L'autorità di controllo capofila adotta la decisione e la notifica allo stabilimento principale o allo stabilimento unico del titolare del trattamento o responsabile del trattamento, a seconda dei casi, e informa le altre autorità di controllo interessate e il comitato la decisione in questione, compresa una sintesi dei fatti e delle motivazioni pertinenti. L'autorità di controllo cui è stato proposto un reclamo informa il reclamante riguardo alla decisione.
8. In deroga al paragrafo 7, in caso di archiviazione o di rigetto di un reclamo, l'autorità di controllo cui è stato proposto il reclamo adotta la decisione e la notifica al reclamante e ne informa il titolare del trattamento.
9. Se l'autorità di controllo capofila e le autorità di controllo interessate convengono di archiviare o rigettare parti di un reclamo e di intervenire su altre parti di tale reclamo, è adottata una decisione separata per ciascuna di tali parti della questione. L'autorità di controllo capofila adotta la decisione per la parte riguardante azioni in relazione al titolare del trattamento e la notifica allo stabilimento principale o allo stabilimento unico del responsabile del trattamento o del responsabile del trattamento sul territorio del suo Stato membro e ne informa il reclamante, mentre l'autorità di controllo del reclamante adotta la decisione per la parte riguardante l'archiviazione o il rigetto di detto reclamo, la notifica a detto reclamante e ne informa il titolare del trattamento o il responsabile del trattamento.
10. Dopo aver ricevuto la notifica della decisione dell'autorità di controllo capofila a norma dei paragrafi 7 e 9, il titolare del trattamento o responsabile del trattamento adotta le misure necessarie per garantire la conformità alla decisione per quanto riguarda le attività di trattamento nel contesto di tutti i suoi stabilimenti nell'Unione. Il titolare del trattamento o responsabile del trattamento notifica le misure adottate per conformarsi alla decisione all'autorità di controllo capofila, che ne informa le altre autorità di controllo interessate.

11. Qualora, in circostanze eccezionali, un'autorità di controllo interessata abbia motivo di ritenere che urga intervenire per tutelare gli interessi degli interessati, si applica la procedura d'urgenza di cui all'articolo 66.

12. L'autorità di controllo capofila e le altre autorità di controllo interessate si scambiano reciprocamente con mezzi elettronici, usando un modulo standard, le informazioni richieste a norma del presente articolo.

Articolo 61

Assistenza reciproca

1. Le autorità di controllo si scambiano le informazioni utili e si prestano assistenza reciproca al fine di attuare e applicare il presente regolamento in maniera coerente, e mettono in atto misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di autorizzazioni e consultazioni preventive e le richieste di effettuare ispezioni e indagini.

2. Ogni autorità di controllo adotta tutte le misure opportune necessarie per dare seguito alle richieste delle altre autorità di controllo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta. Tali misure possono consistere, in particolare, nella trasmissione di informazioni utili sullo svolgimento di un'indagine.

3. La richiesta di assistenza contiene tutte le informazioni necessarie, compresi lo scopo e i motivi della richiesta. Le informazioni scambiate sono utilizzate ai soli fini per cui sono state richieste.

4. L'autorità di controllo richiesta non deve rifiutare di dare seguito alla richiesta, salvo che:

- a) non sia competente per trattare l'oggetto della richiesta o per le misure cui deve dare esecuzione; o
- b) l'accoglimento della richiesta violi le disposizioni del presente regolamento o il diritto dell'Unione o dello Stato membro cui è soggetta l'autorità di controllo che riceve la richiesta.

5. L'autorità di controllo richiesta informa l'autorità di controllo richiedente dell'esito o, a seconda dei casi, dei progressi delle misure adottate per rispondere alla richiesta. L'autorità di controllo richiesta deve fornire le motivazioni del rigetto della richiesta.

6. Di norma, le autorità di controllo richieste forniscono con mezzi elettronici, usando un modulo standard, le informazioni richieste da altre autorità di controllo.

7. Le autorità di controllo richieste non impongono alcuna spesa per le misure da loro adottate a seguito di una richiesta di assistenza reciproca. Le autorità di controllo possono concordare disposizioni di indennizzo reciproco per spese specifiche risultanti dalla prestazione di assistenza reciproca in circostanze eccezionali.

8. Qualora l'autorità di controllo non fornisca le informazioni di cui al paragrafo 5 del presente articolo, entro un mese dal ricevimento della richiesta di un'altra autorità di controllo, l'autorità di controllo richiedente può adottare misure provvisorie nel territorio del suo Stato membro ai sensi dell'articolo 55, paragrafo 1. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 66, paragrafo 1, e che sia necessaria una decisione vincolante d'urgenza da parte del comitato a norma dell'articolo 66, paragrafo 2.

9. La Commissione può, mediante atti di esecuzione, specificare il formato e le procedure per l'assistenza reciproca di cui al presente articolo e le modalità per lo scambio di informazioni con mezzi elettronici tra autorità di controllo e tra le autorità di controllo e il comitato, in particolare il modulo standard di cui al paragrafo 6 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Articolo 62

Operazioni congiunte delle autorità di controllo

1. Se del caso, le autorità di controllo conducono operazioni congiunte, incluse indagini congiunte e misure di contrasto congiunte, cui partecipano membri o personale di autorità di controllo di altri Stati membri.

2. Qualora il titolare del trattamento o responsabile del trattamento abbia stabilimenti in vari Stati membri o qualora esista la probabilità che il trattamento abbia su un numero significativo di interessati in più di uno Stato membro un impatto negativo sostanziale, un'autorità di controllo di ogni Stato membro in questione ha il diritto di partecipare alle operazioni congiunte. L'autorità di controllo che è competente conformemente all'articolo 56, paragrafo 1, o all'articolo 56 paragrafo 4, invita l'autorità di controllo di ogni Stato membro interessato a partecipare all'operazione congiunta in questione e risponde senza ritardo alle richieste di partecipazione delle autorità di controllo.
3. Un'autorità di controllo può, in conformità del diritto degli Stati membri e con l'autorizzazione dell'autorità di controllo ospitata, conferire poteri, anche d'indagine, ai membri o al personale dell'autorità di controllo ospitata che partecipano alle operazioni congiunte o consentire ai membri o al personale dell'autorità di controllo ospitata, nella misura in cui il diritto dello Stato membro dell'autorità di controllo ospite lo permette, di esercitare i loro poteri d'indagine in conformità del diritto dello Stato membro dell'autorità di controllo ospitata. Tali poteri d'indagine possono essere esercitati unicamente sotto il controllo e in presenza di membri o personale dell'autorità di controllo ospite. I membri o il personale dell'autorità di controllo ospitata sono soggetti al diritto dello Stato membro dell'autorità di controllo ospite.
4. Qualora, in conformità del paragrafo 1, il personale di un'autorità di controllo ospitata operi in un altro Stato membro, lo Stato membro dell'autorità di controllo ospite si assume la responsabilità del suo operato, compreso l'obbligo di risarcimento, per i danni causati da detto personale nel corso delle operazioni, conformemente al diritto dello Stato membro nel cui territorio esso opera.
5. Lo Stato membro nel cui territorio sono stati causati i danni risarcisce tali danni alle condizioni applicabili ai danni causati dal proprio personale. Lo Stato membro dell'autorità di controllo ospitata il cui personale ha causato danni a terzi nel territorio di un altro Stato membro rimborsa integralmente a tale altro Stato membro importi corrisposti agli aventi diritto per conto di detti terzi.
6. Fatto salvo l'esercizio dei suoi diritti nei confronti di terzi e fatta eccezione per il paragrafo 5, ciascuno Stato membro rinuncia, nel caso previsto al paragrafo 1, a chiedere a un altro Stato membro il risarcimento dei danni di cui al paragrafo 4.
7. Qualora sia prevista un'operazione congiunta e un'autorità di controllo non si conformi entro un mese all'obbligo di cui al paragrafo 2, seconda frase, del presente articolo, le altre autorità di controllo possono adottare misure provvisorie nel territorio del loro Stato membro ai sensi dell'articolo 55. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 66, paragrafo 1, e che siano necessari un parere o una decisione vincolante d'urgenza da parte del comitato a norma dell'articolo 66, paragrafo 2.

Sezione 2

Coerenza

Articolo 63

Meccanismo di coerenza

Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione.

Articolo 64

Parere del comitato europeo per la protezione dei dati

1. Il comitato emette un parere ove un'autorità di controllo competente intenda adottare una delle misure in appresso. A tal fine, l'autorità di controllo competente comunica il progetto di decisione al comitato, quando la decisione:
 - a) è finalizzata a stabilire un elenco di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;
 - b) riguarda una questione di cui all'articolo 40, paragrafo 7, relativa alla conformità al presente regolamento di un progetto di codice di condotta o una modifica o proroga di un codice di condotta;

- c) è finalizzata ad approvare i criteri per l'accreditamento di un organismo ai sensi dell'articolo 41, paragrafo 3, o di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3;
- d) è finalizzata a determinare clausole tipo di protezione dei dati di cui all'articolo 46, paragrafo 2, lettera d), e all'articolo 28, paragrafo 8;
- e) è finalizzata ad autorizzare clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a); oppure
- f) è finalizzata ad approvare norme vincolanti d'impresa ai sensi dell'articolo 47.
2. Qualsiasi autorità di controllo, il presidente del comitato o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal comitato al fine di ottenere un parere, in particolare se un'autorità di controllo competente non si conforma agli obblighi relativi all'assistenza reciproca ai sensi dell'articolo 61 o alle operazioni congiunte ai sensi dell'articolo 62.
3. Nei casi di cui ai paragrafi 1 e 2, il comitato emette un parere sulla questione che gli è stata presentata, purché non abbia già emesso un parere sulla medesima questione. Tale parere è adottato entro un termine di otto settimane a maggioranza semplice dei membri del comitato. Tale termine può essere prorogato di sei settimane, tenendo conto della complessità della questione. Per quanto riguarda il progetto di decisione di cui al paragrafo 1 trasmesso ai membri del comitato conformemente al paragrafo 5, il membro che non abbia sollevato obiezioni entro un termine ragionevole indicato dal presidente è considerato assentire al progetto di decisione.
4. Senza ingiustificato ritardo, le autorità di controllo e la Commissione comunicano per via elettronica, usando un modulo standard, al comitato tutte le informazioni utili, in particolare, a seconda del caso, una sintesi dei fatti, il progetto di decisione, i motivi che rendono necessaria l'attuazione di tale misura e i pareri delle altre autorità di controllo interessate.
5. Il presidente del comitato informa, senza ingiustificato ritardo, con mezzi elettronici:
- a) i membri del comitato e la Commissione di tutte le informazioni utili che sono state comunicate al comitato con modulo standard. Se necessario, il segretariato del comitato fornisce una traduzione delle informazioni utili; e
- b) l'autorità di controllo di cui, secondo i casi, ai paragrafi 1 e 2, e la Commissione in merito al parere, che rende pubblico.
6. L'autorità di controllo competente si astiene dall'adottare il suo progetto di decisione di cui al paragrafo 1 entro il termine di cui al paragrafo 3.
7. L'autorità di controllo di cui al paragrafo 1 tiene nella massima considerazione il parere del comitato e, entro due settimane dal ricevimento del parere, comunica per via elettronica, usando un modulo standard, al presidente del comitato se intende mantenere o modificare il progetto di decisione e, se del caso, il progetto di decisione modificato.
8. Se entro il termine di cui al paragrafo 7 del presente articolo l'autorità di controllo interessata informa il presidente del comitato, fornendo le pertinenti motivazioni, che non intende conformarsi al parere del comitato, in tutto o in parte, si applica l'articolo 65, paragrafo 1.

Articolo 65

Composizione delle controversie da parte del comitato

1. Al fine di assicurare l'applicazione corretta e coerente del presente regolamento nei singoli casi, il comitato adotta una decisione vincolante nei seguenti casi:
- a) se, in un caso di cui all'articolo 60, paragrafo 4, un'autorità di controllo interessata ha sollevato un'obiezione pertinente e motivata a un progetto di decisione dell'autorità capofila o l'autorità capofila ha rigettato tale obiezione in quanto non pertinente o non motivata. La decisione vincolante riguarda tutte le questioni oggetto dell'obiezione pertinente e motivata, in particolare se sussista una violazione del presente regolamento;

- b) se vi sono opinioni contrastanti in merito alla competenza delle autorità di controllo interessate per lo stabilimento principale;
- c) se un'autorità di controllo competente non richiede il parere del comitato nei casi di cui all'articolo 64, paragrafo 1, o non si conforma al parere del comitato emesso a norma dell'articolo 64. In tal caso qualsiasi autorità di controllo interessata o la Commissione può comunicare la questione al comitato.
2. La decisione di cui al paragrafo 1 è adottata entro un mese dal deferimento della questione da parte di una maggioranza di due terzi dei membri del comitato. Tale termine può essere prorogato di un mese, in considerazione della complessità della questione. La decisione di cui al paragrafo 1 è motivata e trasmessa all'autorità di controllo capofila e a tutte le autorità di controllo interessate ed è per esse vincolante.
3. Qualora non sia stato in grado di adottare una decisione entro i termini di cui al paragrafo 2, il comitato adotta la sua decisione entro due settimane dalla scadenza del secondo mese di cui al paragrafo 2, a maggioranza semplice dei membri del comitato. In caso di parità di voti dei membri del comitato, prevale il voto del presidente.
4. Le autorità di controllo interessate non adottano una decisione sulla questione sottoposta al comitato a norma del paragrafo 1 entro i termini di cui ai paragrafi 2 e 3.
5. Il presidente del comitato notifica senza ingiustificato ritardo alle autorità di controllo interessate la decisione di cui al paragrafo 1 e ne informa la Commissione. La decisione è pubblicata senza ritardo sul sito web del comitato dopo che l'autorità di controllo ha notificato la decisione definitiva di cui al paragrafo 6.
6. L'autorità di controllo capofila o, se del caso, l'autorità di controllo a cui è stato proposto il reclamo adotta la sua decisione definitiva in base alla decisione di cui al paragrafo 1 del presente articolo senza ingiustificato ritardo e al più tardi entro un mese dalla notifica della decisione da parte del comitato. L'autorità di controllo capofila o, se del caso, l'autorità di controllo a cui è stato proposto il reclamo, informa il comitato circa la data in cui la decisione definitiva è notificata rispettivamente al titolare del trattamento o al responsabile del trattamento e all'interessato. La decisione definitiva delle autorità di controllo interessate è adottata ai sensi dell'articolo 60, paragrafi 7, 8 e 9. La decisione finale fa riferimento alla decisione di cui al paragrafo 1 del presente articolo e precisa che la decisione di cui a tale paragrafo sarà pubblicata sul sito web del comitato conformemente al paragrafo 5 del presente articolo. La decisione finale deve accludere la decisione di cui al paragrafo 1 del presente articolo.

Articolo 66

Procedura d'urgenza

1. In circostanze eccezionali, qualora ritenga che urga intervenire per proteggere i diritti e le libertà degli interessati, un'autorità di controllo interessata può, in deroga al meccanismo di coerenza di cui agli articoli 63, 64 e 65, o alla procedura di cui all'articolo 60, adottare immediatamente misure provvisorie intese a produrre effetti giuridici nel proprio territorio, con un periodo di validità determinato che non supera i tre mesi. L'autorità di controllo comunica senza ritardo tali misure e la motivazione della loro adozione alle altre autorità di controllo interessate, al comitato e alla Commissione.
2. Qualora abbia adottato una misura ai sensi del paragrafo 1 e ritenga che urga adottare misure definitive, l'autorità di controllo può chiedere un parere d'urgenza o una decisione vincolante d'urgenza del comitato, motivando tale richiesta.
3. Qualsiasi autorità di controllo può chiedere un parere d'urgenza o una decisione vincolante d'urgenza, a seconda dei casi, del comitato qualora un'autorità di controllo competente non abbia adottato misure adeguate in una situazione in cui urge intervenire per proteggere i diritti e le libertà degli interessati, motivando la richiesta di tale parere o decisione, in particolare l'urgenza dell'intervento.
4. In deroga all'articolo 64, paragrafo 3, e all'articolo 65, paragrafo 2, il parere d'urgenza o la decisione vincolante d'urgenza di cui ai paragrafi 2 e 3 del presente articolo sono adottati entro due settimane a maggioranza semplice dei membri del comitato.

*Articolo 67***Scambio di informazioni**

La Commissione può adottare atti di esecuzione di portata generale per specificare le modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato, in particolare il modulo standard di cui all'articolo 64.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Sezione 3

Comitato europeo per la protezione dei dati*Articolo 68***Comitato europeo per la protezione dei dati**

1. Il comitato europeo per la protezione dei dati («comitato») è istituito quale organismo dell'Unione ed è dotato di personalità giuridica.
2. Il comitato è rappresentato dal suo presidente.
3. Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.
4. Qualora, in uno Stato membro, più autorità di controllo siano incaricate di sorvegliare l'applicazione delle disposizioni del presente regolamento, è designato un rappresentante comune conformemente al diritto di tale Stato membro.
5. La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato comunica alla Commissione le attività del comitato.
6. Nei casi di cui all'articolo 65, il garante europeo della protezione dei dati ha diritto di voto solo per decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione che corrispondono nella sostanza a quelli del presente regolamento.

*Articolo 69***Indipendenza**

1. Nell'esecuzione dei suoi compiti o nell'esercizio dei suoi poteri ai sensi degli articoli 70 e 71, il comitato opera con indipendenza.
2. Fatte salve le richieste della Commissione di cui all'articolo 70, paragrafo 1, lettera b), e all'articolo 70, paragrafo 2, nell'esecuzione dei suoi compiti o nell'esercizio dei suoi poteri il comitato non sollecita né accetta istruzioni da alcuno.

*Articolo 70***Compiti del comitato**

1. Il comitato garantisce l'applicazione coerente del presente regolamento. A tal fine, il comitato, di propria iniziativa o, se del caso, su richiesta della Commissione, in particolare:
 - a) sorveglia il presente regolamento e ne assicura l'applicazione corretta nei casi previsti agli articoli 64 e 65 fatti salvi i compiti delle autorità nazionali di controllo;

- b) fornisce consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, comprese eventuali proposte di modifica del presente regolamento;
- c) fornisce consulenza alla Commissione sul formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa;
- d) pubblica linee guida, raccomandazioni e migliori prassi in materia di procedure per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico di cui all'articolo 17, paragrafo 2;
- e) esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del presente regolamento e pubblica linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del presente regolamento;
- f) pubblica linee guida, raccomandazioni e migliori pratiche conformemente alla lettera e) del presente paragrafo, per specificare ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione ai sensi dell'articolo 22, paragrafo 2;
- g) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, per accertare la violazione di dati personali e determinare l'ingiustificato ritardo di cui all'articolo 33, paragrafi 1 e 2, e le circostanze particolari in cui il titolare del trattamento o il responsabile del trattamento è tenuto a notificare la violazione dei dati personali;
- h) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, relative alle circostanze in cui una violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche di cui all'articolo 34, paragrafo 1;
- i) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, al fine di specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali basati sulle norme vincolanti d'impresa applicate, rispettivamente, dai titolari del trattamento e dai responsabili del trattamento, nonché gli ulteriori requisiti per assicurare la protezione dei dati personali degli interessati di cui all'articolo 47;
- j) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, al fine di specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali sulla base dell'articolo 49, paragrafo 1;
- k) elabora per le autorità di controllo linee guida riguardanti l'applicazione delle misure di cui all'articolo 58, paragrafi 1, 2 e 3, e la previsione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 83;
- l) valuta l'applicazione pratica delle linee guida, raccomandazioni e migliori prassi di cui alle lettere e) e f);
- m) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, per stabilire procedure comuni per le segnalazioni da parte di persone fisiche di violazioni del presente regolamento ai sensi dell'articolo 54, paragrafo 2;
- n) incoraggia l'elaborazione di codici di condotta e l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati ai sensi degli articoli 40 e 42;
- o) effettua l'accreditamento di organismi di certificazione e il suo riesame periodico a norma dell'articolo 43 e tiene un registro pubblico di organismi accreditati a norma dell'articolo 43, paragrafo 6, e dei titolari o responsabili del trattamento accreditati, stabiliti in paesi terzi a norma dell'articolo 42, paragrafo 7;
- p) specifica i requisiti di cui all'articolo 43, paragrafo 3, ai fini dell'accreditamento degli organismi di certificazione ai sensi dell'articolo 42;
- q) fornisce alla Commissione un parere in merito ai requisiti di certificazione di cui all'articolo 43, paragrafo 8;
- r) fornisce alla Commissione un parere in merito alle icone di cui all'articolo 12, paragrafo 7;
- s) fornisce alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale, così come per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione. A tal fine, la Commissione fornisce al comitato tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, con riguardo a tale paese terzo, territorio o settore specifico, o con l'organizzazione internazionale;

- t) emette pareri sui progetti di decisione delle autorità di controllo conformemente al meccanismo di coerenza di cui all'articolo 64, paragrafo 1, e sulle questioni presentate conformemente all'articolo 64, paragrafo 2, ed emette decisioni vincolanti ai sensi dell'articolo 65, anche nei casi di cui all'articolo 66;
 - u) promuove la cooperazione e l'effettivo scambio di informazioni e prassi tra le autorità di controllo a livello bilaterale e multilaterale;
 - v) promuove programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di organizzazioni internazionali;
 - w) promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo;
 - x) emette pareri sui codici di condotta redatti a livello di Unione a norma dell'articolo 40, paragrafo 9; e
 - y) tiene un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza.
2. Qualora chieda consulenza al comitato, la Commissione può indicare un termine, tenuto conto dell'urgenza della questione.
 3. Il comitato trasmette pareri, linee guida, raccomandazioni e migliori prassi alla Commissione e al comitato di cui all'articolo 93, e li pubblica.
 4. Se del caso, il comitato consulta le parti interessate e offre loro la possibilità di esprimere commenti entro un termine ragionevole. Fatto salvo l'articolo 76, il comitato rende pubblici i risultati della procedura di consultazione.

Articolo 71

Relazioni

1. Il comitato redige una relazione annuale sulla protezione delle persone fisiche con riguardo al trattamento nell'Unione e, se del caso, nei paesi terzi e nelle organizzazioni internazionali. La relazione è pubblicata ed è trasmessa al Parlamento europeo, al Consiglio e alla Commissione.
2. La relazione annuale include la valutazione dell'applicazione pratica delle linee guida, raccomandazioni e migliori prassi di cui all'articolo 70, paragrafo 1, lettera l), nonché delle decisioni vincolanti di cui all'articolo 65.

Articolo 72

Procedura

1. Il comitato decide a maggioranza semplice dei suoi membri, salvo se diversamente previsto dal presente regolamento.
2. Il comitato adotta il proprio regolamento interno deliberando a maggioranza di due terzi dei suoi membri e stabilisce le modalità del proprio funzionamento.

Articolo 73

Presidente

1. Il comitato elegge un presidente e due vicepresidenti tra i suoi membri a maggioranza semplice.
2. Il presidente e i vicepresidenti hanno un mandato di cinque anni, rinnovabile una volta.

*Articolo 74***Compiti del presidente**

1. Il presidente ha il compito di:
 - a) convocare le riunioni del comitato e stabilirne l'ordine del giorno;
 - b) notificare le decisioni adottate dal comitato a norma dell'articolo 65 all'autorità di controllo capofila e alle autorità di controllo interessate;
 - c) assicurare l'esecuzione tempestiva dei compiti del comitato, in particolare in relazione al meccanismo di coerenza di cui all'articolo 63.
2. Il comitato europeo stabilisce nel proprio regolamento interno la ripartizione dei compiti tra presidente e vicepresidenti.

*Articolo 75***Segreteria**

1. Il comitato dispone di una segreteria messa a disposizione dal garante europeo della protezione dei dati.
2. La segreteria svolge i propri compiti seguendo esclusivamente le istruzioni del presidente del comitato.
3. Il personale del garante europeo della protezione dei dati coinvolto nell'assolvimento dei compiti attribuiti al comitato dal presente regolamento è soggetto a linee gerarchiche separate rispetto al personale coinvolto nello svolgimento dei compiti attribuiti al garante europeo della protezione dei dati.
4. Se del caso, il comitato e il garante europeo della protezione dei dati stabiliscono e pubblicano un protocollo d'intesa che attua il presente articolo, stabilisce i termini della loro cooperazione e si applica al personale del garante europeo della protezione dei dati coinvolto nell'assolvimento dei compiti attribuiti al comitato dal presente regolamento.
5. La segreteria presta assistenza in materia di analisi, amministrativa e logistica al comitato.
6. La segreteria è incaricata in particolare:
 - a) della gestione ordinaria del comitato;
 - b) della comunicazione tra i membri del comitato, il suo presidente e la Commissione;
 - c) della comunicazione con le altre istituzioni e il pubblico;
 - d) dell'uso di mezzi elettronici per la comunicazione interna ed esterna;
 - e) della traduzione delle informazioni rilevanti;
 - f) della preparazione delle riunioni del comitato e del relativo seguito;
 - g) della preparazione, redazione e pubblicazione dei pareri, delle decisioni sulla composizione delle controversie tra le autorità di controllo e di altri testi adottati dal comitato.

*Articolo 76***Riservatezza**

1. Se il comitato europeo lo ritiene necessario, le sue deliberazioni hanno carattere riservato, come previsto dal suo regolamento interno.

2. L'accesso ai documenti trasmessi ai membri del comitato, agli esperti e ai rappresentanti di terzi è disciplinato dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ⁽¹⁾.

CAPO VIII

Mezzi di ricorso, responsabilità e sanzioni

Articolo 77

Diritto di proporre reclamo all'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.
2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

Articolo 78

Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ogni persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.
2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.
3. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.
4. Qualora siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

Articolo 79

Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.
2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

⁽¹⁾ Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GUL 145 del 31.5.2001, pag. 43).

*Articolo 80***Rappresentanza degli interessati**

1. L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82.
2. Gli Stati membri possono prevedere che un organismo, organizzazione o associazione di cui al paragrafo 1 del presente articolo, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79, qualora ritenga che i diritti di cui un interessato gode a norma del presente regolamento siano stati violati in seguito al trattamento.

*Articolo 81***Sospensione delle azioni**

1. L'autorità giurisdizionale competente di uno Stato membro che venga a conoscenza di azioni riguardanti lo stesso oggetto relativamente al trattamento dello stesso titolare del trattamento o dello stesso responsabile del trattamento pendenti presso un'autorità giurisdizionale in un altro Stato membro, prende contatto con tale autorità giurisdizionale nell'altro Stato membro per confermare l'esistenza delle azioni.
2. Qualora azioni riguardanti lo stesso oggetto relativamente al trattamento dello stesso titolare del trattamento o dello stesso responsabile del trattamento siano pendenti presso un'autorità giurisdizionale in un altro Stato membro, qualunque autorità giurisdizionale competente successivamente adita può sospendere le azioni.
3. Se tali azioni sono pendenti in primo grado, qualunque autorità giurisdizionale successivamente adita può parimenti dichiarare la propria incompetenza su richiesta di una delle parti a condizione che l'autorità giurisdizionale adita per prima sia competente a conoscere delle domande proposte e la sua legge consenta la riunione dei procedimenti.

*Articolo 82***Diritto al risarcimento e responsabilità**

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Articolo 83

Condizioni generali per infliggere sanzioni amministrative pecuniarie

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

- a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
- b) il carattere doloso o colposo della violazione;
- c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
- e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
- f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
- g) le categorie di dati personali interessate dalla violazione;
- h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
- i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
- j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
- k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;
- b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;
- c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

- a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
- b) i diritti degli interessati a norma degli articoli da 12 a 22;
- c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;
- d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;
- e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. L'esercizio da parte dell'autorità di controllo dei poteri attribuiti dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

Articolo 84

Sanzioni

1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

2. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

CAPO IX

Disposizioni relative a specifiche situazioni di trattamento

Articolo 85

Trattamento e libertà d'espressione e di informazione

1. Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria.

2. Ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono esenzioni o deroghe rispetto ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 2 e comunica senza ritardo ogni successiva modifica.

Articolo 86

Trattamento e accesso del pubblico ai documenti ufficiali

I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento.

Articolo 87

Trattamento del numero di identificazione nazionale

Gli Stati membri possono precisare ulteriormente le condizioni specifiche per il trattamento di un numero di identificazione nazionale o di qualsiasi altro mezzo d'identificazione d'uso generale. In tal caso, il numero di identificazione nazionale o qualsiasi altro mezzo d'identificazione d'uso generale sono utilizzati soltanto in presenza di garanzie adeguate per i diritti e le libertà dell'interessato conformemente al presente regolamento.

Articolo 88

Trattamento dei dati nell'ambito dei rapporti di lavoro

1. Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Articolo 89

Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il

rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

4. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi.

Articolo 90

Obblighi di segretezza

1. Gli Stati membri possono adottare norme specifiche per stabilire i poteri delle autorità di controllo di cui all'articolo 58, paragrafo 1, lettere e) e f), in relazione ai titolari del trattamento o ai responsabili del trattamento che sono soggetti, ai sensi del diritto dell'Unione o degli Stati membri o di norme stabilite dagli organismi nazionali competenti, al segreto professionale o a un obbligo di segretezza equivalente, ove siano necessarie e proporzionate per conciliare il diritto alla protezione dei dati personali e l'obbligo di segretezza. Tali norme si applicano solo ai dati personali che il titolare del trattamento o il responsabile del trattamento ha ricevuto o ha ottenuto in seguito a un'attività protetta da tale segreto professionale.

2. Ogni Stato membro notifica alla Commissione le norme adottate ai sensi del paragrafo 1 al più tardi entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Articolo 91

Norme di protezione dei dati vigenti presso chiese e associazioni religiose

1. Qualora in uno Stato membro chiese e associazioni o comunità religiose applichino, al momento dell'entrata in vigore del presente regolamento, *corpus* completi di norme a tutela delle persone fisiche con riguardo al trattamento, tali *corpus* possono continuare ad applicarsi purché siano resi conformi al presente regolamento.

2. Le chiese e le associazioni religiose che applicano i *corpus* completi di norme di cui al paragrafo 1 del presente articolo sono soggette al controllo di un'autorità di controllo indipendente che può essere specifica, purché soddisfi le condizioni di cui al capo VI del presente regolamento.

CAPO X

Atti delegati e atti di esecuzione

Articolo 92

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. La delega di potere di cui all'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, è conferita alla Commissione per un periodo indeterminato a decorrere 24 maggio 2016.
3. La delega di potere di cui all'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.
4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.
5. L'atto delegato adottato ai sensi dell'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di tre mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di tre mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 93

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.
2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.
3. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 8 del regolamento (UE) n. 182/2011 in combinato disposto con il suo articolo 5.

CAPO XI

Disposizioni finali

Articolo 94

Abrogazione della direttiva 95/46/CE

1. La direttiva 95/46/CE è abrogata a decorrere da 25 maggio 2018.
2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento.

Articolo 95

Rapporto con la direttiva 2002/58/CE

Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE.

*Articolo 96***Rapporto con accordi precedentemente conclusi**

Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali che comportano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali conclusi dagli Stati membri prima di 24 maggio 2016 e conformi al diritto dell'Unione applicabile prima di tale data.

*Articolo 97***Relazioni della Commissione**

1. Entro 25 maggio 2020 e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio relazioni di valutazione e sul riesame del presente regolamento.
2. Nel contesto delle valutazioni e del riesame del presente regolamento di cui al paragrafo 1, la Commissione esamina, in particolare, l'applicazione e il funzionamento:
 - a) del capo V sul trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, con particolare riguardo alle decisioni adottate ai sensi dell'articolo 45, paragrafo 3, del presente regolamento, e alle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE;
 - b) del capo VII su cooperazione e coerenza.
3. Ai fini del paragrafo 1, la Commissione può richiedere informazioni agli Stati membri e alle autorità di controllo.
4. Nello svolgere le valutazioni e i riesami di cui ai paragrafi 1 e 2, la Commissione tiene conto delle posizioni e delle conclusioni del Parlamento europeo, del Consiglio, nonché di altri organismi o fonti pertinenti.
5. Se del caso, la Commissione presenta opportune proposte di modifica del presente regolamento tenuto conto, in particolare, degli sviluppi delle tecnologie dell'informazione e dei progressi della società dell'informazione.

*Articolo 98***Riesame di altri atti legislativi dell'Unione in materia di protezione dei dati**

Se del caso, la Commissione presenta proposte legislative di modifica di altri atti legislativi dell'Unione in materia di protezione dei dati personali, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche con riguardo al trattamento. Ciò riguarda in particolare le norme relative alla protezione delle persone fisiche con riguardo al trattamento da parte di istituzioni, organi, uffici e agenzie dell'Unione e le norme sulla libera circolazione di tali dati.

*Articolo 99***Entrata in vigore e applicazione**

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.
2. Esso si applica a decorrere da 25 maggio 2018.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 27 aprile 2016

Per il Parlamento europeo

Il presidente

M. SCHULZ

Per il Consiglio

Il presidente

J.A. HENNIS-PLASSCHAERT

LEGGE 22 marzo 2019, n. 29

Istituzione e disciplina della Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza e del referto epidemiologico per il controllo sanitario della popolazione. (19G00036)

(GU n.81 del 5-4-2019)

Vigente al: 20-4-2019

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

Promulga

la seguente legge:

Art. 1

Istituzione della Rete nazionale dei registri
dei tumori e dei sistemi di sorveglianza

1. E' istituita la Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza dei sistemi sanitari regionali, identificati per ciascuna regione e provincia autonoma ai sensi del decreto del Presidente del Consiglio dei ministri 3 marzo 2017, pubblicato nella Gazzetta Ufficiale n. 109 del 12 maggio 2017, per le seguenti finalita':

a) coordinamento, standardizzazione e supervisione dei dati, alimentati direttamente dai flussi dei registri delle regioni e delle province autonome, nonche' validazione degli studi epidemiologici che discendono dall'istituzione di quanto previsto dall'articolo 4;

b) prevenzione, diagnosi, cura e riabilitazione, programmazione sanitaria, verifica della qualita' delle cure, valutazione dell'assistenza sanitaria;

c) messa in atto di misure di controllo epidemiologico delle malattie oncologiche e delle malattie infettive tumore-correlate;

d) studio dell'incidenza e della prevalenza delle malattie oncologiche e delle malattie infettive tumore-correlate, per poterne monitorare la diffusione e l'andamento;

e) sorveglianza epidemiologica per ridurre il rischio di introduzione o reintroduzione di malattie infettive, anche eliminate o sotto controllo;

f) prevenzione primaria e secondaria;

g) studio della morbosita' e mortalita' per malattie oncologiche e per malattie infettive tumore-correlate;

h) semplificazione delle procedure di scambio di dati, facilitazione della trasmissione degli stessi e loro tutela;

i) studio e monitoraggio dei fattori di rischio e dei fattori di protezione delle malattie sorvegliate;

l) promozione della ricerca scientifica in ambito oncologico, anche nel campo dei tumori rari;

m) monitoraggio dei fattori di rischio di origine professionale, anche attraverso forme di connessione e di scambio di dati con i sistemi informativi esistenti, con particolare riferimento al sistema informativo nazionale per la prevenzione nei luoghi di lavoro (SINP)

di cui all'articolo 8 del decreto legislativo 9 aprile 2008, n. 81, disciplinato dal regolamento di cui al decreto dei Ministri del lavoro e delle politiche sociali e della salute 25 maggio 2016, n. 183.

2. Entro dodici mesi dalla data di entrata in vigore della presente legge, con regolamento da adottare ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, su proposta del Ministro della salute, acquisito il parere del Garante per la protezione dei dati personali, previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le Province autonome di Trento e di Bolzano, sono individuati e disciplinati i dati che possono essere inseriti nella Rete di cui al comma 1, le modalita' relative al loro trattamento, i soggetti che possono avere accesso alla medesima Rete, i dati che possono essere oggetto dell'accesso stesso, le misure per la custodia e la sicurezza dei predetti dati nonche' le modalita' con cui e' garantito agli interessati, in ogni momento, l'esercizio dei diritti previsti dal regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016. Con il regolamento di cui al primo periodo si provvede altresì a semplificare e razionalizzare gli obblighi informativi, in armonia con quanto disposto dal decreto del Presidente del Consiglio dei ministri citato al comma 1 del presente articolo, nell'ambito di un sistema integrato ed unico di flussi di dati, evitando duplicazioni e sovrapposizioni di banche dati sanitarie.

3. Al fine dell'inserimento tempestivo, qualificato e sistematico dei dati nella Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza, le regioni e le Province autonome di Trento e di Bolzano assicurano l'invio dei flussi di dati prescritti secondo i tempi e i modi stabiliti dal regolamento di cui al comma 2, con validazione dei dati di competenza entro e non oltre il 30 aprile dell'anno successivo. I predetti adempimenti sono obbligatori e oggetto di verifica ai sensi dell'articolo 5 della presente legge.

4. Il titolare del trattamento dei dati contenuti nella Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza di cui al comma 1 e' il Ministero della salute.

5. Le attivita' e i compiti della Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza sono svolti nel rispetto dei seguenti principi:

a) i dati devono essere validati scientificamente secondo gli standard qualitativi previsti in sede internazionale dall'Agenzia internazionale per la ricerca sul cancro (IARC) dell'Organizzazione mondiale della sanita', relativi a casi diagnosticati di neoplasia;

b) i dati devono essere trattati per le finalita' di cui al comma 1 e allo scopo di: produrre dati di incidenza, mortalita', sopravvivenza, tipologia e prevalenza dei tumori; descrivere il rischio della malattia per sede e per tipo di tumore, per eta', per sesso; contribuire, attraverso i dati prodotti, alla rilevazione di eventuali differenze nell'accesso alle cure erogate al paziente oncologico in relazione alle condizioni socio-economiche e all'area geografica di provenienza, anche in riferimento a cause di malattia derivanti da inquinamento ambientale; effettuare analisi statistico-epidemiologiche, anche con riferimento ai tumori rari; fornire, a livello nazionale e regionale, un'informazione continua e completa alla popolazione, anche attraverso la pubblicazione dei dati nel sito internet istituzionale del Ministero della salute; monitorare l'efficacia dei programmi di screening oncologici tradizionali e sperimentali attivi e operativi presso le regioni e le Province autonome di Trento e di Bolzano; sostenere e monitorare gli studi epidemiologici finalizzati all'analisi dell'impatto dell'inquinamento ambientale sull'incidenza della patologia oncologica attraverso uno studio integrato sulle matrici ambientali e umane; valutare l'incidenza di fattori di carattere professionale sulla diffusione di patologie oncologiche; monitorare i trattamenti con farmaci dichiarati come innovativi, al fine di fornire nuove evidenze scientifiche sul loro grado di efficacia.

6. Per le finalita' della presente legge, il Ministro della salute puo' stipulare, sentito il Garante per la protezione dei dati personali, accordi di collaborazione a titolo gratuito con universita', con centri di ricerca pubblici e privati e con enti e

associazioni scientifiche che da almeno dieci anni operino, senza fini di lucro, nell'ambito dell'accreditamento dei sistemi di rilevazione dei tumori secondo standard nazionali e internazionali, della formazione degli operatori, della valutazione della qualità dei dati, della definizione dei criteri di realizzazione e di sviluppo di banche dati nazionali e dell'analisi e interpretazione dei dati, purché tali soggetti siano dotati di codici etici e di condotta che prevedano la risoluzione di ogni conflitto di interesse e improntino la loro attività alla massima trasparenza, anche attraverso la pubblicazione, nei rispettivi siti internet, degli statuti e degli atti costitutivi, della composizione degli organismi direttivi, dei bilanci, dei verbali e dei contributi e delle sovvenzioni a qualsiasi titolo ricevuti.

Art. 2

Partecipazione di enti del terzo settore all'attività della Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza.

1. Per le finalità della presente legge, il Ministro della salute può stipulare, sentito il Garante per la protezione dei dati personali, accordi di collaborazione a titolo gratuito con gli enti del terzo settore individuati dall'articolo 4, comma 1, del codice del Terzo settore, di cui al decreto legislativo 3 luglio 2017, n. 117, diversi dalle imprese sociali e dalle cooperative sociali, più rappresentativi e attivi nella tutela della salute umana e della prevenzione oncologica, con le associazioni attive nel campo dell'assistenza socio-sanitaria e con enti e associazioni attivi nella valutazione dell'impatto della patologia oncologica e della quantificazione dei bisogni assistenziali e nell'informazione e comunicazione sui rischi per la popolazione, purché tali soggetti siano dotati di codici etici e di condotta che prevedano la risoluzione di ogni conflitto di interesse e improntino la loro attività alla massima trasparenza, anche attraverso la pubblicazione, nei relativi siti internet, degli statuti e degli atti costitutivi, della composizione degli organismi direttivi, dei bilanci, dei verbali e dei contributi e delle sovvenzioni a qualsiasi titolo ricevuti. A tal fine, i soggetti di cui al presente comma si dotano, senza nuovi o maggiori oneri per la finanza pubblica, di un comitato scientifico composto da esperti in epidemiologia dei tumori e in oncologia, nonché da almeno un rappresentante di un registro dei tumori di popolazione, con il compito di garantire che le informazioni veicolate siano improntate al rispetto della metodologia scientifica ed epidemiologica.

2. Gli enti del terzo settore di cui al comma 1 possono presentare proposte al Ministro della salute in relazione a iniziative finalizzate allo sviluppo e alla valorizzazione dell'attività della Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza, fermo restando il rispetto degli standard scientifici. In caso di mancato accoglimento di tali proposte, il Ministro della salute fornisce alle organizzazioni e associazioni di cui al periodo precedente una risposta scritta e motivata, entro tre mesi dalla data di presentazione della proposta.

Art. 3

Modifica all'articolo 12 del decreto-legge
18 ottobre 2012, n. 179

1. All'articolo 12, comma 11, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, le parole: « sono aggiornati periodicamente con la stessa procedura » sono sostituite dalle seguenti: « sono aggiornati periodicamente con decreto del Ministro della salute, previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le Province autonome di Trento e di Bolzano e acquisito il parere del Garante per la protezione dei dati personali ».

Art. 4

Istituzione del referto epidemiologico

1. Al fine di garantire un controllo permanente dello stato di salute della popolazione, anche nell'ambito dei sistemi di sorveglianza, dei registri di mortalita', dei tumori e di altre patologie identificati ai sensi dell'articolo 12, comma 11, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, il Ministro della salute, acquisito il parere del Garante per la protezione dei dati personali, entro dodici mesi dalla data di entrata in vigore della presente legge, previa intesa in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le Province autonome di Trento e di Bolzano, adotta un decreto per l'istituzione del referto epidemiologico, per il controllo sanitario della popolazione con particolare attenzione alle aree piu' critiche del territorio nazionale, al fine di individuare i soggetti preposti alla raccolta e all'elaborazione dei dati che confluiscono nel referto epidemiologico e di disciplinare il trattamento, l'elaborazione, il monitoraggio continuo e l'aggiornamento periodico dei medesimi dati, nonche' la pubblicazione, con cadenza annuale, del referto epidemiologico, in particolare per quanto riguarda i dati relativi all'incidenza e alla prevalenza delle patologie che costituiscono piu' frequentemente causa di morte, nei siti internet delle regioni e delle Province autonome di Trento e di Bolzano, alle quali spetta il controllo quantitativo e qualitativo dei flussi di dati che alimentano il referto epidemiologico.

2. Ai fini della presente legge, per «referto epidemiologico» si intende il dato aggregato o macrodato corrispondente alla valutazione dello stato di salute complessivo di una comunita' che si ottiene da un esame epidemiologico delle principali informazioni relative a tutti i malati e a tutti gli eventi sanitari di una popolazione in uno specifico ambito temporale e in un ambito territoriale circoscritto o a livello nazionale, attraverso la valutazione dell'incidenza delle malattie, del numero e delle cause dei decessi, come rilevabili dalle schede di dimissione ospedaliera e dalle cartelle cliniche, al fine di individuare la diffusione e l'andamento di specifiche patologie e identificare eventuali criticita' di origine ambientale, professionale o socio-sanitaria.

Art. 5

Conferimento dei dati

1. L'obbligo di raccolta e di conferimento dei dati e di produzione dei flussi nei modi, nei termini e con la consistenza definiti ai sensi dei commi 2 e 3 dell'articolo 1, con particolare riferimento ai dati dei registri di patologia, di cui all'elenco A2) dell'allegato A al decreto del Presidente del Consiglio dei ministri citato al comma 1 dell'articolo 1, rappresenta un adempimento ai fini della verifica dell'erogazione dei livelli essenziali di assistenza (LEA) da parte del Comitato permanente per la verifica dell'erogazione dei livelli essenziali di assistenza e del Tavolo tecnico per la verifica degli adempimenti regionali, di cui agli articoli 9 e 12 dell'intesa 23 marzo 2005, sancita in sede di Conferenza permanente per i rapporti tra lo Stato, le regioni e le Province autonome di Trento e di Bolzano, pubblicata nel supplemento ordinario n. 83 alla Gazzetta Ufficiale n. 105 del 7 maggio 2005.

Art. 6

Relazione alle Camere

1. Entro dodici mesi dalla data di entrata in vigore della presente legge e successivamente entro il 30 settembre di ogni anno, il Ministro della salute trasmette una relazione alle Camere sull'attuazione della presente legge, con specifico riferimento al grado di raggiungimento delle finalita' per le quali e' stata istituita la Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza di cui all'articolo 1, nonche' sull'attuazione del referto epidemiologico di cui all'articolo 4. Nella relazione e'

fornita altresì l'illustrazione dettagliata del livello di attuazione della trasmissione dei dati da parte dei Centri di riferimento regionali di cui all'articolo 2 del decreto del Presidente del Consiglio dei ministri citato all'articolo 1, comma 1, della presente legge.

Art. 7

Clausola di invarianza finanziaria

1. Le amministrazioni interessate provvedono all'attuazione della presente legge nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente e, comunque, senza nuovi o maggiori oneri per la finanza pubblica.

Art. 8

Norme transitorie e finali

1. Entro centottanta giorni dalla data di entrata in vigore della presente legge, le regioni e le Province autonome di Trento e di Bolzano provvedono all'aggiornamento delle normative ivi vigenti in tema di sorveglianza sanitaria della malattia oncologica, in relazione alle disposizioni introdotte dalla presente legge, e adottano le necessarie iniziative affinché la sorveglianza epidemiologica sulla malattia oncologica, nelle aree territoriali di loro pertinenza non coperte alla data di entrata in vigore della presente legge, venga espletata dai registri dei tumori di popolazione già istituiti o di nuova istituzione.

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

Data a Roma, addì 22 marzo 2019

MATTARELLA

Conte, Presidente del Consiglio dei ministri

Visto, il Guardasigilli: Bonafede

PARTE PRIMA

Leggi e regolamenti regionali

REGOLAMENTO REGIONALE 18 gennaio 2023, n. 1

“Regolamento di organizzazione e funzionamento del Registro Tumori della regione Puglia (RTP)”.

IL PRESIDENTE DELLA GIUNTA REGIONALE:

VISTO l’art. 121 della Costituzione, così come modificato dalla legge costituzionale 22 novembre 1999 n. 1, nella parte in cui attribuisce al Presidente della Giunta Regionale l’emanazione dei regolamenti regionali;

VISTO l’art. 42, comma 2, lett. c) della L. R. 12 maggio 2004, n. 7 “Statuto della Regione Puglia”;

VISTO l’art. 44, comma 2, della L. R. 12 maggio 2004, n. 7 “Statuto del Regione Puglia” così come modificato dalla L.R. 20 ottobre 2014, n. 44;

VISTA la Delibera di Giunta Regionale N° 1968 DEL 22/12/2022 di adozione del Regolamento;

EMANA IL SEGUENTE REGOLAMENTO**Art. 1.
Definizioni**

1. Ai fini del presente Regolamento si applicano le definizioni di cui all’articolo 4 del Regolamento (UE) 679/2016 (GDPR).

2. In aggiunta a quanto previsto al comma 1, ai fini del presente Regolamento, si intende per:

a) Registro Tumori: il sistema attivo di raccolta continuativa e sistematica di dati personali anagrafici e sanitari dei casi diagnosticati e accertati di tumore che insorgono nei residenti nel territorio della regione Puglia, realizzato ai fini di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, nonché di elaborazione delle informazioni epidemiologiche e statistiche ai fini di programmazione, gestione, controllo e valutazione dell’assistenza sanitaria.

b) Tumore (neoplasia, cancro, malattia oncologica): malattia a carattere evolutivo, come descritta dai codici 140 – 239 della Classificazione Internazionale delle malattie e cause di morte IX Revisione ovvero dai codici C00-C97 e D00-D48 della Classificazione Internazionale delle Malattie e Cause di morte, X edizione, OMS, 1992, ovvero tutte le lesioni comprese nelle diverse edizioni e revisioni della Classificazione Internazionale delle Malattie per l’Oncologia (ICD-O).

c) Centro di Riferimento regionale: la struttura che cura la raccolta e l’analisi dei dati personali anagrafici e sanitari relativi a casi diagnosticati di neoplasia del territorio della regione Puglia previsti dall’art. 8 del presente regolamento e li ripartisce alle Sezioni Provinciali competenti per territorio, nei modi previsti al medesimo articolo. Il Centro di Riferimento assicura il coordinamento e l’omogeneità delle procedure di rilevazione e di elaborazione dei dati e fornisce supporto metodologico e informativo alle Sezioni Provinciali. Si occupa dell’elaborazione delle informazioni epidemiologiche e statistiche ai fini di programmazione, gestione, controllo e valutazione dell’assistenza sanitaria in campo oncologico.

d) Sezione provinciale: la struttura incardinata presso ogni Azienda Sanitaria Locale che, nei limiti dell'autonomia riconosciuta dal presente regolamento, analizza, codifica, registra ed elabora i dati, acquisiti secondo quanto previsto dall'articolo 8 del presente regolamento, concernenti i casi diagnosticati di neoplasia del territorio di competenza, analizzandoli a fini di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico.

Art. 2.

Oggetto del regolamento

1. Nell'ambito della finalità di rilevante interesse pubblico previste alle lettere v) e cc) del comma 2 dell'art. 2-sexies del D.lgs. 196/2003, il presente Regolamento, ai sensi della legge regionale n. 16/2011, articolo 3, disciplina le specifiche finalità perseguite dal Registro Tumori, i tipi di dati sensibili trattati e le operazioni eseguibili, i soggetti che possono trattare i dati medesimi, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Art. 3.

Finalità specifiche del trattamento di dati

1. Nell'ambito degli scopi di ricerca scientifica di cui all'art. 2, il Registro Tumori è finalizzato a:

- a) produrre misure di incidenza, mortalità, sopravvivenza e prevalenza dei tumori;
- b) descrivere il rischio della malattia per sede e per tipo di tumore, età, genere ed ogni altra variabile di interesse per la ricerca scientifica;
- c) svolgere studi epidemiologici sugli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio dei tumori, sugli esiti degli interventi di diagnosi precoce, delle terapie e dei percorsi diagnostico-terapeutici, anche in collaborazione con altri enti e strutture regionali, nazionali e internazionali di ricerca scientifica in campo epidemiologico;
- d) produrre dati anonimi e aggregati per la programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, inerente gli interventi di prevenzione primaria e secondaria rivolti alle persone ed all'ambiente di vita e lavoro, nonché dell'efficacia dei programmi di screening;
- e) monitorare e valutare i dati relativi all'accesso e alla qualità dei servizi diagnostici e terapeutici, alla sopravvivenza dei pazienti affetti da cancro, fornendo confronti con altre regioni o paesi e indicazioni utili alla programmazione sanitaria;
- f) monitorare e valutare i dati relativi all'appropriatezza e qualità dei servizi diagnostici terapeutici, alla sopravvivenza dei pazienti affetti da cancro.

2. Ciascuna Sezione Provinciale può trattare i dati personali per le medesime finalità di cui sopra, limitatamente alla popolazione residente, assistibile o dimorante in maniera stabile nel territorio di pertinenza.

Art. 4.

Titolare del trattamento dei dati

1. Titolare del trattamento dei dati limitatamente alle funzioni previste del presente regolamento e dall'art. 3 comma 1 lett. p) della legge regionale n.29/2017, è l'Agenzia regionale strategica per la Salute e il Sociale (AReSS) della Regione Puglia presso cui è istituito il Centro di Riferimento del Registro Tumori Puglia.
2. Nell'ambito delle finalità di cui all'art. 3, l'AReSS Puglia garantisce la gestione amministrativa, tecnica ed informatica del Registro Tumori Puglia e il suo coordinamento tecnico-operativo.
3. Alle eventuali richieste di dati e informazioni provenienti da Enti, Organismi, Autorità pubbliche o dalle

articolazioni della Regione Puglia o di enti/soggetti terzi che ne abbiano legittimo interesse, il Centro di Riferimento del Registro Tumori Puglia fornisce riscontro elaborando e trasmettendo esclusivamente dati aggregati in forma rigorosamente anonima, anche con il supporto delle Sezioni Provinciali.

4. I Responsabili e/o autorizzati al trattamento dei dati sono designati dal Titolare esclusivamente nell'ambito delle strutture del Centro di Riferimento del Registro Tumori Puglia (CRT) e delle Sezioni Provinciali del Registro Tumori (SPRT).

Art. 5

Organizzazione del registro

1. Il Registro Tumori, per le finalità di cui all'articolo 3, è implementato dai dati provenienti dalle seguenti Sezioni Provinciali del Registro Tumori Puglia:

- a) Sezione Provinciale dell'ASL BA;
- b) Sezione Provinciale dell'ASL BR;
- c) Sezione Provinciale dell'ASL BT;
- d) Sezione Provinciale dell'ASL TA;
- e) Sezione Provinciale dell'ASL FG;
- f) Sezione Provinciale dell'ASL LE;

2. Le Sezioni Provinciali contribuiscono ad alimentare la base dati del Registro tumori regionale effettuando la ricerca, i controlli di eleggibilità, la codifica e l'inserimento dei casi incidenti nel territorio di competenza, aggiornando periodicamente la storia clinica, la sopravvivenza e la mortalità dei pazienti, garantendo il massimo livello di accuratezza dei dati attraverso periodici controlli di qualità e collaborando all'attività epidemiologica del Registro stesso.

Art. 6.

Tipi di dati sensibili trattati

1. Per il perseguimento delle finalità di cui all'articolo 3, il Titolare del trattamento del Registro Tumori tratta dati relativi alla salute riferiti a casi diagnosticati di tumore, nei limiti di quanto indispensabile per il raggiungimento delle predette finalità e nei modi previsti all'articolo 13 del presente Regolamento, nel rispetto delle prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica specificate nell'allegato 5 al Provvedimento del Garante per la protezione dei dati personali n. 146 del 5 giugno 2019, recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101, nonché nel rispetto delle regole deontologiche e delle misure di garanzia ai sensi degli articoli 2-quater, 2-septies e , Allegato A4 al Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni.

2. Il Titolare del trattamento del Registro Tumori tratta i seguenti dati:

- a) diagnosi e modalità di ammissione e dimissione, relative a ricoveri e a prestazioni ambulatoriali diagnostico terapeutiche e rispettivi D.R.G. (Diagnosis Related Groups);
- b) anamnesi;
- c) interventi chirurgici e procedure diagnostiche e terapeutiche, ivi compresi gli screening oncologici;
- d) indagini cliniche e trattamenti eseguiti;
- e) referti di anatomia patologica;
- f) data e causa di morte e condizioni morbose rilevanti per il decesso.

Art. 7.

Fonti dei dati

1. Il titolare del trattamento del Registro Tumori effettua la raccolta dei dati riferiti a pazienti con diagnosi di tumore di cui all'articolo 6, comma 2, con le modalità e nel rispetto delle misure tecniche e organizzative di cui all'articolo 11 e dettagliate nel Disciplinare tecnico, presso:

A. l'archivio regionale/provinciale delle Schede di dimissioni ospedaliere (SDO), contenenti diagnosi di tumore o relative ai soggetti iscritti o da iscrivere nel Registro Tumori, al fine di individuare nuovi casi non registrati ovvero, ove necessario, verificare i dati già inseriti nel Registro medesimo.

B. i seguenti archivi delle Aziende Sanitarie Locali, delle Aziende Ospedaliere-Universitarie, degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) pubblici e privati e delle strutture sanitarie private accreditate, limitatamente alle informazioni ivi contenute correlate alle patologie tumorali, al fine di implementare il Registro con riferimento ai casi segnalati ed aggiornare il Registro Tumori con l'inserimento di eventuali ulteriori casi:

a) archivi delle schede di morte relativamente ai soggetti con diagnosi di neoplasia definita dal Registro tumori e ai soggetti con neoplasia come causa di morte o condizione morbosa rilevante per il decesso;

b) archivi delle cartelle cliniche;

c) archivi di Anatomia Patologica;

d) archivi di laboratorio e di radiodiagnostica;

e) archivi delle prestazioni ambulatoriali;

f) archivi delle prescrizioni farmaceutiche;

g) archivi delle esenzioni ticket per patologia oncologica;

h) archivi delle protesi di interesse oncologico;

i) archivi delle prestazioni di riabilitazione di interesse oncologico;

l) archivio delle vaccinazioni di interesse oncologico;

m) lettere di dimissioni ospedaliere e relazioni cliniche.

C. l'Anagrafe Sanitaria regionale degli Assistiti per effettuare il raffronto dei dati anagrafici dei soggetti iscritti o da iscrivere nel Registro Tumori con i dati anagrafici contenuti nella predetta Anagrafe, al fine di verificarne ove necessario l'esattezza e l'aggiornamento dei dati e individuare eventuali duplicazioni.

2. I soggetti individuati al comma 1 devono trasmettere le informazioni di cui all'art. 6 comma 2 secondo le modalità specificate ai sensi del Disciplinare tecnico previsto dall'art. 11 del presente regolamento.

Art. 8

Comunicazione dei dati

1. Il Titolare del trattamento del Registro Tumori, per le finalità di cui all'articolo 3, può comunicare le informazioni di cui all'articolo 6, comma 2, ai Titolari del trattamento dei dati dei Registri Tumori di altre Regioni, qualora legittimamente istituiti e regolamentati ai sensi dell'art. 2-sexies del Decreto Legislativo 30 giugno 2003, n.196 e previa stipula di apposita convenzione che definisca le modalità tecniche di trasmissione dei dati medesimi in conformità alle misure di sicurezza individuate nell'Allegato 2 del Prov. del Garante per la protezione dei dati personali n. 393 del 2 luglio 2015 – pubblicato sulla G.U. n. 179 del 4 agosto 2015, nel rispetto dell'articolo 110 del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, nonché delle "Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica" specificate nell'allegato 5 al Provvedimento del Garante per la protezione dei dati personali n. 146 del 5 giugno 2019 recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101. Tali modalità devono garantire un livello di sicurezza equivalente a quello

assicurato dalle misure specificate nel Disciplinare Tecnico previsto dall'art. 11 del presente regolamento.

2. Il Titolare del trattamento del Registro Tumori, per l'esclusivo perseguimento delle finalità di cui al precedente articolo 3, può svolgere studi in campo medico, biomedico ed epidemiologico, anche in collaborazione con Università, Enti ed Istituti di ricerca e società scientifiche, nonché con ricercatori, singoli o associati, che operano nell'ambito delle predette Università, Enti ed Istituti di ricerca e società scientifiche, nel rispetto delle regole previste dal Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici di cui all'allegato A.4 al Decreto Legislativo 30 giugno 2003 n. 196.

Art. 9.

Diffusione dei dati

1. Il Titolare del trattamento dei dati del Registro Tumori, per le finalità di cui all'articolo 3, può diffondere, anche attraverso le Sezioni Provincia e mediante pubblicazione, dati anonimi relativi ai casi registrati in forma esclusivamente aggregata oppure secondo modalità che non rendano identificabili i soggetti interessati.

Art. 10.

Operatori del Registro Tumori

1. I dati personali contenuti nel Registro Tumori sono trattati nel rispetto dei generali principi di liceità, correttezza e trasparenza di cui all'art. 5 del RGDP, soltanto da personale appositamente individuato dal Titolare del trattamento, in conformità all'art. 29 del RGDP e dell'art. 2-*quaterdecies* del decreto legislativo n.196/2003, e sottoposto a regole di condotta analoghe al segreto professionale stabilite dal Titolare del trattamento qualora non sia tenuto per legge al segreto professionale.

2. I soggetti di cui al comma 1 accedono ai dati del Registro Tumori secondo modalità e logiche di elaborazione strettamente pertinenti e non eccedenti ai compiti attribuiti a ciascuno di essi.

Art. 11.

Misure di sicurezza

1. Il titolare del trattamento dei dati contenuti nel Registro Tumori adotta misure tecniche e organizzative individuate ai sensi degli articoli 25 e 32 del Regolamento (UE) 2016/679, anche a seguito di un'adeguata valutazione d'impatto sulla protezione dei dati condotta ai sensi dell'art. 35 del medesimo Regolamento e specificate nel Disciplinare Tecnico contenuto nell'allegato A), che forma parte integrante del presente regolamento.

2. La sicurezza dei dati trattati dal Registro Tumori deve essere garantita in tutte le fasi del trattamento dei dati, mediante l'adozione degli opportuni accorgimenti volti a preservare i medesimi dati da rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 12.

Conservazione dei dati trattati

1. Il Titolare del trattamento prevede congrui e proporzionati termini di conservazione dei dati inseriti nel

Registro o comunque trattati, in conformità al principio di “limitazione della conservazione” di cui all’articolo 5, par. 1, lett. e), del Regolamento (UE) come dettagliato nel Disciplinare Tecnico che forma parte integrante del presente regolamento.

Art. 13.

Codifica dei dati trattati

1. I dati relativi alla salute contenuti nel Registro Tumori, tenuti con l’ausilio di strumenti elettronici, sono trattati mediante l’utilizzo di tecniche di pseudonimizzazione, anche con il ricorso a codici identificativi, nel rispetto di quanto stabilito dal Disciplinare tecnico contenuto nell’allegato A e di quanto previsto dal Decreto del Ministero della Salute 7 dicembre 2016, n. 262 recante «Regolamento recante procedure per l’interconnessione a livello nazionale dei sistemi informativi su base individuale del Servizio sanitario nazionale, anche quando gestiti da diverse amministrazioni dello Stato», in modo tale da tutelare l’identità e la riservatezza degli interessati nel trattamento dei dati, rendendoli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità.
2. I dati relativi alla salute sono trasmessi al Registro e conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 1 anche quando sono tenuti senza l’ausilio di strumenti elettronici.

Art. 14.

Informativa agli interessati

1. Il Titolare del trattamento dei dati del Registro Tumori deve fornire l’informativa agli interessati per il tramite delle strutture del Servizio Sanitario Regionale, pubbliche o private accreditate che erogano le prestazioni sanitarie, nelle modalità previste dagli art.13 e 14 del Regolamento UE 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/64/CE ed è tenuto a garantire agli interessati il pieno e tempestivo esercizio dei diritti previsti da tali articoli.

Art. 15.

Data breach

1. Sono comunicate al Garante, entro settantadue ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali oggetto di trattamento per la tenuta e il funzionamento del Registro Tumori (c.d. data breach) con le modalità previste dall’articolo 33 del Regolamento UE 2016/679. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica le violazioni all’interessato senza ingiustificato ritardo, con le modalità previste dall’art.34 del Regolamento UE 2016/679.

Art. 16.

Risorse finanziarie

1. Il Registro Tumori Regionale può disporre dei seguenti fondi:

- finanziamenti specifici regionali;
- finanziamenti derivanti da progetti di ricerca;
- ogni altro fondo specificamente destinato per legge, o per disposizione delle Istituzioni Sanitarie di riferimento, al Registro Tumori Regionale.

Art. 17.

Norme transitorie

1. L'adeguamento e l'adozione delle modalità tecniche e delle misure di sicurezza di cui al Disciplinare Tecnico previsto dall'articolo 11, devono avvenire entro 180 giorni dall'entrata in vigore del presente Regolamento.

Art. 18.

Entrata in vigore

1. Il presente regolamento è pubblicato sul Bollettino Ufficiale della Regione Puglia ai sensi e per gli effetti dell'art.53 comma 1 della L.R. 12/05/2004, n. 7 "Statuto della Regione Puglia".
2. È fatto obbligo a chiunque spetti di osservarlo e farlo osservare come regolamento della Regione Puglia.

Il presente Regolamento è pubblicato sul Bollettino Ufficiale della Regione Puglia ai sensi e per gli effetti dell'art. 53 comma 1 della L.R. 12/05/2004, n. 7 "Statuto della Regione Puglia". E' fatto obbligo a chiunque spetti di osservarlo e farlo osservare come Regolamento della Regione Puglia.

Dato a Bari, addì 18 gennaio 2023

EMILIANO



REGIONE PUGLIA

DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA PER IL FUNZIONAMENTO DEL REGISTRO TUMORI PUGLIA

PREMESSA

Il presente Disciplinare specifica le misure tecniche e organizzative di cui agli articoli 25 e 32 del Regolamento (UE) 679/2016, da verificare periodicamente da parte del titolare del trattamento, anche a seguito di una valutazione d'impatto sulla protezione dei dati effettuata ai sensi dell'articolo 35 del medesimo Regolamento.

Il presente Disciplinare specifica:

A) le modalità tecniche di raccolta dei dati di cui all'art. 6 comma 2 presso gli archivi individuati all'articolo 7 del Regolamento, che può avvenire mediante:

a) invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web (web services) o cooperazione applicativa);

b) accesso diretto degli incaricati del Registro Tumori ai sistemi informatici delle strutture sanitarie di cui all'articolo 7 del Regolamento;

c) trasmissione su supporti informatici (es. CD, DVD, memorie a stato solido);

d) trasmissione di documenti cartacei in plico chiuso e sigillato nelle more della messa a regime delle modalità di cui alle lettere a), b) e c).

I supporti di cui alla lettera c) e d) sono utilizzati esclusivamente per estrapolare i dati da inserire nel Registro Tumori.

B) le misure di sicurezza che:

a) il Titolare del trattamento del Registro Tumori deve adottare nella tenuta e per il funzionamento del registro medesimo;

b) le strutture presso le quali sono raccolti i dati che alimentano il Registro Tumori, quali la Regione le Aziende sanitarie territoriali e ospedaliere, gli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) nonché le strutture sanitarie private accreditate, devono adottare per comunicare o mettere a disposizione i dati al Titolare del trattamento.

DISPOSIZIONI GENERALI

Il Titolare del trattamento del Registro Tumori istruisce gli autorizzati, individuati ai sensi dell'art. 29 del GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003, sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina in materia di protezione dei dati personali più rilevanti in rapporto alle relative attività, nonché sulle responsabilità che ne derivano.

La sicurezza dei dati contenuti nel Registro Tumori deve essere garantita in tutte le fasi del trattamento dei dati, adottando opportuni accorgimenti che preservino i medesimi dati da



REGIONE PUGLIA

rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. A tal fine si utilizzano tecniche crittografiche con chiavi di cifratura di lunghezza adeguata alla dimensione e al ciclo di vita dei dati sensibili e si garantisce, ove le finalità non richiedano il loro utilizzo, la separazione dei dati anagrafici da quelli sanitari.

Le postazioni di lavoro informatiche utilizzate per il trattamento dei dati necessari per la tenuta e il funzionamento del Registro Tumori, sono dotate di:

- a) sistemi antivirus e antimalware costantemente aggiornati;
- b) sistemi di protezione perimetrale, costantemente attivati e adeguatamente configurati in funzione del contesto operativo (firewall);
- c) software di base e applicativo costantemente aggiornato.

1. FASE DI RACCOLTA DATI

La raccolta dei dati presso le banche dati e gli archivi di cui all'art. 7 del Regolamento deve in ogni caso conformarsi alle seguenti modalità:

1.1. Il Titolare del trattamento del Registro Tumori raccoglie con periodicità almeno semestrale dall'archivio regionale delle Schede di dimissioni ospedaliere (SDO) della Regione i dati necessari all'individuazione dei casi diagnosticati di tumore oppure, ove necessario, alla verifica dei dati già presenti nel Registro Tumori. Verifica, inoltre, l'esattezza e l'aggiornamento dei dati anagrafici dei soggetti iscritti o da iscrivere nel Registro Tumori mediante il raffronto con i dati contenuti nell'Anagrafe Sanitaria Regionale degli Assistibili:

- a) garantire l'accesso selettivo ai soli dati di cui all'articolo 6 comma 2 del Regolamento;
- b) assegnare al personale incaricato del trattamento credenziali di autenticazione e profili di autorizzazione specifici alle attività di consultazione e raffronto;
- c) predisporre strumenti e procedure per il meccanismo di autorizzazione e autenticazione del personale incaricato al trattamento dei dati nonché per delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati garantendo che:

c.1 la raccolta dei dati avvengano soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP del Titolare del trattamento del Registro Tumori o dotate di certificato digitale, emesso da una Certification Authority ufficiale, che identifichi univocamente la postazione di lavoro;

c.2 laddove la raccolta dei dati avvenga secondo le modalità della cooperazione applicativa, in forma di web services, le condizioni d'uso di tali servizi, che devono individuare idonee garanzie per il trattamento dei dati personali, siano trasposte in appositi accordi di servizio, secondo le specifiche tecniche del Sistema pubblico di connettività (SPC) istituito dal Codice dell'Amministrazione Digitale;



REGIONE PUGLIA

c.3 laddove invece la raccolta dei dati avvenga attraverso l'utilizzo di applicazioni web su Internet, vengano impiegati canali di trasmissione protetti (protocolli https/ssl); siano visualizzabili le informazioni relative alla sessione corrente e all'ultima sessione effettuata con le stesse credenziali (con l'indicazione almeno di data, ora e indirizzo di rete da cui è effettuata la connessione); sia asseverata l'identità digitale dei server erogatori di servizi, tramite l'utilizzo di certificati digitali emessi da una Certification Authority iscritta all'elenco nazionale dei certificatori attivi;

c.4 nella fase transitoria di cui all'articolo 17 del Regolamento, necessaria per l'adeguamento tecnologico, la password venga consegnata al singolo incaricato separatamente rispetto al codice per l'identificazione e sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi;

c.5 siano utilizzati sistemi di autenticazione a più fattori per l'abilitazione degli incaricati del registro all'accesso telematico agli archivi delle strutture sanitarie individuate dall'art.7, comma 2, del Regolamento, per estrapolare i dati destinati ad alimentare e ad aggiornare il Registro stesso;

c.6 sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;

c.7 sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;

c.8 siano disattivate le credenziali di autenticazione non utilizzate da almeno sei mesi;
d) effettuare periodiche verifiche, anche a fronte di cambiamenti organizzativi o eventi anomali, circa la sussistenza dei presupposti che hanno originato l'abilitazione degli incaricati. Eventuali esiti negativi delle predette verifiche, devono dar luogo alla tempestiva revisione del profilo di abilitazione, alla eventuale disabilitazione dello stesso o alla disattivazione delle credenziali;

e) prevedere la registrazione in appositi file di log, ai fini della verifica della correttezza e legittimità del trattamento dei dati, delle seguenti informazioni: il soggetto (codice identificativo) che ha effettuato l'accesso, la data e l'ora dell'accesso, l'operazione effettuata, l'indirizzo IP della postazione di lavoro e del server interconnesso, i dati trattati). Inoltre:

- i log sono protetti con idonee misure contro ogni uso improprio;
 - i log sono conservati per 24 mesi e cancellati alla scadenza;
 - i dati contenuti nei log sono trattati da personale appositamente incaricato del trattamento esclusivamente in forma aggregata; possono essere trattati in forma non aggregata unicamente laddove ciò risulti indispensabile ai fini della verifica della correttezza e legittimità delle singole operazioni effettuate;
- nel caso di cooperazione applicativa:
- sono conservati i file di log degli invii delle informazioni al registro;
 - sono conservati i file di log delle ricevute del registro;
 - a seguito dell'avvenuta ricezione delle ricevute il contenuto delle comunicazioni effettuate è eliminato;



REGIONE PUGLIA

f) utilizzare sistemi di audit log per la verifica periodica degli accessi ai dati e per il rilevamento delle anomalie

1.2 Invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web (web services) o cooperazione applicativa)

L'invio telematico dei dati al Registro Tumori da parte delle aziende sanitarie, degli istituti di ricovero e cura a carattere scientifico e delle strutture sanitarie private accreditate avviene adottando le seguenti misure di sicurezza:

a) utilizzo di canali di trasmissione protetti (FTP sicuro, VPN IPSEC/SSL o HTTPS o sistemi equivalenti) adeguati in relazione allo stato dell'arte dell'evoluzione tecnologica;

b) cifratura dei dati mediante sistemi crittografici basati su protocolli a chiave asimmetrica, la cui componente pubblica è resa nota alle aziende sanitarie, degli istituti di ricovero e cura a carattere scientifico e delle strutture sanitarie private accreditate dal Titolare del Trattamento del Registro Tumori; la componente "privata" della chiave è conservata in un dispositivo sicuro (smart card), assegnato al Titolare medesimo, unitamente al relativo P.I.N.;

c) nel caso di utilizzo della PEC, cifratura dei dati sensibili che devono essere riportati in appositi allegati utilizzando gli strumenti di cui al punto b).

Il Titolare del trattamento dei dati del Registro Tumori è tenuto a stipulare previamente una convenzione (o altro atto bilaterale) con ciascuno dei soggetti di cui all'articolo 7 del regolamento, secondo uno schema tipo predisposto dalla Regione/Provincia, volta a definire le specifiche modalità tecniche di raccolta dei dati e le misure di sicurezza nel rispetto di quanto previsto dal presente disciplinare tecnico e dal provvedimento del Garante per la protezione dei dati personali recante "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015".

1.3 Accesso diretto degli incaricati del Registro Tumori ai sistemi informatici delle strutture sanitarie di cui all'articolo 7 del Regolamento

Il Titolare del trattamento dei dati del Registro Tumori, per la raccolta delle informazioni di cui all'articolo 6 comma 2 effettuata con modalità informatiche direttamente dai propri incaricati presso i sistemi informatici delle aziende sanitarie, degli istituti di ricovero e cura a carattere scientifico e delle strutture sanitarie private accreditate è tenuto ad adottare le seguenti misure di sicurezza:

a) utilizzo di canali di trasmissione protetti (VPN IPSEC/SSL o canali HTTPS);

b) identificazione, autenticazione, autorizzazione degli incaricati del Registro Tumori, abilitati ad accedere alle fonti di dati di cui all'art 7 del regolamento.

1.4 Trasmissione su supporti informatici (es. CD, DVD, memorie a stato solido)

Il Titolare del trattamento dei dati del Registro Tumori, per la raccolta delle informazioni di cui all'articolo 6 comma 2 effettuata mediante trasmissione su supporti informatici è tenuto ad adottare le seguenti misure di sicurezza;



REGIONE PUGLIA

a) i supporti informatici, devono essere inseriti in plico chiuso, inviati mediante corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di trasporto e consegna del plico medesimo;

b) devono essere utilizzati accorgimenti tecnici per garantire l'integrità dei dati contenuti in tali supporti;

1.5 Trasmissione di documenti cartacei

Il Titolare del trattamento dei dati del Registro Tumori, per la raccolta delle informazioni di cui all'articolo 6 comma 2 effettuata mediante trasmissione di documenti cartacei è tenuto ad adottare le seguenti misure di sicurezza:

- i documenti cartacei devono essere inseriti in plico chiuso, inviati mediante corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di trasporto e consegna del plico medesimo;
- sul plico apporre la dicitura "Contiene dati personali. Riservato agli incaricati del trattamento dell'Ufficio "XXX";
- utilizzare plichi o "incarti" non trasparenti al fine di rendere inintelligibile il contenuto;
- apporre una firma o sigla sui lembi di chiusura del plico.

È in ogni caso vietato inviare via fax o a mezzo e-mail documenti contenenti dati sensibili.

2. FASE DI ELABORAZIONE DEI DATI

2.1. Ai fini dell'attuazione di quanto previsto all'articolo 13 del Regolamento, il sistema di codifica dei dati identificativi degli interessati raccolti dal Registro Tumori deve consistere in un numero predefinito di caratteri alfanumerici ottenuti attraverso procedure di cifratura invertibili, con algoritmo biunivoco e reversibile.

2.2. I dati raccolti nel Registro Tumori sono trattati dagli incaricati del Registro Tumori esclusivamente attraverso applicazioni software dotate di adeguati sistemi di autenticazione e di autorizzazione in funzione del ruolo degli incaricati e delle esigenze di accesso e trattamento dei dati, avendo cura di delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati e di predisporre meccanismi per la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi. Tali applicazioni devono possedere le seguenti caratteristiche:

a) un sistema di autenticazione a più fattori. Nella fase transitoria di cui all'articolo 16 del Regolamento necessaria per l'adeguamento tecnologico a tale soluzione, non superiore a 180 giorni dall'entrata in vigore del Regolamento, è possibile utilizzare credenziali costituite da codice identificativo e parola chiave riservata robusta, univoca, non condivisa, modificata con cadenza massima di 90 giorni;

b) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;

c) sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;



REGIONE PUGLIA

d) siano visualizzabili le informazioni relative alla sessione corrente e all'ultima sessione effettuata con le stesse credenziali (con l'indicazione almeno di data, ora e indirizzo di rete da cui è effettuata la connessione);

2.3 Le postazioni di lavoro utilizzate per il trattamento dei dati devono appartenere alla rete IP del Titolare del trattamento del Registro Tumori o essere dotate di certificato digitale, emesso da una Certification Authority ufficiale, che identifichi univocamente la postazione di lavoro.

2.4 Devono essere altresì adottate le misure di sicurezza e gli accorgimenti tecnici specificati nelle lettere d), e) e f) del punto 1.1 del presente disciplinare.

3. FASE DI CONSERVAZIONE DEI DATI

3.1 I dati raccolti dal Titolare del trattamento del Registro Tumori, codificati ai sensi del punto 2.1, devono essere memorizzati e conservati in luoghi e con modalità prestabilite dal Titolare stesso, in modo tale da proteggere l'identità e tutelare la riservatezza degli interessati.

3.2 I dati di cui al punto 3.1 devono essere conservati con garanzie di riservatezza, integrità e disponibilità, con conseguente possibilità di ripristino dei dati stessi in caso di guasti e malfunzionamenti, per un periodo di 1 anno, al fine di eventuali successive verifiche ed integrazione dei dati.

3.3 Il ripristino dei dati di cui al punto 3.1 deve avvenire secondo una documentata procedura di restore, prestabilita dal Titolare del trattamento.

3.4 I supporti informatici e i documenti cartacei contenenti i dati del Registro devono essere riposti dagli incaricati in appositi archivi, organizzati secondo una documentata procedura relativa alla nomenclatura e alla classificazione dei supporti in modo che siano univocamente identificabili, soltanto attraverso apposito codice in caso di necessità e di verifica.

4. ACCESSO AI LOCALI DEL REGISTRO TUMORI

4.1. L'accesso ai locali del Registro Tumori, ivi compresi i locali destinati a ospitare gli archivi di supporti informatici o cartacei, deve avvenire secondo una documentata procedura, prestabilita dal Titolare del trattamento, che preveda l'identificazione delle persone che accedono e la registrazione degli orari di ingresso e uscita di tali persone.

5. MANUTENZIONE DEI SISTEMI INFORMATICI

5.1 Nel rispetto di quanto prescritto dall'art.28 del GDPR, i soggetti esterni che effettuino delle attività di manutenzione dei sistemi informatici, che possono comportare il



REGIONE PUGLIA

trattamento dei dati del Registro Tumori, devono essere designati Responsabili del trattamento in outsourcing.

5.2 I contratti di manutenzione, stipulati con i soggetti di cui al punto 5.1, devono prevedere specifiche clausole di riservatezza dei dati, la registrazione degli interventi con l'indicazione degli orari di inizio e fine, le persone che li hanno effettuati e le motivazioni che hanno determinato la necessità dei medesimi interventi.

6. CANCELLAZIONE DEI DATI E DISMISSIONE DEI SUPPORTI E DOCUMENTI CONTENENTI DATI

6.1 I dati presenti sul sistema informatico del Registro Tumori, devono essere cancellati o resi anonimi in maniera irreversibile trascorso un periodo di 30 anni dal decesso dell'interessato cui i dati si riferiscono.

6.2 La procedura di anonimizzazione di cui al punto precedente deve adottare tecniche adeguate alla protezione dell'identità del paziente da rischi legati all'identificabilità mediante individuazione, correlabilità e deduzione a partire dai dati sanitari. Devono essere applicate tecniche di randomizzazione e generalizzazione dei dati, tenuto conto dell'evoluzione tecnologica, in modo da mantenere nel complesso la distribuzione degli elementi rilevanti per finalità di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria espressamente previsti dal Regolamento all'articolo 3 comma 1 lettera d).

6.3 I supporti informatici (es. memorie di massa dei server e delle postazioni di lavoro, supporti rimovibili etc.) del Registro Tumori devono essere dismessi secondo quanto previsto dal Provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" (G.U. n. 287 del 9 dicembre 2008).

6.4 I supporti cartacei del Registro Tumori, contenenti dati sanitari, devono essere distrutti secondo una documentata procedura, prestabilita dal Titolare del trattamento, entro un periodo di 10 anni dal decesso dell'interessato, cui i dati si riferiscono.

7. DATA BREACH

7.1 il titolare del Registro adotta misure tecniche e organizzative adeguate a rilevare tempestivamente eventuali violazioni dei dati personali e adempiere alle previsioni di cui agli articoli 33 e 34 del Regolamento UE 2016/679.

L.R. 14 luglio 2022, n. 12**Istituzione del Registro Tumori della Regione Abruzzo.**

(Approvata dal Consiglio regionale con [verbale n. 70/1 del 5 luglio 2022](#), pubblicata nel BURA 22 luglio 2022, n. 102 Speciale ed entrata in vigore il 23 luglio 2022)

Testo vigente

(in vigore dal 23/07/2022)

Art. 1

(Istituzione e finalita')

1. E' istituito il Registro Tumori della Regione Abruzzo, finalizzato a garantire un sistema attivo di raccolta sistematica di dati anagrafici, sanitari ed epidemiologici volti a produrre misura dell'incidenza, mortalita', sopravvivenza e prevalenza dei tumori; descrivere il rischio della malattia per sede e per tipo di tumore, eta', genere e ogni altra variabile di interesse per la ricerca scientifica; svolgere studi epidemiologici sugli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio dei tumori, sugli esiti degli interventi di diagnosi precoce, delle terapie e dei percorsi diagnostico-terapeutici, in collaborazione con la struttura dipartimentale dell'amministrazione regionale competente per materia, con enti del servizio sanitario regionale e nazionale, con enti internazionali di ricerca scientifica in campo epidemiologico; produrre dati anonimi e aggregati per la programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, inerente gli interventi di prevenzione primaria e secondaria rivolti alle persone ed all'ambiente di vita e lavoro, nonche' dell'efficacia dei programmi di screening; monitorare e valutare i dati relativi all'appropriatezza e qualita' dei servizi diagnostici terapeutici, alla sopravvivenza dei pazienti affetti da cancro.
2. Il Registro Tumori della Regione Abruzzo assicura l'inserimento tempestivo, qualificato e sistematico dei dati nella Rete Nazionale dei Registri dei Tumori e dei Sistemi di Sorveglianza, secondo le modalita' di raccolta, conferimento e produzione dei flussi nei termini e con la consistenza definiti ai sensi dei commi 2 e 3 dell'[articolo 1 della legge 22 marzo 2019, n. 29](#) (Istituzione e disciplina della Rete nazionale dei registri dei tumori e dei sistemi di sorveglianza e del referto epidemiologico per il controllo sanitario della popolazione).

Art. 2

(Organizzazione)

1. Il Registro Tumori della Regione Abruzzo e' istituito presso l'Agenzia Sanitaria Regionale - ASR Abruzzo, che ne garantisce la gestione amministrativa, tecnica ed informatica nell'ambito delle risorse assegnate annualmente in via ordinaria.
2. Insieme al Registro tumori, e quali fonti aggiuntive di dati, la ASR Abruzzo gestisce i registri della sezione regionale del Registro Nazionale dei Mesoteliomi (ReNaM) e del Registro Nazionale dei Tumori Naso-Sinusali (ReNaTuNS).
3. E' istituito, in seno al Registro Tumori della Regione Abruzzo, il Comitato tecnico- scientifico del Registro tumori, con funzioni di indirizzo, di controllo degli standard e dei sistemi e metodi utilizzati, di valutazione di qualita' e di adesione a linee guida, di formazione e di aggiornamento.
4. Con il regolamento per il funzionamento del Registro tumori della Regione Abruzzo di cui all'articolo 3 e' definita la composizione del Comitato tecnico-scientifico del Registro tumori della Regione Abruzzo, presieduta dal Direttore dell'Agenzia Sanitaria Regionale, i cui componenti svolgono l'attivita' richiesta a titolo gratuito.
5. All'interno del Comitato tecnico-scientifico sono individuati un responsabile della gestione e un suo vicario, con il compito di garantire la puntualita', la correttezza e la completezza degli argomenti del Registro e dell'interfacciamento con la Rete Nazionale dei Registri Tumori.

Art. 3

(Regolamento)

1. Entro 30 giorni dall'entrata in vigore della presente legge la Giunta regionale propone, secondo le disposizioni dell'articolo 36 e seguenti dello Statuto della Regione Abruzzo, il progetto di regolamento per il funzionamento del Registro tumori della Regione Abruzzo, che disciplina, in attuazione ed in conformita' all'[articolo 12 del decreto legge 18 ottobre 2012, n. 179](#) (Ulteriori misure urgenti per la crescita del Paese), convertito con modificazioni nella [legge 17 dicembre 2012, n. 221](#), l'implementazione dei flussi informativi necessari all'inserimento dei dati nella Rete Nazionale Registri Tumori e Sistemi di Sorveglianza.
2. Il regolamento definisce altresì le modalita' di attuazione della normativa statale in materia di protezione dei dati personali, in conformita' al parere espresso dal Garante per la protezione dei dati personali ai sensi degli [articoli 20 e 154, comma 1, lettera g, del decreto legislativo 30 giugno 2003, n. 196](#) (Codice in materia di protezione dei dati personali) e del [Reg. \(CE\) 27 aprile 2016, n. 2016/679/UE Regolamento 2 del Parlamento Europeo](#) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati). Vengono definiti le

tipologie di dati particolari o sensibili, le operazioni eseguibili, le specifiche finalita' perseguite dal registro, i soggetti che possono avere accesso ai registri e le misure per la custodia e per la sicurezza dei dati.

Art. 4

(Digitalizzazione del Registro Nominativo delle cause di Morte)

1. A decorrere dall'anno 2023 le Aziende Sanitarie Locali della Regione Abruzzo sono tenute a digitalizzare il "Registro Nominativo delle cause di Morte" istituito ai sensi del [decreto del Presidente della Repubblica 10 settembre 1990, n. 285](#) (Approvazione del regolamento di polizia mortuaria) e ad inviare i dati aggiornati al gestore del Registro Tumori con cadenza semestrale, nel formato definito da apposito disciplinare proposto dalla Giunta regionale entro 180 giorni dall'entrata in vigore della presente legge.

Art. 5

(Invarianza finanziaria)

1. Dall'applicazione della presente legge non derivano nuovi o maggiori oneri per il bilancio regionale. Gli enti interessati provvedono agli adempimenti previsti con risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

Art. 6

(Entrata in vigore)

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nel Bollettino Ufficiale della Regione Abruzzo in versione Telematica (BURAT).

LEGGE REGIONALE 01 giugno 2017, n. 9**FUSIONE DELL'AZIENDA UNITÀ SANITARIA LOCALE DI REGGIO EMILIA E DELL'AZIENDA OSPEDALIERA 'ARCISPEDALE SANTA MARIA NUOVA'. ALTRE DISPOSIZIONI DI ADEGUAMENTO DEGLI ASSETTI ORGANIZZATIVI IN MATERIA SANITARIA**

Testo coordinato con le modifiche apportate da:

L.R. 27 dicembre 2017 n. 25

L.R. 27 dicembre 2018, n. 24

L.R. 30 luglio 2019, n. 13

L.R. 29 luglio 2021, n. 8

**CAPO I
Disposizioni generali***Art. 1**Oggetto e finalità*

1. La presente legge detta disposizioni per l'adeguamento del governo e della gestione dei servizi sanitari. In particolare, al fine di assicurare e potenziare i servizi sanitari nell'interesse delle persone e della collettività, in condizioni di valorizzazione qualitativa, omogeneità, appropriatezza ed efficienza, la presente legge realizza forme di integrazione funzionali e strutturali e di razionalizzazione organizzativa idonee a garantire lo snellimento amministrativo ed il contenimento della spesa pubblica.

2. Le finalità di cui al comma 1 sono perseguite attraverso:

a) la fusione delle strutture aziendali dell'Azienda unità sanitaria locale di Reggio Emilia e dell'Azienda ospedaliera "Arcispedale Santa Maria Nuova", per effetto della quale risulta costituita un'unica Azienda sanitaria, di seguito denominata Azienda USL di Reggio Emilia;

b) il trasferimento della titolarità dell'Istituto di ricovero e cura a carattere scientifico "Istituto in tecnologie avanzate e modelli assistenziali in oncologia" in capo all'Azienda USL di Reggio Emilia.

3. La presente legge detta altresì misure organizzative dirette a perseguire, nel rispetto delle competenze dello Stato, politiche di prevenzione della corruzione e di promozione della trasparenza, nonché l'istituzione dei registri di rilevante interesse regionale di cui all'articolo 6.

**CAPO II
Misure di adeguamento del governo e della gestione dei servizi sanitari***Art. 2**Fusione dell'Azienda unità sanitaria locale di Reggio Emilia e dell'Azienda ospedaliera "Arcispedale Santa Maria Nuova"*

1. A decorrere dall'1 luglio 2017, l'Azienda unità sanitaria locale di Reggio Emilia e l'Azienda ospedaliera "Arcispedale Santa Maria Nuova" sono fuse. Dalla data di fusione, l'Azienda ospedaliera "Arcispedale Santa Maria Nuova" cessa e l'Azienda USL di Reggio Emilia subentra a tutti gli effetti e senza soluzione di continuità nell'attività e nei rapporti attivi e passivi, interni ed esterni dell'Azienda ospedaliera cessata.

2. Il patrimonio dell'Azienda ospedaliera "Arcispedale Santa Maria Nuova", costituito dai beni mobili e immobili ad essa appartenenti, comunque acquisiti nell'esercizio della propria attività o a seguito di atti di liberalità, è trasferito all'Azienda USL di Reggio Emilia. La presente legge costituisce titolo per la trascrizione ai sensi dell'articolo 5, comma 3, del decreto legislativo 30 dicembre 1992, n. 502 (Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421).

3. I direttori generali dell'Azienda unità sanitaria locale di Reggio Emilia e dell'Azienda ospedaliera "Arcispedale Santa Maria Nuova", in carica all'entrata in vigore della presente legge, assicurano tutti gli adempimenti, anche di carattere ricognitivo, organizzativi, gestionali, fiscali, economico-finanziari e patrimoniali necessari alla fusione delle due Aziende e alla cessazione dell'Azienda ospedaliera "Arcispedale Santa Maria Nuova". In particolare, effettuano la ricognizione:

a) al patrimonio immobiliare e mobiliare al 30 giugno 2017;

b) della dotazione organica complessiva al 30 giugno 2017 e dei fondi contrattuali così come determinati dalla vigente contrattazione decentrata.

4. Il personale in servizio nella preesistente Azienda ospedaliera, con contratto di lavoro subordinato, a tempo indeterminato o determinato, è trasferito senza soluzione di continuità all'Azienda USL di Reggio Emilia conformemente a quanto previsto dal decreto legislativo 30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche). A tal fine, la Giunta regionale può fornire indirizzi con specifico atto.

5. In coerenza con i principi previsti dalla legge regionale 23 dicembre 2004, n. 29 (Norme generali sull'organizzazione ed il funzionamento del Servizio sanitario regionale), il processo di fusione e integrazione di cui alla presente legge è svolto garantendo la valorizzazione delle risorse umane e professionali degli operatori, la qualità e la sicurezza del lavoro, l'ottimale allocazione delle risorse per l'esercizio dei servizi, la formazione e la riqualificazione condivisa delle risorse umane, nonché il confronto con le organizzazioni sindacali, delle quali si riconosce il ruolo.

Testo non ufficiale. La sola stampa del bollettino ufficiale ha carattere legale

*Art. 3**Norme di prima applicazione sull'organizzazione e funzionamento dell'Azienda USL di Reggio Emilia*

1. Gli organi dell'Azienda unità sanitaria locale di Reggio Emilia, in essere al 30 giugno 2017, permangono in carica sino alla loro naturale scadenza. Il Collegio di direzione deve essere ricostituito conformemente al nuovo assetto istituzionale e organizzativo al fine di garantirne la piena e tempestiva funzionalità.
2. Entro il 30 giugno 2018, il direttore generale dell'Azienda USL di Reggio Emilia adegua l'atto aziendale della medesima al nuovo assetto istituzionale e organizzativo fissato dalla presente legge. L'atto aziendale adeguato è sottoposto alla Giunta regionale ai fini della verifica di conformità di cui all' articolo 3, comma 4, della legge regionale n. 29 del 2004.
3. L'Azienda USL di Reggio Emilia persegue la riorganizzazione e la fusione delle attività di amministrazione e di supporto logistico e tecnico-professionale, con lo scopo di garantire efficienza organizzativa e trasparenza, e di omogeneizzare e snellire le procedure del nuovo assetto aziendale.
4. Al fine di promuovere e valorizzare le forme di cooperazione e di innalzare il livello qualitativo dei servizi sanitari erogati, con particolare riguardo a quelli di più alta complessità, la riorganizzazione deve prevedere la costituzione di un presidio ospedaliero unico, articolato in più stabilimenti, che incorpori il presidio ospedaliero in essere dell'Azienda unità sanitaria locale di Reggio Emilia all'Arcispedale Santa Maria Nuova.
5. Il perseguimento degli obiettivi di cui al presente Capo, i processi di programmazione dei servizi sanitari e socio-sanitari nel territorio di Reggio Emilia, nonché lo svolgimento degli adempimenti necessari alla costituzione dell'unica Azienda sanitaria, avvengono attraverso il confronto con le organizzazioni sindacali.

*Art. 4**Trasferimento dell'IRCCS "Istituto in tecnologie avanzate e modelli assistenziali in oncologia" all'Azienda USL di Reggio Emilia. Organizzazione e funzionamento dell'Istituto*

1. A decorrere dal 1 luglio 2017, la titolarità dell'Istituto di ricovero e cura a carattere scientifico (IRCCS) "Istituto in tecnologie avanzate e modelli assistenziali in oncologia", di seguito denominato Istituto, costituito all'interno dell'Azienda ospedaliera "Arcispedale Santa Maria Nuova" ai sensi dell' articolo 12, comma 3, lettera b), della legge regionale 19 febbraio 2008, n. 4 (Disciplina degli accertamenti della disabilità - Ulteriori misure di semplificazione ed altre disposizioni in materia sanitaria e sociale), è trasferita all'Azienda USL di Reggio Emilia. L'Istituto svolge l'attività di assistenza e ricerca nell'ambito degli indirizzi e della programmazione regionale e concorre alla realizzazione dei livelli essenziali e uniformi di assistenza, secondo il ruolo attribuito dalla legislazione vigente agli Istituti di ricovero e cura a carattere scientifico.
2. L'organizzazione e il funzionamento dell'Istituto continuano ad essere disciplinati dalla vigente normativa nazionale e regionale.
3. L'atto aziendale dell'Azienda USL di Reggio Emilia, adeguato ai sensi dell'articolo 3, comma 2, disciplina l'assetto degli organi e le rispettive competenze, configura la forma organizzativa e le afferenti strutture, prevede la collaborazione con l'Università e con la rete europea, nazionale e regionale degli Istituti di ricerca in oncologia.
4. Il Consiglio di indirizzo e verifica e il direttore scientifico, in essere al 30 giugno 2017, permangono in carica sino alla loro naturale scadenza.
5. Al fine di garantire l'integrazione tra l'attività assistenziale e l'attività di ricerca, il direttore scientifico per l'esercizio delle sue funzioni opera in diretta collaborazione con il direttore generale.
6. Ai sensi di quanto previsto dalla legge regionale n. 4 del 2008, all'Istituto è assicurata autonomia scientifica, organizzativa e contabile, con assegnazione di beni, personale e risorse, secondo quanto specificamente indicato nello statuto e nell'atto organizzativo dell'Istituto.

CAPO III**Altre misure di adeguamento in materia sanitaria***Art. 5**Politiche di prevenzione della corruzione e di promozione della trasparenza*

1. In coerenza con i principi e le finalità della legge regionale 28 ottobre 2016, n. 18 (Testo unico per la promozione della legalità e per la valorizzazione della cittadinanza e dell'economia responsabili) e, nello specifico, con quanto disposto dall'articolo 15, le Aziende e gli Enti del Servizio sanitario regionale perseguono gli obiettivi di prevenzione e contrasto della corruzione e di promozione della trasparenza, in particolare mediante:
 - a) l'adozione delle migliori prassi di attuazione delle disposizioni della legge 6 novembre 2012, n. 190 (Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione), al fine di rafforzare l'efficacia e l'effettività delle misure di contrasto al fenomeno corruttivo;
 - b) la programmazione, nell'ambito dei Piani triennali per la prevenzione della corruzione, di obbligatorie misure di rotazione degli incarichi, con particolare riferimento agli incarichi dirigenziali, secondo criteri definiti in coerenza con gli indirizzi contenuti nel Piano nazionale anticorruzione; solo nei casi, adeguatamente motivati, in cui la rotazione non sia possibile, devono essere programmate misure alternative di prevenzione della corruzione con effetti analoghi;

Testo non ufficiale. La sola stampa del bollettino ufficiale ha carattere legale

c) l'adozione delle migliori prassi di attuazione delle disposizioni del decreto legislativo 14 marzo 2013, n. 33 (Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni) e delle misure specifiche contenute all'interno del Piano triennale per la prevenzione della corruzione, al fine di garantire un adeguato livello di trasparenza, la legalità e lo sviluppo della cultura dell'integrità;

d) l'emanazione, ai sensi dell' articolo 54 del decreto legislativo n. 165 del 2001, del codice di comportamento dei dipendenti, al fine di assicurare la qualità dei servizi, la prevenzione dei fenomeni di corruzione, il rispetto dei doveri costituzionali di diligenza, lealtà, imparzialità e servizio esclusivo alla cura dell'interesse pubblico. Il codice di comportamento prevede il dovere da parte del personale di assicurare la pubblicizzazione, tramite apposita dichiarazione da rendersi annualmente in forma completa all'ente di appartenenza, di tutti i rapporti intercorsi, a qualsiasi titolo, con soggetti esterni dai quali possa derivare un conflitto di interessi anche potenziale; detta dichiarazione specifica tutti gli eventuali emolumenti percepiti e i benefici goduti, sia direttamente che indirettamente. Il codice di comportamento deve contenere la previsione per cui l'eventuale violazione del dovere di rendere la predetta dichiarazione, nonché di fornire le informazioni sulla propria situazione patrimoniale e le dichiarazioni annuali dei redditi soggetti all'imposta sui redditi delle persone fisiche, previsto dalla vigente normativa di legge per il personale titolare di incarico dirigenziale, è fonte di responsabilità disciplinare ed è rilevante ai fini della responsabilità civile, amministrativa e contabile, ai sensi dell' articolo 54, comma 3, del decreto legislativo n. 165 del 2001. A decorrere dall'entrata in vigore della presente legge, le disposizioni contenute nei due periodi precedenti integrano il contenuto dei codici di comportamento definiti dalle Aziende e dagli Enti del Servizio sanitario regionale. Le predette amministrazioni sono tenute ad esercitare il potere disciplinare in caso di mancato assolvimento, nel rispetto delle procedure definite dalle amministrazioni stesse, dei doveri prima richiamati.

Art. 5 bis

*Pubblicità legale degli atti delle aziende sanitarie e degli enti del Servizio sanitario regionale
(aggiunto da art. 23 L.R. 27 dicembre 2018, n. 24)*

1. *Le aziende sanitarie e gli enti del Servizio sanitario regionale pubblicano, anche per estratto, nell'albo istituito ai sensi dell'articolo 32 della legge 18 giugno 2009, n. 69 (Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile) e nel rispetto di quanto disposto dalla normativa in materia di protezione dei dati personali, le deliberazioni del direttore generale e le determinazioni dirigenziali. Tali atti sono pubblicati per quindici giorni consecutivi, se non diversamente stabilito da specifiche disposizioni, e diventano esecutivi dal giorno della loro pubblicazione.*

Art. 6

Registri di rilevante interesse regionale

(prima aggiunta lett. q bis.) comma 1 da art. 55 L.R. 27 dicembre 2017 n. 25, successivamente aggiunta lett. q ter.) da art. 13 L.R. 29 luglio 2021, n. 8)

1. Nel rispetto delle disposizioni del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e in conformità a quanto previsto dall' articolo 12, comma 12, del decreto legge 18 ottobre 2012, n. 179 (Ulteriori misure urgenti per la crescita del Paese), convertito con legge 17 dicembre 2012, n. 221 (Conversione, con modificazioni, del decreto-legge 18 ottobre 2012, n. 179, recante ulteriori misure urgenti per la crescita del Paese), sono istituiti i seguenti registri di rilevante interesse regionale:

- a) Registro tumori;
- b) Registro diabete;
- c) Registro impiantologia protesica ortopedica (RIPO);
- d) Registro insufficienza renale cronica e trattamento sostitutivo (Dialisi);
- e) Registro regionale per le malattie rare;
- f) Registro indagine malformazioni congenite in Emilia-Romagna (IMER);
- g) Registro delle broncopolmonopatie croniche ostruttive (BPCO);
- h) Registro interventi in ambito cardiologico e cardiocirurgico;
- i) Registro angioplastiche coronariche;
- j) Registro aritmologia interventistica;
- k) Registro delle malattie reumatologiche e dei trattamenti;
- l) Registro nati pretermine;
- m) Registro endometriosi;
- n) Registro della narcolessia e delle ipersonnie rare;
- o) Registro sclerosi laterale amiotrofica (SLA);
- p) Registro gravi cerebrolesioni acquisite (GRACER);
- q) Registro dei traumi gravi.

q bis.) *Registro regionale Malattie Emorragiche Congenite (MEC).*

q ter.) *Registro Regionale Epilessia (RREP).*

2. I registri di cui al comma 1 sono istituiti allo scopo di garantire un sistema attivo di raccolta sistematica di dati anagrafici, sanitari ed epidemiologici per registrare e caratterizzare tutti i casi di rischio per la salute, di una particolare malattia e dei suoi trattamenti ed esiti o di una condizione di salute rilevante in una popolazione definita.

3. Con successivo regolamento regionale, adottato in conformità al parere espresso dal Garante per la

protezione dei dati personali, ai sensi degli articoli 20, 22 e 154, comma 1, lettera g), del decreto legislativo n. 196 del 2003, sono individuati i tipi di dati sensibili, le operazioni eseguibili, le specifiche finalità perseguite da ciascun registro, il titolare del trattamento del singolo registro, i soggetti che possono avervi accesso, i dati che possono conoscere e le misure per la custodia e la sicurezza dei dati. Resta fermo l'adeguamento alle disposizioni previste dal regolamento da adottare ai sensi dell' articolo 17, comma 1, della legge 23 agosto 1988, n. 400 (Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri) come disposto dall' articolo 12, comma 13, del decreto legge n. 179 del 2012, convertito con legge n. 221 del 2012.

4. Le previsioni del regolamento di cui al comma 3 devono, in ogni caso, informarsi ai principi di indispensabilità, necessità, pertinenza e non eccedenza di cui agli articoli 3, 11 e 22 del decreto legislativo n. 196 del 2003.

Art. 6 bis

Disposizioni per l'applicazione della legge n. 219 del 2017 sulle disposizioni anticipate di trattamento (DAT - testamento biologico) (aggiunto da art. 24 L.R. 27 dicembre 2018, n. 24, poi sostituito da art. 38 L.R. 30 luglio 2019 n. 13)

1. *Per l'applicazione della legge 22 dicembre 2017, n. 219 (Norme in materia di consenso informato e di disposizioni anticipate di trattamento), e nel rispetto della disciplina del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) e del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), la Regione Emilia-Romagna istituisce il Portale regionale DAT (di seguito denominato "Portale") quale strumento di raccolta delle informazioni relative ai dati personali e di contatto delle persone residenti in Regione, iscritte al Servizio sanitario nazionale, che hanno scelto di redigere la disposizione anticipata di trattamento (DAT), oltre che degli eventuali fiduciari, ricevute dai Comuni della Regione e, previa specifica convenzione con il Comitato regionale dei Consigli notarili dell'Emilia-Romagna, dai notai.*

2. *Il Portale, in coerenza con quanto stabilito dalla legge n. 219 del 2017, è istituito al fine di perseguire, in via transitoria, nelle more della realizzazione della banca dati di cui all'articolo 1, comma 418, della legge 27 dicembre 2017, n. 205 (Bilancio di previsione dello Stato per l'anno finanziario 2018 e bilancio pluriennale per il triennio 2018-2020), le finalità di rilevante interesse pubblico tese a gestire in maniera unificata e appropriata il processo di raccolta e la gestione delle informazioni relative all'esistenza delle DAT ed ai soggetti che hanno scelto di redigerla, ai fini della comunicazione dei dati tra i punti di raccolta previsti dalla normativa statale e le strutture sanitarie regionali, al momento della presa in carico del disponente.*

3. *La Giunta regionale con successivi atti, anche di natura regolamentare, definisce le modalità attuative in ordine alle modalità operative di registrazione e trattamento dei dati raccolti, alle misure di sicurezza del trattamento, nel rispetto della disciplina relativa al trattamento dei dati personali, nonché alla definizione di una o più convenzioni con il Comitato regionale dei Consigli notarili dell'Emilia-Romagna, ferme restando le ulteriori disposizioni assunte ai sensi dell'articolo 1, comma 419, della legge n. 205 del 2017.*

Art. 6 ter

Promozione della medicina di iniziativa all'interno del Servizio sanitario regionale (aggiunto da art. 39 L.R. 30 luglio 2019 n. 13)

1. *Il sistema sanitario regionale riconosce e promuove la medicina di iniziativa quale modello assistenziale della sanità moderna finalizzato alla prevenzione e diagnosi precoce delle patologie croniche ed alla conseguente attivazione di interventi mirati al cambiamento degli stili di vita e alla presa in carico integrata e multidisciplinare. A tal fine la medicina di iniziativa opera la stratificazione, da parte della Regione, del rischio degli assistiti e assistibili attraverso l'analisi statistica dei dati gestiti nell'ambito dei diversi archivi del servizio informativo sanitario regionale.*

2. *La Giunta regionale, con atto di natura regolamentare, reca disposizioni tese a promuovere la diffusione della medicina di iniziativa, nel rispetto dei seguenti criteri:*

- a) *identificazione dei soggetti in condizioni di rischio aumentato per malattie croniche non trasmissibili o che, in assenza di sintomatologia evidente, ne siano già affetti;*
- b) *presa in carico e gestione del paziente, da parte dell'ente del Servizio sanitario regionale territorialmente competente, attraverso l'adozione di modelli e strumenti atti a garantire:*
 - 1) *interventi personalizzati per la gestione del paziente che tengano conto non solo della condizione clinica, ma anche delle diverse determinanti socio-economiche;*
 - 2) *definizione di un piano di cura personalizzato volto favorire anche lo sviluppo delle abilità di auto-cura;*
 - 3) *continuità delle cure durante la transizione tra tutti i livelli di assistenza;*
 - 4) *una risposta integrata ai bisogni di salute sociali e sanitari;*
 - 5) *progetti di formazione del team multidisciplinare;*
 - 6) *sostegno alle attività di formazione e informazione dei pazienti, delle loro famiglie e dei caregiver, anche valorizzandone il ruolo.*

3. *La Giunta regionale col regolamento di cui al comma 2 disciplina la specifica individuazione dei tipi di dati personali che possono essere trattati, le operazioni eseguibili nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. I trattamenti di dati personali sono effettuati per i motivi di interesse pubblico rilevante di cui alle disposizioni del Regolamento (UE) 2016/679, articolo 9, paragrafo 2, lettere g) e h).*

4. *La Giunta regionale trasmette annualmente alla competente commissione assembleare una relazione sulle azioni di promozione e di sostegno della medicina di iniziativa attuate nel territorio regionale.*

Art. 7

Nullaosta alle sperimentazioni cliniche

Testo non ufficiale. La sola stampa del bollettino ufficiale ha carattere legale

1. Le sperimentazioni cliniche e gli studi, che secondo la legge o altra fonte normativa devono essere sottoposti al parere del competente Comitato etico, richiedono espresso e motivato nullaosta del direttore generale della struttura sanitaria in cui è condotta l'attività, affinché sia garantita anche l'assenza di pregiudizi per l'attività assistenziale. L'avvio della sperimentazione clinica o dello studio, in assenza del predetto nullaosta, è fonte di responsabilità disciplinare ed è rilevante ai fini della responsabilità civile, amministrativa e contabile dello sperimentatore. Le amministrazioni di appartenenza sono tenute ad esercitare il relativo potere disciplinare.

CAPO IV
Disposizioni finali

Art. 8
Monitoraggio

1. Decorsi 18 mesi dalla costituzione dell'Azienda USL di Reggio Emilia, la Giunta regionale elabora e trasmette alla competente Commissione assembleare una relazione intermedia sullo stato di attuazione delle disposizioni di cui al Capo II.

2. Dopo tre anni dall'entrata in vigore della presente legge, la Giunta regionale elabora e trasmette alla competente Commissione assembleare una relazione finale sull'attuazione delle disposizioni di cui al Capo II.

Art. 9
Abrogazioni

1. L'articolo 14 (Istituzione di registri di rilevante interesse sanitario) della legge regionale n. 4 del 2008 è abrogato.

Art. 10
Entrata in vigore

1. La presente legge entra in vigore il giorno stesso della sua pubblicazione nel Bollettino Ufficiale Telematico della Regione Emilia-Romagna.



DELIBERAZIONE DELLA GIUNTA REGIONALE

ADUNANZA N. 303 LEGISLATURA N. Xdelibera
36

PR/PR/ARS Oggetto: Regolamento regionale di competenza della Giunta
0 NC regionale concernente: "Disposizioni per il
funzionamento del registro tumori di cui alla legge
Prot. Segr. regionale 10 aprile 2012, n. 6 (Osservatorio
66 Epidemiologico Regionale. Registri regionali delle
cause di morte e di patologia)"

Lunedì 27 gennaio 2020, nella sede della Regione Marche, ad Ancona,
in via Gentile da Fabriano, si è riunita la Giunta regionale,
regolarmente convocata.

Sono presenti:

- LUCA CERISCIOLI	Presidente
- ANNA CASINI	Vicepresidente
- MANUELA BORA	Assessore
- FABRIZIO CESETTI	Assessore
- MORENO PIERONI	Assessore
- ANGELO SCIAPICHETTI	Assessore

E' assente:

- LORETTA BRAVI	Assessore
-----------------	-----------

Constatato il numero legale per la validità dell'adunanza, assume la
Presidenza il Presidente della Giunta regionale, Luca Ceriscioli. Assiste
alla seduta il Segretario della Giunta regionale, Deborah Giraldi.

Riferisce in qualità di relatore il Presidente Luca Ceriscioli.

La deliberazione in oggetto è approvata all'unanimità dei presenti.

NOTE DELLA SEGRETERIA DELLA GIUNTA

Inviata per gli adempimenti di competenza

- alla struttura organizzativa: _____
- alla P.O. di spesa: _____
- al Presidente del Consiglio regionale
- alla redazione del Bollettino ufficiale

Il _____

L'INCARICATO

Proposta o richiesta di parere trasmessa al Presidente
del Consiglio regionale il _____
prot. n. _____

L'INCARICATO



REGIONE MARCHE

GIUNTA REGIONALE

seduta del
27 GEN. 2020pag.
2Delibera
36

DELIBERAZIONE DELLA GIUNTA REGIONALE

OGGETTO: Regolamento regionale di competenza della Giunta regionale concernente: "Disposizioni per il funzionamento del registro tumori di cui alla legge regionale 10 aprile 2012, n. 6 (Osservatorio Epidemiologico Regionale. Registri regionali delle cause di morte e di patologia)".

LA GIUNTA REGIONALE

VISTA l'allegata proposta di regolamento regionale di competenza della Giunta regionale concernente: "Disposizioni per il funzionamento del registro tumori di cui alla legge regionale 10 aprile 2012, n. 6 (Osservatorio Epidemiologico Regionale. Registri regionali delle cause di morte e di patologia)", e il documento istruttorio, riportato in calce alla presente deliberazione, predisposti dalla PF Produzione legislativa;

RITENUTO, per i motivi riportati nel predetto documento istruttorio e che vengono condivisi, di deliberare in merito;

VISTO il parere favorevole di cui all'articolo 16 bis della legge regionale 15 ottobre 2001, n. 20, sotto il profilo della legittimità e della regolarità tecnica della dirigente della PF Flussi informativi sanitari e monitoraggio del SSR e l'attestazione della stessa che dalla presente deliberazione non deriva né può derivare alcun impegno di spesa a carico della Regione;

VISTA la proposta del Direttore dell'Agenzia Regionale Sanitaria (ARS);

VISTO l'articolo 28 dello Statuto della Regione;

con la votazione, resa in forma palese, riportata a pagina 1

DELIBERA

di approvare il regolamento regionale di competenza della Giunta regionale concernente: "Disposizioni per il funzionamento del registro tumori di cui alla legge regionale 10 aprile 2012, n. 6 (Osservatorio Epidemiologico Regionale. Registri regionali delle cause di morte e di patologia)", così come riportato nell'allegato A, parte integrante del presente atto.

Il Segretario della Giunta regionale
(Deborah Giraldi)

Il Presidente della Giunta regionale
(Luca Ceriscioli)



REGIONE MARCHE

GIUNTA REGIONALE

seduta del
27 GEN. 2020pag.
3Delibera
36

DELIBERAZIONE DELLA GIUNTA REGIONALE

DOCUMENTO ISTRUTTORIO

La PF Produzione legislativa ha predisposto, d'intesa con l'Agenzia Regionale Sanitaria (ARS), l'allegato schema di deliberazione contenente il regolamento regionale di competenza della Giunta regionale concernente: "Disposizioni per il funzionamento del registro tumori di cui alla legge regionale 10 aprile 2012, n. 6 (Osservatorio Epidemiologico Regionale. Registri regionali delle cause di morte e di patologia)".

Il comma 7 dell'articolo 2 della l.r. 6/2012 prevede che "Il trattamento dei dati dei registri (...) è effettuato in esecuzione del regolamento adottato dalla Giunta regionale ai sensi degli articoli 20 e 154, comma 1, lettera g), del D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)".

La Conferenza delle Regioni e delle Province autonome in data 21 giugno 2018 ha approvato lo schema tipo di deliberazione per l'adozione da parte delle regioni e province autonome di un regolamento recante norme per il funzionamento del registro tumori. Tale schema tipo è stato preventivamente sottoposto al vaglio del Garante per la protezione dei dati personali che, con nota del 18 aprile 2018, ha espresso parere favorevole con la seguente precisazione: "a partire dal 25 maggio 2018, dovrà definitivamente applicarsi il Regolamento (UE) 2016/679 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE), il quale prevede, tra l'altro, che vengano fornite agli interessati talune informazioni supplementari sul trattamento dei dati personali rispetto a quelle previste dal Codice (artt. 13 e 14) e, nell'estendere l'obbligo di notifica delle violazioni di dati personali, ne ridefinisce in parte i termini e le condizioni (art. 33 e 34). In proposito, si sottolinea quindi l'esigenza di adeguare a tale nuovo quadro giuridico, le pertinenti disposizioni dello schema tipo di regolamento in esame, tenendo in considerazione che gli atti regolamentari che saranno adottati in conformità a tale schema tipo dovranno conformarsi alle disposizioni del citato Regolamento europeo stante la sua imminente applicazione". In ogni caso per il Garante "l'adozione di un regolamento conforme allo schema tipo valutato positivamente (...) non rende necessario chiedere all'Autorità uno specifico parere".

In merito alla proposta di regolamento si è tenuta, in data 30 ottobre 2019, la conferenza dei servizi prevista dall'articolo 20 del regolamento interno della Giunta regionale nella quale sono state concordate le modifiche da apportare alla proposta di regolamento, redatto sulla base dello schema tipo, alla luce delle intervenute disposizioni del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (RGPD).

La proposta di regolamento non contiene alcuna disciplina transitoria in quanto la Regione ha già adottato le misure previste nel disciplinare tecnico di cui all'Allegato 1 della proposta di regolamento.

Per le ragioni sopra riportate il regolamento che si intende adottare quindi non è trasmesso per il parere al Garante per la tutela dei dati personali, ai sensi dell'articolo 36, comma 4, del RGPD in quanto preventivamente sottoposto al vaglio della medesima autorità di controllo.

Il verbale della conferenza è trasmesso unitamente alla proposta, senza farne parte integrante, ai sensi del comma 3 del medesimo articolo 20. Alla luce di quanto sopra evidenziato si propone alla Giunta di approvare il Regolamento regionale di competenza della Giunta regionale concernente:



REGIONE MARCHE

GIUNTA REGIONALE

seduta del
27 GEN. 2020pag.
4Delibera
36

DELIBERAZIONE DELLA GIUNTA REGIONALE

“Disposizioni per il funzionamento del registro tumori di cui alla legge regionale 10 aprile 2012, n. 6 (Osservatorio Epidemiologico Regionale. Registri regionali delle cause di morte e di patologia)”, così come riportato nell'allegato A, parte integrante e sostanziale del presente atto.

Il sottoscritto, in relazione al presente provvedimento, dichiara, ai sensi dell'articolo 47 del D.P.R. 445/2000, di non trovarsi in situazioni anche potenziali di conflitto di interesse ai sensi dell'articolo 6 bis della L. 241/1990 e degli articoli 6 e 7 del DPR 62/2013 e della DGR 64/2014.

Per il Dirigente della PF Produzione legislativa
Il Dirigente della PF Consulenza giuridica
(Alessandro Agostini)

PARERE DEL DIRIGENTE DELLA PF FLUSSI INFORMATIVI SANITARI E
MONITORAGGIO DEL SSR

La sottoscritta, considerata la motivazione espressa nell'atto, esprime parere favorevole sotto il profilo della legittimità e della regolarità tecnica della presente deliberazione e dichiara, ai sensi dell'articolo 47 del D.P.R. 445/2000, che in relazione al presente atto non si trova in situazioni anche potenziali di conflitto di interesse ai sensi dell'articolo 6 bis della L. 241/1990 e degli articoli 6 e 7 del DPR 62/2013 e della DGR 64/2014. Attesta inoltre che dalla presente deliberazione non deriva, né può derivare, alcun impegno di spesa a carico della Regione.

Il Dirigente della PF
(Liana Spazzafumo)

PROPOSTA DEL DIRETTORE DELL'AGENZIA REGIONALE SANITARIA

Il sottoscritto, considerata la motivazione espressa nell'atto, propone l'adozione alla Giunta regionale della presente deliberazione, in relazione alla quale dichiara, ai sensi dell'articolo 47 del D.P.R. 445/2000, di non trovarsi in situazioni anche potenziali di conflitto di interesse ai sensi dell'articolo 6 bis della L. 241/1990 e degli articoli 6 e 7 del DPR 62/2013 e della DGR 64/2014.

Il Direttore
(Rodolfo Pasquini)

La presente deliberazione si compone di n. 16 pagine, di cui n. 12 pagine di allegati, che formano parte integrante della stessa.

Il Segretario della Giunta
(Deborah Givaldi)



REGIONE MARCHE

GIUNTA REGIONALE

seduta del
27 GEN. 2020pag.
5Delibera
36

DELIBERAZIONE DELLA GIUNTA REGIONALE

Allegato A

Regolamento regionale di competenza della Giunta regionale concernente: "Disposizioni per il funzionamento del registro tumori di cui alla legge regionale 10 aprile 2012, n. 6 (Osservatorio Epidemiologico Regionale. Registri regionali delle cause di morte e di patologia)".

Art. 1*(Oggetto e finalità)*

1. Questo regolamento, ai sensi dell'articolo 2 della legge regionale 10 aprile 2012, n. 6 (Osservatorio Epidemiologico Regionale. Registri regionali delle cause di morte e di patologia), disciplina il trattamento dei dati inseriti nel registro tumori, con particolare riferimento ai tipi di dati, alle operazioni eseguibili, ai soggetti che possono trattare tali dati e alle misure per la sicurezza.

2. Il trattamento dei dati di cui al comma 1 avviene nel rispetto delle finalità previste dall'articolo 2 sexies, comma 2, lettere t) e u), e dall'articolo 110, comma 1 del decreto legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento UE n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE).

Art. 2*(Definizioni)*

1. Ai fini del presente regolamento si applicano le definizioni di cui all'articolo 4 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (RGPD).

2. In aggiunta a quanto previsto al comma 1, ai fini del presente regolamento, si intende per:

a) Registro tumori: un sistema attivo di raccolta sistematica di dati personali anagrafici e sanitari dei casi di tumore che insorgono nei residenti nel territorio regionale, realizzato ai fini di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, nonché di elaborazione delle informazioni epidemiologiche e statistiche a supporto delle attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;



DELIBERAZIONE DELLA GIUNTA REGIONALE

b) tumore o neoplasia: malattia a carattere evolutivo, come descritta dai codici 140 – 239 della Classificazione Internazionale delle malattie e cause di morte IX Revisione ovvero dai codici C00-C97 e D00-D48 della Classificazione Internazionale delle Malattie e Cause di morte, X edizione, OMS, 1992, ovvero tutte le lesioni comprese nelle diverse edizioni e revisioni della Classificazione Internazionale delle Malattie per l'Oncologia (ICD-O).

Art. 3

(Finalità specifiche del trattamento di dati)

1. Nell'ambito delle finalità di rilevante interesse pubblico di cui all'articolo 1, il Registro tumori funge da supporto per:

- a) produrre misure dell'incidenza, mortalità, sopravvivenza e prevalenza dei tumori;
- b) descrivere il rischio della malattia per sede e per tipo di tumore, età, genere e ogni altra variabile di interesse per la ricerca scientifica;
- c) svolgere studi epidemiologici sugli andamenti temporali e la distribuzione territoriale dei casi, sui fattori di rischio dei tumori, sugli esiti degli interventi di diagnosi precoce, delle terapie e dei percorsi diagnostico-terapeutici, anche in collaborazione con altri enti e strutture regionali, nazionali e internazionali di ricerca scientifica in campo epidemiologico;
- d) produrre dati anonimi e aggregati per la programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, inerente gli interventi di prevenzione primaria e secondaria rivolti alle persone e all'ambiente di vita e lavoro, nonché dell'efficacia dei programmi di screening;
- e) monitorare e valutare i dati relativi all'appropriatezza e qualità dei servizi diagnostici terapeutici, alla sopravvivenza dei pazienti affetti da tumore.

Art. 4

(Titolare del trattamento dei dati)

1. Titolare del trattamento dei dati personali contenuti nel registro tumori è l'Agenzia regionale sanitaria (ARS) di cui all'articolo 4 della legge regionale 17 luglio 1996, n. 26 (Riordino del servizio sanitario regionale), presso cui è istituito il registro.

2. Nell'ambito delle finalità di cui all'articolo 3, l'ARS garantisce la gestione amministrativa, tecnica e informatica del registro tumori.


DELIBERAZIONE DELLA GIUNTA REGIONALE
Art. 5
(Tipi di dati trattati)

1. Per il perseguimento delle finalità di cui all'articolo 3, il Titolare del trattamento del Registro tumori tratta dati personali idonei a rivelare lo stato di salute riferiti a casi diagnosticati di tumore, nei limiti di quanto indispensabile per il raggiungimento delle predette finalità e nei modi previsti all'articolo 10, nonché nel rispetto delle previsioni delle Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, di cui all'allegato A4 del d.lgs. 196/2003, in quanto compatibili.

2. Il Titolare del trattamento del Registro tumori tratta i seguenti dati.

- a) diagnosi e modalità di ammissione e dimissione, relative a ricoveri e a prestazioni ambulatoriali diagnostico terapeutiche e rispettivi "diagnosis related groups" (DRG);
- b) anamnesi;
- c) interventi chirurgici e procedure diagnostiche e terapeutiche, ivi compresi gli screening oncologici;
- d) indagini cliniche e trattamenti eseguiti;
- e) referti di anatomia patologica;
- f) data e causa di morte e condizioni morbose rilevanti per il decesso.

Art. 6
(Fonti dei dati)

1. Il Titolare del trattamento del Registro tumori effettua la raccolta dei dati di cui all'articolo 5, comma 2, riferiti ai casi diagnosticati di tumore, con le modalità e nel rispetto delle misure di sicurezza di cui all'articolo 32 RGPD, come recepite all'articolo 10, presso:

- a) l'archivio regionale, istituito presso l'ARS, delle schede di dimissioni ospedaliere (SDO), contenenti diagnosi di tumore o relative ai soggetti iscritti o da iscrivere nel registro tumori, al fine di individuare nuovi casi non registrati ovvero, ove necessario, verificare i dati già inseriti nel registro medesimo;
- b) i seguenti archivi costituiti presso gli enti del Servizio Sanitario Regionale (SSR) di cui all'articolo 2 della legge regionale 20 giugno 2003, n. 13 (Riorganizzazione del Servizio sanitario regionale), degli Istituti di ricovero e cura a carattere scientifico (IRCCS) e delle strutture sanitarie private accreditate, limitatamente alle informazioni ivi contenute correlate alle patologie tumorali, al fine di implementare il registro con riferimento ai casi segnalati e aggiornare il registro tumori con l'inserimento di eventuali ulteriori casi:
 - 1) archivi delle schede di morte relativamente ai soggetti con diagnosi di neoplasia definita dal registro tumori e ai soggetti con neoplasia come causa di morte o condizione morbosa rilevante per il decesso;
 - 2) archivi delle cartelle cliniche;
 - 3) archivi di anatomia patologica;
 - 4) archivi di laboratorio e di radiodiagnostica;
 - 5) archivi delle prestazioni ambulatoriali;



DELIBERAZIONE DELLA GIUNTA REGIONALE

- 6) archivi delle prescrizioni farmaceutiche;
 - 7) archivi delle esenzioni ticket per patologia oncologica;
 - 8) archivi delle protesi di interesse oncologico;
 - 9) archivi delle prestazioni di riabilitazione di interesse oncologico;
 - 10) archivio delle vaccinazioni di interesse oncologico;
 - 11) lettere di dimissioni ospedaliere e relazioni cliniche;
- c) l'anagrafe sanitaria regionale degli assistiti per effettuare il raffronto dei dati anagrafici dei soggetti iscritti o da iscrivere nel Registro tumori con i dati anagrafici contenuti nella predetta anagrafe, al fine di verificarne, ove necessario, l'esattezza e l'aggiornamento dei dati e individuare eventuali duplicazioni.

Art. 7*(Comunicazione dei dati)*

1. Il Titolare del trattamento del Registro tumori, per le finalità di cui all'articolo 3, può comunicare le informazioni di cui all'articolo 5, comma 2, ai titolari del trattamento dei dati dei Registri tumori di altre Regioni, qualora legittimamente istituiti e regolamentati ai sensi dell'articolo 6, paragrafo 3, lettera b) del RGPD e dell'articolo 2 ter del d.lgs.196/2003 e previa stipula di apposita convenzione che definisca le modalità tecniche di trasmissione dei dati medesimi in conformità alle misure di sicurezza individuate nell'Allegato 2 del Provvedimento del Garante per la protezione dei dati personali n. 393 del 2 luglio 2015. Tali modalità devono garantire un livello di sicurezza equivalente a quello assicurato dalle misure specificate nel disciplinare tecnico previsto dall'articolo 10 del presente regolamento.

2. Il Titolare del trattamento del Registro tumori, per l'esclusivo perseguimento delle finalità di cui all'articolo 3, può svolgere studi in campo medico, biomedico ed epidemiologico, anche in collaborazione con università, enti e istituti di ricerca e società scientifiche, nonché con ricercatori, singoli o associati, che operano nell'ambito delle predette università, enti e istituti di ricerca e società scientifiche, nel rispetto delle Regole deontologiche per i trattamenti ai fini statistici o di ricerca scientifica di cui all'allegato A.4 al d.lgs. 196/2003.

Art. 8*(Diffusione dei dati)*

1. Il Titolare del trattamento del Registro tumori, per le finalità di cui all'articolo 3, diffonde, anche mediante pubblicazione, dati anonimi relativi ai casi registrati in forma esclusivamente aggregata oppure secondo modalità che non rendano identificabili i soggetti interessati.



DELIBERAZIONE DELLA GIUNTA REGIONALE

Art. 9*(Operatori del Registro Tumori)*

1. I dati personali contenuti nel Registro tumori sono trattati nel rispetto dei principi di cui all'articolo 5 del RGPD, soltanto da personale appositamente individuato dal Titolare del trattamento, in conformità all'articolo 29 del RGPD e dell'articolo 2 quaterdecies del d.lgs. 196/2003, e sottoposto a regole di condotta analoghe al segreto professionale stabilite dal Titolare del trattamento qualora non sia tenuto per legge al segreto professionale.

2. I soggetti di cui al comma 1 accedono ai dati del Registro tumori secondo modalità e logiche di elaborazione strettamente pertinenti e non eccedenti i compiti attribuiti a ciascuno di essi.

Art. 10*(Misure di sicurezza)*

1. Il Titolare del trattamento del Registro tumori adotta ai sensi dell'articolo 32 del RGPD adeguate modalità tecniche e misure di sicurezza dei dati e dei sistemi, specificate nel Disciplinare tecnico contenuto nell'Allegato 1.

2. La sicurezza dei dati trattati dal registro tumori deve essere garantita in tutte le fasi del trattamento dei dati, mediante l'adozione degli opportuni accorgimenti volti a preservare i medesimi dati da rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 11*(Codifica dei dati trattati)*

1. I dati di cui all'articolo 9, comma 1, del RGPD contenuti nel Registro tumori, tenuti con l'ausilio di strumenti elettronici, sono trattati mediante l'utilizzo di codici identificativi, nel rispetto di quanto stabilito dal Disciplinare tecnico contenuto nell'Allegato 1, in modo tale da tutelare l'identità e la riservatezza degli interessati nel trattamento dei dati, rendendoli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità.

2. I dati idonei a rivelare lo stato di salute sono trasmessi al Registro e conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 1 anche quando sono tenuti senza l'ausilio di strumenti elettronici.



DELIBERAZIONE DELLA GIUNTA REGIONALE

Art. 12*(Informativa agli interessati)*

1. Il Titolare del trattamento dei dati del Registro tumori deve fornire l'informativa agli interessati per il tramite delle strutture del SSR, pubbliche o private accreditate che erogano le prestazioni sanitarie, secondo le modalità previste dagli articoli 13 e 14 del RGPD ed è tenuto a garantire agli interessati il pieno e tempestivo esercizio dei diritti previsti da tali articoli.

Art. 13*(Violazione dei dati personali)*

1. Sono comunicate al Garante per la protezione dei dati personali, entro settantadue ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali oggetto di trattamento per la tenuta e il funzionamento del Registro tumori (c.d. data breach) con le modalità previste dall'articolo 33 del RGPD e utilizzando il modello di comunicazione dell'allegato 1 del provvedimento del Garante per la protezione dei dati personali n. 157 del 30 luglio 2019. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica le violazioni all'interessato senza ingiustificato ritardo, con le modalità previste dall'articolo 34 del RGPD.

Art. 14*(Abrogazione)*

1. Il regolamento regionale 9 marzo 2015, n. 3 (Trattamento dei dati inseriti nel registro tumori di cui alla legge regionale 10 aprile 2012, n. 6. Osservatorio epidemiologico regionale. Registri regionali delle cause di morte e di patologia), è abrogato.



DELIBERAZIONE DELLA GIUNTA REGIONALE

Allegato 1

DISCIPLINARE TECNICO IN MATERIA DI MISURE DI SICUREZZA PER IL FUNZIONAMENTO DEL REGISTRO TUMORI IN ATTUAZIONE DELLA LEGGE REGIONALE 10 APRILE 2012, N. 6 (OSSERVATORIO EPIDEMIOLOGICO REGIONALE. REGISTRI REGIONALI DELLE CAUSE DI MORTE E DI PATOLOGIA).**PREMESSA**

In relazione alle misure di sicurezza, individuate dall'articolo 32 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (RGPD), questo disciplinare specifica:

1) le modalità tecniche di raccolta dei dati di cui all'articolo 5, comma 2, del regolamento regionale sul funzionamento del Registro tumori, d'ora in poi Regolamento, presso gli archivi individuati all'articolo 6 del medesimo regolamento, che può avvenire mediante:

a) invio telematico (trasferimento di file con modalità che assicurino la sicurezza del trasporto, PEC, servizi web, c.d. web services, o cooperazione applicativa);

b) accesso diretto degli incaricati del Registro tumori ai sistemi informatici delle strutture sanitarie di cui all'articolo 6 del Regolamento;

c) trasmissione su supporti informatici (es. CD, DVD, memorie a stato solido);

d) trasmissione di documenti cartacei in plico chiuso e sigillato nelle more della messa a regime delle modalità di cui alle lettere a), b) e c).

I supporti di cui alla lettera c) e d) sono utilizzati esclusivamente per estrapolare i dati da inserire nel Registro tumori;

2) le misure di sicurezza che:

a) il Titolare del trattamento del Registro tumori deve adottare nella tenuta e per il funzionamento del registro medesimo;

b) le strutture presso le quali sono raccolti i dati che alimentano il Registro tumori, quali la Regione le aziende sanitarie territoriali e ospedaliere, gli istituti di ricovero e cura a carattere scientifico (IRCCS) nonché le strutture sanitarie private accreditate, devono adottare per comunicare o mettere a disposizione i dati al Titolare del trattamento.

DISPOSIZIONI GENERALI

Il Titolare del trattamento del Registro tumori istruisce gli incaricati, individuati ai sensi dell'articolo 2 quaterdecies del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento UE n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE), sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina in materia di protezione dei dati personali più rilevanti in rapporto alle relative attività, nonché sulle responsabilità che ne derivano.

La sicurezza dei dati contenuti nel Registro tumori deve essere garantita in tutte le fasi del trattamento dei dati, adottando opportuni accorgimenti che preservino i medesimi dati da rischi di distruzione o perdita,



DELIBERAZIONE DELLA GIUNTA REGIONALE

anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. A tal fine si utilizzano tecniche crittografiche con chiavi di cifratura di lunghezza adeguata alla dimensione e al ciclo di vita dei dati personali e si garantisce, ove le finalità non richiedano il loro utilizzo, la separazione dei dati anagrafici da quelli sanitari.

Le postazioni di lavoro informatiche utilizzate per il trattamento dei dati necessari per la tenuta e il funzionamento del Registro tumori, sono dotate di:

- a) sistemi antivirus e *antimalware* costantemente aggiornati;
- b) sistemi di protezione perimetrale, costantemente attivati e adeguatamente configurati in funzione del contesto operativo (*firewall*);
- c) *software* di base e applicativo costantemente aggiornato.

1. FASE DI RACCOLTA DEI DATI

1.1 Il Titolare del trattamento del Registro tumori raccoglie con periodicità semestrale dall'archivio regionale delle schede di dimissioni ospedaliere (SDO) della Regione i dati necessari all'individuazione dei casi diagnosticati di tumore oppure, ove necessario, alla verifica dei dati già presenti nel Registro tumori. Verifica inoltre l'esattezza e l'aggiornamento dei dati anagrafici dei soggetti iscritti o da iscrivere nel Registro tumori mediante il raffronto con i dati contenuti nell'Anagrafe sanitaria regionale degli assistibili.

La raccolta dei dati presso le banche dati e gli archivi di cui all'articolo 6 del Regolamento deve in ogni caso conformarsi alle seguenti modalità:

- a) garantire l'accesso selettivo ai soli dati di cui all'articolo 5 comma 2 del Regolamento;
- b) assegnare al personale incaricato del trattamento credenziali di autenticazione e profili di autorizzazione specifici alle attività di consultazione e raffronto;
- c) predisporre strumenti e procedure per il meccanismo di autorizzazione e autenticazione del personale incaricato al trattamento dei dati nonché per delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati garantendo che:
 - c.1) la raccolta dei dati avvengano soltanto tramite l'uso di postazioni di lavoro appartenenti alla rete IP del Titolare del trattamento del Registro tumori o dotate di certificato digitale, emesso da una *Certification Authority* ufficiale, che identifichi univocamente la postazione di lavoro;
 - c.2) laddove la raccolta dei dati avvenga secondo le modalità della cooperazione applicativa, in forma di *web services*, le condizioni d'uso di tali servizi, che devono individuare idonee garanzie per il trattamento dei dati personali, siano trasposte in appositi accordi di servizio, secondo le specifiche tecniche del Sistema pubblico di connettività (SPC) istituito dal decreto legislativo 7 marzo 2005, n. 82 (Codice dell'amministrazione digitale);
 - c.3) laddove invece la raccolta dei dati avvenga attraverso l'utilizzo di applicazioni web su Internet, vengano impiegati canali di trasmissione protetti (protocolli https/ssl); siano visualizzabili le informazioni relative alla sessione corrente e all'ultima sessione effettuata con le stesse credenziali (con l'indicazione almeno di data, ora e indirizzo di rete da cui è effettuata la connessione); sia asseverata l'identità digitale dei server erogatori di servizi, tramite l'utilizzo di certificati digitali emessi da una *Certification Authority* iscritta all'elenco nazionale dei certificatori attivi;
 - c.4) siano utilizzati sistemi di autenticazione a più fattori per l'abilitazione degli incaricati del registro all'accesso telematico agli archivi delle strutture sanitarie individuate dall'articolo 6, comma 1, del Regolamento, per estrapolare i dati destinati ad alimentare e ad aggiornare il Registro stesso;
 - c.5) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;



REGIONE MARCHE

GIUNTA REGIONALE

seduta del
27 GEN. 2020pag.
13Delibera
36

DELIBERAZIONE DELLA GIUNTA REGIONALE

- c.6) sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;
c.7) siano disattivate le credenziali di autenticazione non utilizzate da almeno sei mesi;

d) effettuare periodiche verifiche, anche a fronte di cambiamenti organizzativi o eventi anomali, circa la sussistenza dei presupposti che hanno originato l'abilitazione degli incaricati. Eventuali esiti negativi delle predette verifiche, devono dar luogo alla tempestiva revisione del profilo di abilitazione, alla eventuale disabilitazione dello stesso o alla disattivazione delle credenziali;

e) prevedere la registrazione in appositi file di *log*, ai fini della verifica della correttezza e legittimità del trattamento dei dati, delle seguenti informazioni: il soggetto (codice identificativo) che ha effettuato l'accesso, la data e l'ora dell'accesso, l'operazione effettuata, l'indirizzo IP della postazione di lavoro e del *server* interconnesso, i dati trattati). Inoltre:

- i *log* sono protetti con idonee misure contro ogni uso improprio;
- i *log* sono conservati per 24 mesi e cancellati alla scadenza;
- i dati contenuti nei *log* sono trattati da personale appositamente incaricato del trattamento esclusivamente in forma aggregata; possono essere trattati in forma non aggregata unicamente laddove ciò risulti indispensabile ai fini della verifica della correttezza e legittimità delle singole operazioni effettuate.

Nel caso di cooperazione applicativa:

- sono conservati i file di *log* degli invii delle informazioni al registro;
- sono conservati i file di *log* delle ricevute del registro;
- a seguito dell'avvenuta ricezione delle ricevute il contenuto delle comunicazioni effettuate è eliminato;

f) utilizzare sistemi di *audit log* per la verifica periodica degli accessi a dati e per il rilevamento delle anomalie.

1.2. Invio telematico. L'invio telematico dei dati al Registro tumori da parte delle aziende sanitarie, degli istituti di ricovero e cura a carattere scientifico e delle strutture sanitarie private accreditate avviene adottando le seguenti misure di sicurezza:

a) utilizzo di canali di trasmissione protetti (FTP sicuro, VPN IPSEC/SSL o HTTPS o sistemi equivalenti) adeguati in relazione allo stato dell'arte dell'evoluzione tecnologica;

b) cifratura dei dati mediante sistemi crittografici basati su protocolli a chiave asimmetrica, la cui componente pubblica è resa nota alle aziende sanitarie, agli istituti di ricovero e cura a carattere scientifico e alle strutture sanitarie private accreditate dal Titolare del trattamento del Registro tumori; la componente "privata" della chiave è conservata in un dispositivo sicuro (*smart card*), assegnato al titolare medesimo, unitamente al relativo P.I.N.;

c) nel caso di utilizzo della PEC, cifratura dei dati sensibili che devono essere riportati in appositi allegati utilizzando gli strumenti di cui al punto b).

Il Titolare del trattamento dei dati del Registro tumori è tenuto a stipulare previamente una convenzione (o altro atto bilaterale) con ciascuno dei soggetti di cui all'articolo 6 del regolamento, secondo uno schema tipo predisposto dalla Regione o Provincia autonoma, volta a definire le specifiche modalità tecniche di raccolta dei dati e le misure di sicurezza nel rispetto di quanto previsto dal presente disciplinare tecnico e dal provvedimento del Garante per la protezione dei dati personali del 2 luglio 2015, recante "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche".



DELIBERAZIONE DELLA GIUNTA REGIONALE

1.3 Accesso diretto degli incaricati del Registro Tumori ai sistemi informatici delle strutture sanitarie. Il Titolare del trattamento dei dati del Registro tumori, per la raccolta delle informazioni di cui all'articolo 5, comma 2, effettuata con modalità informatiche direttamente dai propri incaricati presso i sistemi informatici delle aziende sanitarie, degli istituti di ricovero e cura a carattere scientifico e delle strutture sanitarie private accreditate, è tenuto ad adottare le seguenti misure di sicurezza:

- a) utilizzo di canali di trasmissione protetti (VPN IPSEC/SSL o canali HTTPS);
- b) identificazione, autenticazione, autorizzazione degli incaricati del Registro tumori, abilitati ad accedere alle fonti di dati di cui all'articolo 6 del regolamento.

1.4 Trasmissione su supporti informatici. Il Titolare del trattamento dei dati del Registro tumori, per la raccolta delle informazioni di cui all'articolo 5, comma 2, effettuata mediante trasmissione su supporti informatici, è tenuto ad adottare le seguenti misure di sicurezza:

- a) i supporti informatici, devono essere inseriti in plico chiuso, inviati mediante corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di trasporto e consegna del plico medesimo;
- b) devono essere utilizzati accorgimenti tecnici per garantire l'integrità dei dati contenuti in tali supporti.

1.5 Trasmissione di documenti cartacei. Il Titolare del trattamento dei dati del Registro tumori, per la raccolta delle informazioni di cui all'articolo 5, comma 2, effettuata mediante trasmissione di documenti cartacei è tenuto ad adottare le seguenti misure di sicurezza:

- a) i documenti cartacei devono essere inseriti in plico chiuso, inviati mediante corriere espresso, posta assicurata o recapito a mano, con garanzia di tracciabilità in fase di trasporto e consegna del plico medesimo;
- b) sul plico apporre la dicitura "Contiene dati personali. Riservato agli incaricati del trattamento dell'Osservatorio epidemiologico dell'Agenzia regionale sanitaria (ARS)";
- c) utilizzare plichi o "incarti" non trasparenti al fine di rendere inintelligibile il contenuto;
- d) apporre una firma o sigla sui lembi di chiusura del plico.

È vietato inviare via fax documenti dati oggetto di trattamento.

2. FASE DI ELABORAZIONE DEI DATI

2.1. Ai fini dell'attuazione di quanto previsto all'articolo 11 del Regolamento, il sistema di codifica dei dati identificativi degli interessati raccolti dal Registro tumori deve consistere in un numero predefinito di caratteri alfanumerici ottenuti attraverso procedure di cifratura invertibili, con algoritmo biunivoco e reversibile.

2.2. I dati raccolti nel Registro tumori sono trattati dagli incaricati del Registro tumori esclusivamente attraverso applicazioni *software* dotate di adeguati sistemi di autenticazione e di autorizzazione in funzione del ruolo degli incaricati e delle esigenze di accesso e trattamento dei dati, avendo cura di delimitare nel tempo e nella localizzazione sulla rete la possibilità di accesso ai medesimi dati e di predisporre meccanismi per la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi. Tali applicazioni devono possedere le seguenti caratteristiche:

- a) un sistema di autenticazione a più fattori;
- b) sia vietata la possibilità di effettuare accessi contemporanei con le medesime credenziali;
- c) sia vietato l'utilizzo di dispositivi automatici che consentano di consultare i dati in forma massiva;



DELIBERAZIONE DELLA GIUNTA REGIONALE

d) siano visualizzabili le informazioni relative alla sessione corrente e all'ultima sessione effettuata con le stesse credenziali (con l'indicazione almeno di data, ora e indirizzo di rete da cui è effettuata la connessione).

2.3 Le postazioni di lavoro utilizzate per il trattamento dei dati devono appartenere alla rete IP del Titolare del trattamento del Registro tumori o essere dotate di certificato digitale, emesso da una *Certification authority* ufficiale, che identifichi univocamente la postazione di lavoro.

2.4 Devono essere altresì adottate le misure di sicurezza e gli accorgimenti tecnici specificati nelle lettere d), e) e f) del punto 1.1 del presente disciplinare.

3. FASE DI CONSERVAZIONE DEI DATI

3.1 I dati raccolti dal Titolare del trattamento del Registro tumori, codificati ai sensi del punto 2.1, devono essere memorizzati e conservati in luoghi e con modalità prestabilite dal titolare stesso, in modo tale da proteggere l'identità e tutelare la riservatezza degli interessati.

3.2 I dati di cui al punto 3.1 devono essere conservati con garanzie di riservatezza, integrità e disponibilità, con conseguente possibilità di ripristino dei dati stessi in caso di guasti e malfunzionamenti, per un periodo di 1 anno, al fine di eventuali successive verifiche e integrazione dei dati.

3.3 Il ripristino dei dati di cui al punto 3.1 deve avvenire secondo una documentata procedura di *restore*, prestabilita dal Titolare del trattamento.

3.4 I supporti informatici e i documenti cartacei contenenti i dati del registro devono essere riposti dagli incaricati in appositi archivi, organizzati secondo una documentata procedura relativa alla nomenclatura e alla classificazione dei supporti in modo che siano univocamente identificabili, soltanto attraverso apposito codice in caso di necessità e di verifica.

4. ACCESSO AI LOCALI DEL REGISTRO TUMORI

4.1. L'accesso ai locali del Registro tumori, ivi compresi i locali destinati a ospitare gli archivi di supporti informatici o cartacei, deve avvenire secondo una documentata procedura, prestabilita dal Titolare del trattamento, che preveda l'identificazione delle persone che accedono e la registrazione degli orari di ingresso e uscita di tali persone.

5. MANUTENZIONE DEI SISTEMI INFORMATICI

5.1. Nel rispetto di quanto prescritto dall'articolo 28 del RGPD, i soggetti esterni che effettuino delle attività di manutenzione dei sistemi informatici, che possono comportare il trattamento dei dati del Registro tumori, devono essere designati Responsabili del trattamento in *outsourcing*.

5.2. I contratti di manutenzione, stipulati con i soggetti di cui al punto 5.1, devono prevedere specifiche clausole di riservatezza dei dati, la registrazione degli interventi con l'indicazione degli orari di inizio e fine, le persone che li hanno effettuati e le motivazioni che hanno determinato la necessità dei medesimi interventi.



DELIBERAZIONE DELLA GIUNTA REGIONALE

6. CANCELLAZIONE DEI DATI E DISMISSIONE DEI SUPPORTI E DOCUMENTI CONTENENTI DATI

6.1. I dati presenti nel sistema informatico del Registro tumori devono essere cancellati o resi anonimi in maniera irreversibile trascorso un periodo di 30 anni dal decesso dell'interessato cui i dati si riferiscono.

6.2 La procedura di anonimizzazione di cui al punto precedente deve adottare tecniche adeguate alla protezione dell'identità del paziente da rischi legati all'identificabilità mediante individuazione, correlabilità e deduzione a partire dai dati sanitari. Devono essere applicate tecniche di randomizzazione e generalizzazione dei dati, tenuto conto dell'evoluzione tecnologica, in modo da mantenere nel complesso la distribuzione degli elementi rilevanti per finalità di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria espressamente previsti dal Regolamento all'articolo 3 comma 1 lettera d).

6.3. I supporti informatici (es. memorie di massa dei *server* e delle postazioni di lavoro, supporti rimovibili) del Registro tumori devono essere dismessi secondo quanto previsto dal provvedimento del Garante per la protezione dei dati personali del 13 ottobre 2008 sui "Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali" (G.U. n. 287 del 9 dicembre 2008).

6.4. I supporti cartacei del Registro tumori, contenenti dati sanitari, devono essere distrutti secondo una documentata procedura, prestabilita dal Titolare del trattamento, entro un periodo di 10 anni dal decesso dell'interessato, cui i dati si riferiscono.

Istituzione del registro tumori di popolazione della Regione Lazio (1)

Numero della legge: 7

Data: 12 giugno 2015

Numero BUR: 48

Data BUR: 16/06/2015

L.R. 12 Giugno 2015, n. 7

Istituzione del registro tumori di popolazione della Regione Lazio (1)

Art. 1

(Istituzione e finalità del Registro tumori di popolazione della Regione Lazio)

1. La presente legge istituisce il Registro tumori di popolazione della Regione Lazio, di seguito denominato Registro tumori della Regione Lazio, con una copertura estesa a tutto il territorio regionale.

2. Le finalità programmatiche del Registro tumori della Regione Lazio sono così definite:

- a) realizzare la raccolta, l'elaborazione e la registrazione di dati statistici completi, di buona qualità e validati scientificamente, provenienti da molteplici fonti di flussi informativi in campo sanitario, per incidenza, prevalenza e sopravvivenza, secondo l'andamento spaziale e temporale, dei casi di tumore anche infantili che si verificano nella popolazione della Regione;
- b) rappresentare uno strumento di consultazione per progetti regionali, nazionali ed internazionali, di ricerca anche transnazionale in oncologia;
- c) essere di supporto per piani regionali per le cure palliative e terapia del dolore;
- d) contribuire, attraverso i dati prodotti, alla valutazione dell'appropriatezza dei trattamenti terapeutici in oncologia, alla rilevazione di eventuali differenze nell'accesso alle cure erogate al paziente oncologico, in relazione alle condizioni socio-economiche e all'area geografica di provenienza;
- e) consentire interventi mirati di prevenzione primaria e valutazioni per l'attivazione di campagne specifiche di diagnosi precoce oncologica quali screening oncologici;
- f) essere strumento di monitoraggio sull'efficacia dei programmi di screening oncologici, tradizionali e/o sperimentali attivi ed operativi presso le aziende sanitarie locali della Regione;
- g) essere strumento di supporto per gli studi epidemiologici finalizzati all'analisi dell'impatto dell'ambiente sull'incidenza della patologia oncologica, attraverso uno studio integrato matrici ambientali-matrici umane;
- h) realizzare un'informazione continua e completa nei confronti della popolazione della Regione anche in relazione ad episodi di concentrazioni spazio-temporali di casi oncologici (cluster).

Art. 2

(Organizzazione e gestione del Registro tumori della Regione Lazio)

1. Il Registro tumori della Regione Lazio costituisce parte integrante del Sistema informativo sanitario regionale.

2. Il Registro tumori della Regione Lazio è allocato presso il dipartimento di epidemiologia del Servizio sanitario regionale, di seguito denominato DEP Lazio, ed è collegato funzionalmente a cinque Unità come di seguito indicate:

- a) Unità funzionale della Città metropolitana di Roma presso l'Istituto nazionale tumori "Regina Elena" (IRCCS – IFO);
- b) Unità funzionale presso l'azienda sanitaria locale Frosinone;
- c) Unità funzionale presso l'azienda sanitaria locale Latina;
- d) Unità funzionale presso l'azienda sanitaria locale Rieti;
- e) Unità funzionale presso l'azienda sanitaria locale Viterbo;
- f) Unità funzionale regionale dei tumori infantili presso il DEP Lazio.

3. Il responsabile del Registro tumori della Regione Lazio è nominato dal direttore del DEP Lazio, individuato tra i direttori delle Unità operative complesse del dipartimento medesimo, con documentata esperienza almeno decennale in epidemiologia.

4. Per i fini di cui al comma 2, il direttore generale delle aziende sanitarie locali e dell'Istituto

nazionale tumori "Regina Elena" (IRCCS – IFO) entro sessanta giorni dalla data di entrata in vigore della presente legge identifica l'Unità operativa presso la quale è allocata la relativa Unità funzionale, il referente medico responsabile ed il personale addetto alla rilevazione, codifica ed archiviazione dei casi.

5. L'Unità funzionale regionale dei tumori infantili provvede alla registrazione dei dati relativi agli ammalati di tumore della Regione per le fasce di età da zero ai quattordici anni e dai quindici ai diciannove anni.

6. Le attività del Registro tumori della Regione Lazio hanno carattere continuativo.

7. Per facilitare l'interscambio, anche a livello nazionale, dei flussi informativi tra i diversi registri tumori secondo quanto indicato dal Piano oncologico nazionale (PON) 2010-2012, il Registro tumori della Regione Lazio provvede ad accreditarsi presso l'Associazione italiana registri tumori (AirTum Onlus) per inserire i dati prodotti nella banca dati AirTum (AirTum BD), secondo procedure tecniche indicate nei protocolli AirTum sulla definizione delle norme di accesso alla banca dati stessa.

Art. 3

(Fonti dei flussi informativi e organizzazione delle attività)

1. Il Registro tumori della Regione Lazio procede alle attività di rilevamento, catalogazione, elaborazione e registrazione dei dati individuali, sanitari e amministrativi sugli ammalati di tumore, attraverso l'utilizzo delle seguenti fonti di flussi informativi in campo sanitario:

- a) schede di dimissione ospedaliera (SDO);
- b) schede di morte trasmesse dal Registro nominativo delle cause di morte (ReNCaM);
- c) schede di morte trasmesse dagli archivi anagrafici comunali;
- d) banche dati dell'anagrafe degli assistiti;
- e) archivio dei referti dei servizi di anatomia patologica di cui all'articolo 9;
- f) archivio delle prescrizioni appartenenti alla farmaceutica ospedaliera (File-F);
- g) archivio delle prestazioni specialistiche ambulatoriali;
- h) registri di esenzione ticket per patologia oncologica;
- i) banche dati dell'Istituto nazionale di previdenza sociale (INPS) sulle attività delle commissioni per l'invalidità civile;
- l) banca dati dell'Associazione italiana ematologia oncologia pediatrica (AIEOP).

2. Per le attività di cui al comma 1, il regolamento regionale di cui all'articolo 13 definisce le modalità dell'estrazione dei dati dai flussi informativi, la periodicità della trasmissione dei dati al responsabile dell'Unità funzionale nonché la periodicità del flusso dei dati dalle Unità funzionali al DEP Lazio.

3. I servizi clinici ospedalieri sono tenuti alla collaborazione con le Unità funzionali per la raccolta dei dati non inclusi nei sistemi informativi correnti, quali cartelle cliniche e referti radiologici, su richiesta dei responsabili dell'Unità funzionale medesima.

4. Il Registro tumori della Regione Lazio e le Unità funzionali possono utilizzare qualunque altra fonte di flussi informativi ritenuta utile e/o necessaria per le finalità di cui alla presente legge. In particolare per i tumori ematologici possono essere utilizzati database specializzati, supportati da reti relative a linfomi e mielodisplasie.

Art. 4

(Collaborazione dei comuni)

1. I comuni collaborano alle operazioni svolte dal Registro tumori della Regione Lazio sui dati sanitari ed amministrativi degli ammalati e provvedono ad indicare la sezione di censimento dell'Istituto nazionale di statistica (ISTAT).

Art. 5

(Istituzione del Comitato tecnico-scientifico del Registro tumori della Regione Lazio)

1. E' istituito il Comitato tecnico-scientifico del Registro tumori della Regione Lazio, di seguito denominato Comitato tecnico-scientifico, che si riunisce ogni sei mesi presso l'assessorato regionale competente in materia di sanità.

2. I membri del Comitato tecnico-scientifico restano in carica tre anni, salvo rinnovo, e sono:
- a) il direttore del DEP Lazio con funzioni di coordinatore;

- b) i direttori generali delle aziende sanitarie locali o loro delegati;
 - c) il direttore generale dell'Istituto nazionale tumori "Regina Elena" (IRCCS- IFO);
 - d) il responsabile del Registro mesoteliomi della Regione Lazio o suo delegato;
 - e) il responsabile regionale della Società italiana di anatomia patologica e citologia diagnostica (SIAPEC-IAP) o suo delegato;
 - f) un componente delegato, nominato dall'Associazione italiana registri tumori (AirTum Onlus);
 - g) un componente delegato nominato dalla Rete oncologica regionale e dall'Associazione italiana di oncologia medica (AIOM);
 - h) un componente delegato dalle associazioni di tutela dei diritti del malato;
 - i) un componente delegato dall'Associazione italiana ematologia oncologica pediatrica (AIEOP).
3. Il Comitato tecnico-scientifico ha funzioni di indirizzo, di controllo degli standard e dei sistemi e metodi utilizzati, di valutazione di qualità e di adesione a linee guida, di formazione e di aggiornamento.

Art. 6

(Coordinamento del Registro tumori della Regione Lazio)

1. Al fine di coordinare le attività del Registro tumori della Regione Lazio, il DEP Lazio indice, con cadenza trimestrale, riunioni di coordinamento a cui partecipano:
- a) il direttore del DEP Lazio o suo delegato;
 - b) il referente della registrazione dei tumori infantili del DEP Lazio;
 - c) i responsabili delle Unità funzionali;
 - d) un funzionario nominato dall'assessorato regionale competente in materia di sanità.
2. Nelle riunioni di cui al comma 1 si provvede:
- a) a monitorare l'andamento della raccolta e della gestione dei dati prodotti da ciascuna Unità funzionale nonché della raccolta dei dati dei tumori infantili;
 - b) alla validazione scientifica dei dati prodotti e trasmessi periodicamente dalle Unità funzionali al DEP Lazio;
 - c) a redigere ogni tre mesi una relazione sulle attività del Registro tumori della Regione Lazio che viene trasmessa al Comitato tecnico-scientifico;
 - d) a supportare, in collaborazione con l'Associazione italiana registri tumori (AirTum Onlus), le attività di formazione individuate dal Comitato tecnico-scientifico ed a partecipare all'elaborazione dei relativi programmi di formazione.

Art. 7

(Spese per le attività del Registro tumori della Regione Lazio)

1. Le voci di spesa ammissibili per lo svolgimento delle attività del Registro tumori della Regione Lazio, con obbligo di rendicontazione analitica annuale all'assessorato regionale competente in materia di sanità, sono le seguenti:
- a) acquisto di beni strumentali, ivi compresi sistemi hardware e software;
 - b) spese per le attività di coordinamento di cui all'articolo 6 e del Comitato tecnico-scientifico;
 - c) spese per comunicazioni e informazioni con particolare riguardo alla pubblicazione di atti e/o documenti, anche su richiesta;
 - d) spese generali.
2. I componenti del Comitato tecnico-scientifico operano a titolo gratuito.

Art. 8

(Rapporti di cooperazione del Registro tumori della Regione Lazio con i medici di medicina generale e con i pediatri di libera scelta)

1. I medici di medicina generale, prevalentemente in forma associata, ed i pediatri di libera scelta partecipano alle attività del Registro tumori della Regione Lazio, e sono tenuti a collaborare per la raccolta dei dati relativi a casi accertati o sospetti di tumori nonché a casi in cui le terapie hanno mostrato la loro efficacia.

Art. 9

(Istituzione del Registro dei referti dei servizi di anatomia patologica)

1. Per le finalità della realizzazione del Registro tumori della Regione Lazio è istituito il Registro dei referti dei servizi di anatomia patologica (RSAP) che rappresenta la fonte di dati

per l'accertamento diagnostico delle patologie tumorali e per la determinazione della morfologia, della topografia, dello stadio e grado della malattia nonché degli effetti prodotti dalle terapie adottate.

2. Il RSAP raccoglie i dati dei referti dei servizi di anatomia patologica relativi a prelievi e a pezzi operatori di interesse oncologico.

3. La banca dati è realizzata nell'ambito del Sistema informativo regionale, che si avvale del supporto di Lait S.p.A., e gestita dal DEP Lazio in collaborazione con l'assessorato regionale competente in materia di sanità e con i servizi di anatomia patologica pubblici e accreditati della Regione.

4. Il regolamento regionale di cui all'articolo 13 definisce:

a) l'iter per la realizzazione del RSAP;

b) l'assegnazione delle competenze per la definizione della standardizzazione nella refertazione e nella codifica topografica e morfologica, per la definizione di un tracciato record e per l'allestimento della piattaforma informatica;

c) le misure adottate per la protezione dei dati personali;

d) la quota parte del finanziamento per il Registro tumori della Regione Lazio e per il RSAP necessaria per l'avvio del sistema.

5. I servizi di anatomia patologica sono tenuti ad adattare i propri sistemi informativi in relazione alla necessità di implementare il flusso centrale, secondo gli standard definiti.

Art. 10

(Monitoraggio delle attività del Registro tumori della Regione Lazio)

1. In caso di interruzione della trasmissione delle fonti dei flussi informativi di cui alla presente legge per un periodo superiore a un mese, il Comitato tecnico-scientifico provvede ad inviare apposito sollecito formale al responsabile che gestisce la fonte del flusso informativo di cui si è interrotta la trasmissione, fissando un termine non superiore a quindici giorni per ripristinare le procedure informatizzate di trasmissione.

2. Il DEP Lazio provvede alla pubblicazione dei dati statistici registrati dal Registro tumori della Regione Lazio entro il 31 dicembre su apposita sezione del sito web della Regione dal titolo "Registro tumori di popolazione della Regione Lazio".

3. Entro il 31 marzo di ogni anno la direzione regionale competente in materia di sanità presenta alla commissione consiliare competente una relazione sullo stato delle attività del Registro tumori della Regione Lazio evidenziando:

a) il grado di conseguimento delle finalità programmatiche del Registro tumori della Regione Lazio;

b) l'eventuale interruzione della trasmissione telematica di flussi informativi, le azioni poste in essere per ripristinare le procedure di trasmissione dei dati e la loro efficacia;

c) le altre eventuali criticità emerse nello svolgimento delle attività;

d) l'utilizzo dei dati prodotti e registrati per la programmazione sanitaria regionale.

4. La relazione di cui al comma 3 è pubblicata su apposita sezione del sito web della Regione dal titolo "Registro tumori di popolazione della Regione Lazio".

Art. 11

(Richiesta di elaborazione ed estrazione di dati statistici dal Registro tumori della Regione Lazio)

1. Il Registro tumori della Regione Lazio produce elaborazioni ed estrazioni di dati statistici sugli ammalati di tumore in riferimento a determinate aree geografiche subcomunali, anche su richiesta di enti pubblici, aziende ospedaliere, università, amministratori locali, studi medici, ricercatori, cittadini, associazioni di volontariato e/o fondazioni con qualifica di onlus.

2. La richiesta di cui al comma 1, depositata presso il Registro tumori della Regione Lazio, deve essere motivata da fini scientifici e/o di studio e/o processuali specificati nella domanda.

3. Il responsabile del Registro tumori della Regione Lazio provvede a fornire risposta scritta entro centoventi giorni, previo parere vincolante del Comitato tecnico-scientifico.

Art. 12

(Rapporti di cooperazione del Registro tumori della

**Regione Lazio con le associazioni di volontariato
e/o con fondazioni con qualifica di onlus)**

1. La presente legge promuove forme di partecipazione delle associazioni di volontariato e/o delle fondazioni con qualifica di onlus alle attività del Registro tumori della Regione Lazio.
2. Le associazioni e/o fondazioni di cui al comma 1, attive nel settore della tutela della salute umana e della prevenzione oncologica, possono chiedere audizioni al Comitato tecnico-scientifico.

**Art. 13
(Regolamento)**

1. Entro novanta giorni dalla data di entrata in vigore della presente legge, la Giunta regionale, sentita la commissione consiliare competente in materia di sanità, adotta, ai sensi dell'articolo 47, comma 2, lettera b), dello Statuto, un regolamento (2) che definisce contenuti, tempi, strumenti dei flussi informativi, inclusa la definizione delle spese di cui all'articolo 7. In particolare definisce compiti e attività del DEP Lazio e delle Unità funzionali di cui all'articolo 2.
2. Il regolamento definisce inoltre le modalità di attuazione della normativa statale in materia di protezione dei dati personali, in conformità al parere espresso dal Garante per la protezione dei dati personali ai sensi degli articoli 20 e 154, comma 1, lettera g), del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) e successive modifiche. Vengono definiti le tipologie di dati sensibili, le operazioni eseguibili, le specifiche finalità perseguite dal registro, i soggetti che possono avere accesso ai registri e le misure per la custodia e per la sicurezza dei dati.

**Art. 14
(Clausola valutativa)**

1. Il Consiglio regionale, tramite la commissione consiliare competente, esercita il controllo sull'attuazione della presente legge e ne valuta i risultati ottenuti. A tal fine la Giunta regionale, trascorsi due anni dalla data di entrata in vigore della presente legge e con successiva periodicità biennale, avvalendosi anche dei dati e delle informazioni prodotte dal Comitato tecnico-scientifico, presenta al Consiglio regionale una relazione sullo stato di attuazione e sull'efficacia della legge. In particolare la relazione dovrà contenere dati e informazioni su:
 - a) livello raggiunto relativo alla mappatura di tutte le patologie tumorali nel territorio regionale;
 - b) interventi da parte della Giunta regionale nella programmazione sanitaria e nella rimodulazione dell'offerta sanitaria territoriale ed ospedaliera, anche in termini di campagne di prevenzione specifiche per aree geografiche o tipologia di screening, che tengano conto delle analisi e delle ricerche elaborate grazie ai dati raccolti dal Registro tumori della Regione Lazio;
 - c) criticità riscontrate nella gestione del Registro tumori della Regione Lazio, in particolare le anomalie nella corretta e completa ricezione dei flussi di dati, e interventi posti in essere per ridurre al minimo le interruzioni.
2. La Regione può promuovere forme di valutazione partecipata coinvolgendo cittadini e soggetti attuatori degli interventi previsti.
3. Le competenti strutture del Consiglio e della Giunta regionale si raccordano per la migliore valutazione della presente legge.

**Art. 15
(Disposizioni transitorie e finali)**

1. Il Registro tumori della Provincia di Latina e il Registro tumori della Provincia di Viterbo, così come altri registri comunali preesistenti alla data di entrata in vigore della presente legge, continuano la loro attività di raccolta, elaborazione e registrazione dei dati sugli ammalati di tumore secondo quanto previsto dai protocolli di intesa adottati in materia fino alla data di entrata in vigore della presente legge.
2. Entro un anno dalla data di entrata in vigore della presente legge i Registri tumori di cui al comma 1 si adeguano al sistema di rilevazione previsto dalla presente legge e si costituiscono in Unità funzionali.
3. I Registri tumori di cui al comma 1 sono tenuti inoltre ad inviare al DEP Lazio tutti i dati retrospettivi raccolti dalla data di inizio della loro istituzione, al fine di implementare il Registro tumori della Regione Lazio.

4. Il Comitato tecnico-scientifico si riunisce entro due mesi dalla data di entrata in vigore del regolamento di cui all'articolo 13.
5. Entro tre mesi dalla data di entrata in vigore del regolamento di cui all'articolo 13 il DEP Lazio provvede ad attivare il Registro tumori della Regione Lazio in collegamento con le Unità funzionali di cui all'articolo 2.
6. Entro quattro mesi dalla data di entrata in vigore della presente legge è indetta la prima riunione di coordinamento di cui all'articolo 6.
7. Entro tre anni dalla data di entrata in vigore della presente legge il Registro tumori della Regione Lazio provvede all'accreditamento presso l'AirTum Onlus ai sensi dell'articolo 2, comma 7.

Art. 16

(Clausola di salvaguardia e disposizione finanziaria)

1. Le disposizioni della presente legge si applicano in quanto compatibili con le previsioni del piano di rientro dal disavanzo sanitario della Regione e con quelle dei programmi operativi di cui all'articolo 2, comma 88 della legge 23 dicembre 2009, n. 191 (Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato – Finanziaria 2010) e con le funzioni attribuite al commissario ad acta per la prosecuzione del piano di rientro dal disavanzo sanitario.
2. Fermo restando quanto previsto dal comma 1, agli oneri necessari ai fini dell'adozione delle prime misure attuative di cui alla presente legge si fa fronte mediante l'istituzione, nell'ambito del programma 07 "Ulteriori spese in materia sanitaria" della missione 13 "Tutela della salute", di un apposito fondo denominato: "Fondo per le attività del Registro Tumori della Regione Lazio", nel quale confluiscono, per l'anno 2015, le risorse pari a 100.000,00 euro, iscritte a legislazione vigente, a valere sulla medesima annualità, nel fondo speciale di parte corrente di cui al programma 03 "Altri fondi" della missione 20 "Fondi ed accantonamenti".

Note:

- (1) Legge pubblicata sul Bollettino ufficiale della Regione del 16 giugno 2015, n. 48
- (2) Vedi regolamento regionale 15 novembre 2017, n. 28 (BUR 21 novembre 2017, n. 93)

Il testo non ha valore legale; rimane, dunque, inalterata l'efficacia degli atti legislativi originari.



Regolamento regionale 15 Novembre 2017 n. 28

[Condividi](#)

BUR 21 Novembre 2017, n. 93

Consiglio regionale della Calabria
Testo vigente al: 14/05/2021

III Commissione

Regolamento di attuazione e integrazione della Legge regionale 12 giugno 2015, n. 7 (Istituzione del Registro tumori di popolazione della Regione Lazio).

(Oggetto)

1. Il presente regolamento, adottato ai sensi dell'articolo 13 della legge regionale 12 giugno 2015, n. 7 (Istituzione del registro tumori di popolazione della Regione Lazio), di seguito denominata legge, nel rispetto delle disposizioni di cui al decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), definisce le modalità di funzionamento del registro tumori della Regione Lazio, di seguito denominato registro tumori, e in particolare:

- a) le finalità perseguite dal registro;
- b) i tipi di dati sensibili trattati e le operazioni eseguibili;
- c) i soggetti che possono trattare i dati di cui alla lettera b);
- d) l'assetto organizzativo e le modalità di funzionamento del registro;
- e) le modalità da adottare per tutelare l'identità e la riservatezza degli individui i cui dati sensibili sono contenuti nel registro;
- f) la definizione delle voci di spesa ammissibili per lo svolgimento delle attività del Registro di cui all'articolo 7 della legge.

Art. 2

(Finalità del Registro)

1. Ai sensi degli articoli 85, comma 1, lettera b) e 98, comma 1, lettera c) del d.lgs. 196/2003, nell'ambito delle finalità programmatiche individuate dall'articolo 1, comma 2, della legge, nonché delle finalità di carattere scientifico perseguite dal servizio sanitario regionale, il registro tumori raccoglie, elabora e registra i casi diagnosticati di tumore allo scopo di:

- a) produrre misure dell'incidenza, mortalità, sopravvivenza e prevalenza dei tumori;
- b) descrivere il rischio della malattia per sede e per tipo di tumore, età, genere ed ogni altra variabile di interesse per la ricerca scientifica;
- c) svolgere studi epidemiologici sui fattori di rischio dei tumori, sugli esiti degli interventi di diagnosi precoce, delle terapie e dei percorsi diagnostico-terapeutici;
- d) svolgere studi epidemiologici finalizzati all'analisi dell'impatto dell'ambiente e valutazione di episodi di concentrazione spazio-temporali dei casi oncologici.

Art. 3

(Definizioni)

[Cookie policy](#) |

1. Ai fini del presente regolamento si applicano le definizioni di cui all'articolo 4 del d.lgs. 196/2003.

2. In aggiunta a quanto previsto al comma 1, ai fini del presente regolamento, si intende per:

- a) registro tumori, l'archivio informatizzato che in maniera continuativa e sistematica raccoglie, organizza ed elabora dati personali, amministrativi e sanitari relativi a casi di neoplasia riferiti a soggetti residenti nella Regione a fini di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;
- b) tumore (neoplasia, cancro, malattia oncologica), la malattia a carattere evolutivo, come descritta nelle classificazioni internazionali delle malattie e delle cause di morte dell'organizzazione mondiale della sanità e tutte le lesioni rappresentate nelle diverse edizioni e revisioni della classificazione internazionale delle malattie per l'oncologia;
- c) DEP Lazio, il Dipartimento di epidemiologia del Servizio sanitario regionale -ASL Roma 1, di cui all'articolo 35 della legge regionale 28 giugno 2013 n. 4 (Disposizioni urgenti di adeguamento all'articolo 2 del decreto legge 10 ottobre 2012, n. 174, convertito, con modificazioni, dalla legge 7 dicembre 2012, n. 213, relativo alla riduzione dei costi della politica, nonché misure in materia di razionalizzazione, controlli e trasparenza dell'organizzazione degli uffici e dei servizi della Regione);
- d) casi incidenti, i nuovi casi di una specifica patologia che si verificano in una determinata popolazione in un determinato periodo di tempo.

Art. 4

(Titolare del trattamento dei dati)

1. Il titolare del trattamento dei dati contenuti nel registro è il DEP Lazio presso il quale è allocato il registro tumori ai sensi dell'articolo 2, comma 2, della legge.

Art. 5

(Organizzazione del registro)

1. Ai sensi dell'articolo 2 della legge, il registro tumori costituisce parte integrante del Sistema informativo sanitario regionale ed è gestito dal DEP Lazio, in raccordo con la Direzione regionale competente.

2. Il registro tumori è collegato alle seguenti Unità funzionali (UF):

- a) Unità funzionale della Città metropolitana di Roma, presso l'Istituto nazionale tumori "Regina Elena" (IRCCS – IFO);
- b) Unità funzionale presso l'azienda sanitaria locale Frosinone;
- c) Unità funzionale presso l'azienda sanitaria locale Latina;
- d) Unità funzionale presso l'azienda sanitaria locale Rieti;
- e) Unità funzionale presso l'azienda sanitaria locale Viterbo;
- f) Unità funzionale regionale dei tumori infantili presso il DEP Lazio.

3. Le UF contribuiscono ad alimentare la base dati del registro tumori, a verificare la storia clinica dei casi, a codificare i casi stessi e collaborano alle attività epidemiologiche del registro tumori.

4. Ai sensi dell'articolo 2, comma 3, della legge e ai fini del coordinamento delle attività necessarie per l'organizzazione del registro tumori, il DEP Lazio provvede alla nomina del responsabile del registro tumori medesimo individuandolo tra i direttori delle unità operative complesse del DEP Lazio medesimo, con documentata esperienza almeno decennale in epidemiologia. Il responsabile del registro tumori è anche il responsabile del trattamento dei dati ivi contenuti ai sensi dell'articolo 4, comma 1, lettera g) del d.lgs. 196/2003.

5. Ai sensi dell'articolo 2, comma 4, della legge i direttori generali delle strutture di cui al comma 2 individuano:

- a) le unità operative presso le quali sono allocate le UF;
- b) i referenti medici responsabili delle UF ed il personale addetto alla rilevazione, codifica ed archiviazione dei casi.

6. Nel rispetto degli articoli 29 e 30 del d.lgs. 196/2003, il DEP Lazio designa, per le singole UF:

- a) i referenti medici, di cui al comma 5, quali responsabili del trattamento dei dati personali relativi al registro;
- b) il personale addetto alla rilevazione, codifica ed archiviazione dei casi, quale personale incaricato al trattamento dei dati personali relativi al registro.

7. Il DEP Lazio, nell'ambito delle finalità di cui all'articolo 2, garantisce la gestione amministrativa, tecnica e informatica del registro tumori e, ai sensi dell'articolo 6 della legge, ne coordina le attività, attraverso riunioni periodiche, al fine di:

- a) monitorare l'andamento della raccolta e della gestione dei dati prodotti da ciascuna UF nonché della raccolta dei dati dei tumori infantili;
- b) validare i dati prodotti periodicamente dalle UF al DEP Lazio;
- c) redigere relazioni con periodicità trimestrale sulle attività del registro tumori, da trasmettere al Comitato tecnico-

scientifico di cui all'articolo 5 della legge;

d) supportare, in collaborazione con l'Associazione Italiana Registri Tumori (AirTum Onlus), le attività di formazione individuate dal Comitato Tecnico Scientifico e partecipare all'elaborazione dei relativi programmi di formazione.

8. Alle riunioni di coordinamento partecipa un rappresentante della Direzione regionale competente in materia di sistema informativo sanitario regionale.

Art. 6

(Tipologia di dati sensibili trattati)

1. Per il perseguimento delle finalità di cui all'articolo 2, il titolare del trattamento dei dati contenuti nel registro tumori tratta i dati personali, sanitari e amministrativi, idonei a rivelare lo stato di salute, riferiti a casi diagnosticati di tumore, nei limiti di quanto indispensabile per il raggiungimento delle predette finalità e nei modi previsti dal presente regolamento, nonché nel rispetto di quanto previsto dal Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici di cui all'allegato A.4 del d.lgs. n. 196/2003, in quanto compatibili.

2. Il titolare del trattamento dei dati contenuti nel registro tumori tratta i dati relativi a:

a) diagnosi e modalità di ammissione e dimissione, relative a ricoveri e a prestazioni diagnostico-terapeutiche;

b) anamnesi;

Consiglio regionale della Calabria

III Commissione

~~c) interventi chirurgici e procedure diagnostiche e terapeutiche, ivi compresi gli screening oncologici;~~

d) indagini clinico - strumentali e trattamenti eseguiti;

e) referti di anatomia patologica;

f) data e causa di morte e condizioni morbose rilevanti per il decesso.

Art. 7

(Fonti dei flussi informativi)

1. Ai fini della tenuta del registro, le operazioni di raccolta, elaborazione e registrazione dei dati personali, sanitari e amministrativi, sugli ammalati di tumore sono realizzate attraverso l'utilizzo delle fonti di flussi informativi esistenti in campo sanitario, con le modalità e nel rispetto delle misure di sicurezza di cui al titolo V, della parte I del d.lgs. 196/2003 nonché di quelle individuate all'allegato A.

2. Le attività connesse alle operazioni di cui al comma 1 sono consentite se rientrano tra le attività previste per le operazioni inerenti il trattamento dei dati di cui all'articolo 1, comma 1, lettera a), del d.lgs. 196/2003.

3. Limitatamente ai dati personali indispensabili all'individuazione dei casi di neoplasia, le fonti di cui al comma 1 sono quelle individuate dall'articolo 3 della legge e, in particolare:

a) dai seguenti flussi informativi regionali:

1) schede di dimissioni ospedaliere (SDO);

2) sistemi informativi di mortalità;

3) sistemi informativi regionali delle prestazioni ambulatoriali;

4) sistema informativo delle prescrizioni farmaceutiche;

5) archivio regionale delle esenzioni ticket;

6) archivio regionale della prestazioni di riabilitazione di interesse oncologico;

7) anagrafe degli assistiti;

b) dai seguenti archivi delle aziende sanitarie territoriali e ospedaliere, degli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) e delle strutture sanitarie private accreditate:

1) archivi delle cartelle cliniche;

2) archivi di anatomia patologica, nelle more dell'attuazione delle disposizioni di cui all'articolo 11;

3) archivi di laboratorio e di radiodiagnostica;

4) archivi delle protesi di interesse oncologico;

5) lettere di dimissioni ospedaliere e relazioni cliniche.

4. Per i dati relativi ai tumori infantili, il DEP Lazio, oltre alle fonti di cui al comma 3, si avvale dell'archivio dati dell'Associazione Italiana Ematologia Oncologia Pediatrica previa stipula di apposita convenzione che definisca le modalità tecniche di trasmissione dei dati medesimi, indicando idonee misure di sicurezza nel rispetto delle disposizioni di cui al titolo V della parte I del d.lgs. 196/2003 e del disciplinare tecnico di cui all'allegato A.

5. L'utilizzo dei dati provenienti dall'archivio di cui al comma 4 è subordinato alla verifica dei presupposti di liceità del loro trattamento, nel rispetto della disciplina sulla protezione dei dati personali di cui al d.lgs. 196/2003 e delle indicazioni dell'Autorità Garante per la protezione dei dati personali.

6. Il processo di estrazione, elaborazione e validazione dei dati sui casi incidenti, ricavati dai flussi informativi di cui al presente articolo, è organizzato secondo le modalità e la tempistica del disciplinare tecnico di cui all'Allegato A.

7. La fonte dei dati anagrafici per i casi identificati dal registro tumori è rappresentata dall'anagrafe degli assistiti della Regione di cui al comma 3, lettera a), numero 7). In relazione alle operazioni di trattamento effettuabili con i dati personali contenuti nell'anagrafe degli assistiti il raffronto dei dati anagrafici dei soggetti iscritti o da iscrivere nel registro tumori con i dati della predetta anagrafe è consentito solo al fine di verificarne l'esattezza e l'aggiornamento ed eliminare eventuali duplicati.

8. Ai sensi dell'articolo 4 della legge, i Comuni partecipano, previa eventuale richiesta da parte del titolare o dei responsabili del trattamento dei dati e attraverso i rispettivi servizi anagrafici, alla verifica e all'aggiornamento dei dati anagrafici contenuti nel registro tumori, nel rispetto delle disposizioni di cui agli articoli 33, 34 e 35 del decreto del Presidente della Repubblica 30 maggio 1989 n. 223 (Approvazione del nuovo regolamento anagrafico della popolazione residente) ed in conformità al provvedimento del Garante del 2 luglio 2015 sulle misure di sicurezza e le modalità di scambio dei dati personali tra amministrazioni pubbliche.

9. Ai sensi dell'articolo 8, comma 1, della legge, i medici di medicina generale e i pediatri di libera scelta convenzionati con il servizio sanitario regionale, previa documentata richiesta da parte del titolare o del responsabile del trattamento dei dati, forniscono informazioni sulla storia clinica del paziente, ove indispensabile ai fini della definizione dei casi specifici.

Art. 8

(Misure per la tutela della riservatezza degli individui e della sicurezza dei dati)

1. Il titolare del trattamento dei dati, al fine di tutelare l'identità e la riservatezza degli individui i cui dati sensibili sono contenuti nel registro tumori, adotta le modalità tecniche e le misure di sicurezza dei dati e dei sistemi informativi secondo quanto previsto dagli articoli 31 e seguenti del d.lgs. 196/2003 e dal disciplinare tecnico di cui all'allegato A al presente regolamento.

2. La sicurezza dei dati trattati dal registro tumori è garantita in tutte le fasi del trattamento, mediante l'adozione degli opportuni accorgimenti volti a preservare i medesimi dati da rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

3. I dati contenuti nel registro tumori sono trattati esclusivamente da personale incaricato appositamente individuato, in conformità agli articoli 29 e 30 del d.lgs. 196/2003 e previa sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale, stabilite dal titolare al trattamento dei dati.

4. I soggetti di cui al comma 3 accedono ai dati del registro tumori secondo modalità e logiche di elaborazione strettamente pertinenti ai compiti attribuiti a ciascuno di essi.

Art. 9

(Codifica dei dati trattati)

1. I dati sensibili contenuti nel registro tumori, tenuti con l'ausilio di strumenti elettronici, sono trattati mediante l'utilizzo di codici identificativi, nel rispetto di quanto stabilito dal Disciplinare tecnico di cui all'allegato A, in modo tale da tutelare l'identità e la riservatezza degli interessati nel trattamento dei dati, rendendoli temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettendo di identificare gli interessati solo in caso di necessità, così come previsto dall'articolo 22, comma 6, del d.lgs. 196/2003.

2. I dati idonei a rivelare lo stato di salute sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 1 anche quando sono tenuti senza l'ausilio di strumenti elettronici, così come previsto dall'articolo 22, comma 7, del d.lgs. 196/2003.

Art. 10

(Informativa agli interessati)

1. Agli interessati è fornita l'informativa di cui all'articolo 13 del d.lgs. 196/2003 per il tramite delle strutture del Servizio Sanitario Regionale, pubbliche o private accreditate, che erogano le prestazioni sanitarie, anche mediante l'integrazione dei modelli di informativa già in uso presso le stesse strutture. Agli interessati è garantito altresì il pieno e tempestivo esercizio dei diritti previsti dall'articolo 7 del d.lgs. 196/2003.

Art. 11

(Registro dei referti dei servizi di anatomia patologica)

1. Il registro dei referti dei servizi di anatomia patologica (RSAP), istituito ai sensi dell'articolo 9 della legge, è un archivio centralizzato dei referti dei servizi di anatomia patologica della Regione relativi a prelievi e a pezzi operatori di interesse oncologico, e rappresenta per il registro tumori la fonte di dati per l'accertamento diagnostico delle patologie tumorali e per la determinazione della morfologia, della topografia, dello stadio e grado della malattia nonché degli effetti prodotti dalle terapie adottate.

2. Ai fini della tenuta del registro di cui al presente articolo, le operazioni di raccolta dei dati personali e sanitari già esistenti presso i servizi di anatomia patologica sono realizzate con le modalità e nel rispetto delle misure di sicurezza di cui al Titolo V della parte I del d.lgs. 196/2003 nonché di quelle individuate all'allegato B.

3. Il RSAP è allocato presso il DEP Lazio, che è il titolare del trattamento dei dati e che designa il responsabile e gli incaricati del trattamento dei dati del RSAP.

4. Ai fini della realizzazione del RSAP entro un anno dalla data di entrata in vigore del presente regolamento è necessario:

a) definire un tracciato record minimo comune ai fini della costruzione e aggiornamento del RSAP;

Consiglio regionale del Lazio
b) stabilire le modalità di centralizzare la refertazione secondo raccomandazioni specifiche e che rispondano alle esigenze di codifica automatica;

c) mettere a punto una piattaforma informatica per l'archiviazione centralizzata dei referti;

d) sviluppare una procedura comune di diagnostica assistita basata su un sistema di check-list, secondo contenuti e metodi condivisi su tutto il territorio regionale.

e) garantire l'accesso selettivo al RSAP;

f) garantire misure di sicurezza nel trattamento dei dati personali in osservanza delle disposizioni di cui al titolo V della parte I del d.lgs. 196/2003 e di quanto previsto all'allegato A;

g) garantire misure di protezione dei dati sensibili volte ad assicurare la qualità dei dati, l'utilizzo di codici identificativi degli interessati nonché la conservazione dei dati sanitari separatamente dagli altri dati personali trattati per finalità che non richiedono il loro utilizzo, nel rispetto delle disposizioni di cui agli articoli 11 e 22, commi 6 e 7, del d.lgs. 196/2003.

5. Per le finalità di cui al comma 4, è costituito un apposito gruppo di lavoro, coordinato dal DEP Lazio e composto dai responsabili del trattamento dei dati del registro tumori, del RSAP e delle UF e da un dirigente e/o funzionario della struttura della Regione Lazio competente in materia di sistema informativo sanitario regionale.

Art. 12

(Comunicazione e diffusione dei dati)

1. Il titolare del trattamento dei dati contenuti nel registro tumori, per le finalità di cui all'articolo 1, nel rispetto delle regole previste dai codici di deontologia per i trattamenti di dati personali per scopi statistici e scientifici, di cui all'allegato A4 al d.lgs. 196/2003, in raccordo con il Direttore della Direzione regionale competente in materia:

a) diffonde, anche mediante pubblicazione, risultati statistici soltanto in forma aggregata ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti;

b) svolge studi in campo medico, biomedico ed epidemiologico, anche in collaborazione con Università, Enti ed Istituti di ricerca e società scientifiche nonché con ricercatori, singoli o associati, che operano nell'ambito delle predette Università, Enti ed Istituti di ricerca e società scientifiche;

c) può comunicare le informazioni provenienti dal registro tumori ai titolari del trattamento dei dati contenuti in registri tumori di altre regioni, qualora legittimamente istituiti e regolamentati ai sensi degli articoli 20 e 22 del d.lgs. n. 196/2003 e previa stipula di apposita convenzione redatta in conformità dal provvedimento del Garante del 2 luglio 2015 sulle misure di sicurezza e le modalità di scambio dei dati personali tra amministrazioni pubbliche;

d) alimenta, attraverso la trasmissione dei dati in forma anonima e aggregata, la banca dati nazionale di cui all'articolo 2, comma 7, della legge, nel rispetto di quanto previsto dall'articolo 3 del d.lgs. 196/2003.

Art. 13

(Spese)

1. Il direttore della direzione regionale competente in materia di sanità definisce annualmente, su proposta del DEP Lazio, gli oneri per l'avvio e il funzionamento del suddetto registro.
2. Ai sensi dell'articolo 7 della legge le spese, nell'ambito degli oneri di cui al comma 1, ritenute ammissibili per il funzionamento del registro tumori sono inerenti a:
 - a) progettazione e realizzazione del sistema informatico del registro tumori, ivi compresa la strumentazione hardware e software e la relativa manutenzione;
 - b) eventuali spese, per le attività di coordinamento del registro tumori e del Comitato tecnico scientifico di cui rispettivamente agli articoli 5 e 6 della legge;
 - c) pubblicazioni di atti e/o documenti, privilegiando il sistema di pubblicazione elettronica delle ricerche scientifiche.
3. I componenti del Comitato tecnico-scientifico e i partecipanti alle riunioni di coordinamento di cui, rispettivamente, agli articoli 5 e 6 della legge, operano a titolo gratuito.

Art. 14 (Norme finali)

1. Entro sessanta giorni dall'entrata in vigore del presente regolamento, il DEP Lazio provvede a redigere manuali operativi ~~contenenti dettagli tecnici in grado di garantire l'uniformità delle attività relative alla gestione del registro tumori sul territorio regionale.~~
2. Per quanto non previsto dal presente regolamento si rinvia alla legge.

Art. 15 (Entrata in vigore)

1. Il presente regolamento entra in vigore il giorno successivo a quello della sua pubblicazione sul Bollettino Ufficiale della Regione Lazio.

SOMMARIO

Art. 1 (Oggetto)

Art. 2 (Finalità del Registro tumori di popolazione della Regione Lazio)

Art. 3 (Definizioni)

Art. 4 (Titolare del trattamento dei dati)

Art. 5 (Organizzazione del Registro)

Art. 6 (Tipologia di dati sensibili trattati)

Art. 7 (Fonti dei flussi informativi)

Art. 8 (Misure per la tutela della riservatezza degli individui e della sicurezza dei dati)

Art. 9 (Codifica dei dati trattati)

Art. 10 (Informativa agli interessati)

Art. 11 (Registro dei referti dei servizi di anatomia patologica)

Art. 12 (Comunicazione e diffusione dei dati)

Art. 13 (Spese)

Art. 14 (Norme finali)

Art. 15 (Entrata in vigore)

ALLEGATO A (Disciplinare tecnico in materia di misure di sicurezza per il funzionamento del registro tumori)

ALLEGATO B (Disciplinare tecnico in materia di misure di sicurezza per il funzionamento del registro dei referti dei servizi di anatomia patologica – RSAP)

Il testo non ha valore legale; rimane, dunque, inalterata l'efficacia degli atti normativi originari

File allegati:

