Consiglio dell'Unione europea

Bruxelles, 28 gennaio 2016
(OR. en)

5455/16

Fascicolo interistituzionale: 2012/0011 (COD)

DATAPROTECT 3
JAI 44
MI 27
DIGIT 2
DAPIX 13
FREMP 5
COMIX 39
CODEC 55

NOTA PUNTO "I/A"

Origine:	presidenza
Destinatario:	Comitato dei rappresentanti permanenti/Consiglio
n. doc. prec.:	15321/15
Oggetto:	Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)[prima lettura] - Accordo politico

INTRODUZIONE

1. Il 25 gennaio 2012 la Commissione ha proposto un pacchetto completo sulla protezione dei dati comprendente:

   – la succitata proposta di regolamento generale sulla protezione dei dati, intesa a sostituire la direttiva del 1995 sulla protezione dei dati (ex primo pilastro);

   – una proposta di direttiva 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, intesa a sostituire la decisione quadro del 2008 sulla protezione dei dati (ex terzo pilastro).

2. L'obiettivo del regolamento generale sulla protezione dei dati è rafforzare i diritti delle persone fisiche con riguardo alla protezione dei dati e agevolare la libera circolazione dei dati personali nel mercato unico digitale, anche grazie alla riduzione degli oneri amministrativi.

3. Il 12 marzo 2014 il Parlamento europeo ha adottato, in prima lettura, il regolamento generale proposto sulla protezione dei dati (7427/14).

4. Il 15 giugno 2015 il Consiglio ha concordato un orientamento generale (9565/15) sul regolamento generale sulla protezione dei dati, dando così alla presidenza un mandato di negoziato per avviare triloghi con il Parlamento europeo.

5. In seguito ai dieci triloghi svoltisi dal giugno 2015, la presidenza e i rappresentanti del Parlamento europeo, assistiti dalla Commissione, hanno raggiunto un accordo sul testo di compromesso globale.

6. Nella riunione del 16 dicembre il Comitato dei rappresentanti permanenti ha approvato il testo scaturito dal trilogo del 15 dicembre 2015.

7. Il 17 dicembre la commissione LIBE del Parlamento europeo ha votato, in una riunione straordinaria, il testo concordato in sede di trilogo. Lo stesso giorno il presidente del Comitato dei rappresentanti permanenti ha ricevuto dal presidente della commissione LIBE una lettera (15323/15) in cui indica che avrebbe raccomandato alla commissione LIBE e alla plenaria di approvare l'accordo raggiunto in sede di trilogo senza emendamenti, fatta salva la revisione giuridico-linguistica.

8. Nella riunione del 18 dicembre 2015, il Coreper ha confermato il testo in vista di un accordo (15321/15).

9. Si invita il Comitato dei rappresentanti permanenti a raccomandare al Consiglio di adottare un accordo politico sul testo del regolamento generale sulla protezione dei dati, riportato nell'allegato della presente nota.

ALLEGATO

REGOLAMENTO (UE) N. XXX/2016
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (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],

visto il parere del garante europeo della protezione dei dati[3],

deliberando secondo la procedura legislativa ordinaria[4],

---

1 **[XXX]**
2 **[XXX]**
3 **[XXX]**
4 Posizione del Parlamento europeo del 14 marzo 2014 e decisione del Consiglio del **[XXX]**.

considerando quanto segue:

(1) La tutela delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del trattato 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 nazionalità o dalla residenza dell'interessato. Ciò dovrebbe 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.

(3) Obiettivo della direttiva 95/46/CE del Parlamento europeo e del Consiglio è 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.

(3 bis) 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 contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea e sanciti dai trattati, in particolare il diritto al rispetto della vita privata e familiare, del domicilio e delle comunicazioni, il diritto alla 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, così come la diversità culturale, religiosa e linguistica.

(4) L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha portato a un considerevole aumento dei flussi transfrontalieri e quindi anche dei dati 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.

(5) 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 è aumentata in modo vertiginoso; 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 e, sempre più spesso, gli stessi privati rendono pubbliche sulla rete mondiale informazioni personali che li riguardano. Le nuove tecnologie hanno trasformato non solo l'economia ma anche le relazioni sociali e dovrebbero facilitare ancora di più la libera circolazione dei dati 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.

(6) Tale evoluzione richiede un quadro giuridico 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 i privati quanto per gli operatori economici e le autorità pubbliche.

(6 bis) Ove il presente regolamento preveda specifiche o limitazioni delle sue norme da parte 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 regolamento nei rispettivi diritti nazionali.

(7) Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione delle modalità di applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica e la percezione, largamente diffusa nel pubblico, che soprattutto le operazioni on line comportino notevoli rischi per la tutela delle persone fisiche. La compresenza di diversi livelli di tutela dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, riservata 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. Il divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE.

(8) Al fine di garantire un livello coerente ed elevato di tutela delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È pertanto opportuno garantire un'applicazione coerente ed omogenea delle norme a tutela 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 responsabile del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di precisare 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 dati sensibili. In tal senso il presente regolamento non esclude la legislazione degli Stati membri che definisce le condizioni di specifiche situazioni di trattamento, anche quando sono determinate con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

(9) Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la precisazione dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, ma anche poteri equivalenti per controllare e garantire il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per i trasgressori negli Stati membri.

(10) L'articolo 16, paragrafo 2, del trattato conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati.

(11) Per garantire un livello coerente di tutela delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati 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 azionabilità dei diritti, definisca obblighi e responsabilità dei responsabili del trattamento e degli incaricati del trattamento e assicuri un monitoraggio costante 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 tutela 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 serie di deroghe. Inoltre, le istituzioni e gli organi dell'Unione, 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. Il concetto di micro, piccola e media impresa dovrebbe ispirarsi alla raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese.

(12) La tutela prevista dal presente regolamento si applica alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei dati personali. È opportuno che la tutela offerta dal presente regolamento non possa essere invocata per il trattamento dei dati relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e le sue coordinate di contatto.

(13) La tutela delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dipendere dalle tecniche impiegate; in caso contrario, si correrebbero gravi rischi di elusione. La tutela delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati sono contenuti o destinati ad essere contenuti in un archivio. Non dovrebbero rientrare nel campo di applicazione del presente regolamento i fascicoli o le serie di fascicoli, e le rispettive copertine, non strutturati secondo criteri specifici.

(14) Il presente regolamento non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività concernenti la sicurezza nazionale, né 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.

(14 bis) Il regolamento (CE) n. 45/2001 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 strumenti giuridici dell'Unione applicabili a tale trattamento di dati personali dovrebbero essere adeguati ai principi e alle norme del presente regolamento e applicati alla luce dello stesso. Per offrire un quadro di protezione dei dati solido e coerente nell'Unione, si dovrebbe procedere, dopo l'adozione del presente regolamento, ai necessari adeguamenti del regolamento (CE) n. 45/2001, al fine di consentirne l'applicazione contemporaneamente al presente regolamento.

(15) Il presente regolamento non dovrebbe applicarsi 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 corrispondenza e gli indirizzari, o la socializzazione in rete e attività in linea intraprese nell'ambito di tali attività a carattere personale o domestico. Tuttavia, il presente regolamento dovrebbe valere per i responsabili del trattamento o gli incaricati del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

(16) 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, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, e la libera circolazione di tali dati sono oggetto di uno specifico strumento giuridico a livello di Unione. Il presente regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per queste finalità. I dati trattati dalle autorità pubbliche in forza del presente regolamento a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali dovrebbero invece essere disciplinati dal più specifico strumento giuridico a livello di Unione (direttiva XX/YYY). Gli Stati membri possono conferire alle autorità competenti ai sensi della direttiva XX/YYY 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 nel campo di applicazione del presente regolamento. Con riguardo al trattamento dei dati personali da parte di tali autorità competenti per finalità rientranti nel campo di applicazione del regolamento generale sulla protezione dei dati, gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adattare l'applicazione delle disposizioni del regolamento generale sulla protezione dei dati. 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 di denaro o di attività di laboratorio forense.

(16 bis) Sebbene il presente regolamento si applichi 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'esercizio delle loro funzioni giurisdizionali, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento dei suoi compiti giurisdizionali, compreso il relativo processo decisionale. Il controllo su tali trattamenti di dati può essere affidato ad organismi specifici all'interno del sistema giudiziario dello Stato membro, che dovrebbero in particolare controllare la conformità alle norme del presente regolamento, promuovere la sensibilizzazione della magistratura agli obblighi che alla stessa derivano dal presente regolamento ed esaminare i reclami in relazione a tale trattamento.

(17) Il presente regolamento non dovrebbe pregiudicare l'applicazione della direttiva 2000/31/CE del Parlamento europeo e del Consiglio, 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.

(18) (…)

19) Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o incaricato del trattamento nel territorio dell'Unione dovrebbe essere conforme al presente regolamento, che il trattamento avvenga all'interno dell'Unione o al di fuori. 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.

(20) Onde evitare che una persona fisica venga privata della tutela 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 responsabile del trattamento o da un incaricato del trattamento non stabilito nell'Unione, quando le attività di trattamento sono legate all'offerta di beni o servizi a detti interessati indipendentemente dal fatto che vi sia un pagamento correlato. Per determinare se tale responsabile o incaricato del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Se la semplice accessibilità del sito web 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 responsabile 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, e/o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del responsabile del trattamento di offrire beni o servizi a detti interessati nell'Unione.

(21) È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un responsabile del trattamento o di un incaricato del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al controllo del comportamento di detti interessati, quest'ultimo inteso all'interno dell'Unione europea. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le operazioni che questi esegue su Internet sono tracciate, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati volte alla profilazione dell'utente, in particolare per prendere decisioni che lo riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.

(22) Laddove vige la legislazione nazionale 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 responsabile del trattamento non stabilito nell'Unione.

(23) È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati sottoposti a pseudonimizzazione, che potrebbero essere attribuiti ad 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 responsabile del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona 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 dello sviluppo tecnologico. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono ad una persona fisica identificata o identificabile o a dati 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 e di ricerca.

(23 bis bis)Il presente regolamento non dovrebbe applicarsi ai dati delle persone decedute. Gli Stati membri possono prevedere norme concernenti il trattamento dei dati delle persone decedute.

(23 bis) L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i responsabili del trattamento e gli incaricati del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della "pseudonimizzazione" negli articoli del presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati.

(23 ter) (…)

(23 quater) 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 responsabile del trattamento, qualora il responsabile del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il rispettivo trattamento, l'attuazione delle disposizioni del presente regolamento, e garantendo che le informazioni aggiuntive per l'attribuzione dei dati personali ad un interessato specifico siano conservate separatamente. Il responsabile del trattamento che effettua il trattamento dei dati fa altresì riferimento alle persone autorizzate all'interno dello stesso responsabile del trattamento.

(24) Le persone fisiche possono essere associate a identificativi on line 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 e identificare gli utenti.

(24 quater nuovo) Le autorità pubbliche a cui i dati sono comunicati per adempiere un obbligo legale ai fini dell'esercizio della loro missione ufficiale, 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, possono non essere considerate destinatari qualora ricevano dati 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 portare all'interconnessione di archivi. Il trattamento di tali dati da parte delle autorità pubbliche dovrebbe essere conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento.

(25) Il consenso dovrebbe essere espresso mediante un'azione positiva inequivocabile con la quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare che i dati personali che lo riguardano siano oggetto di trattamento, ad esempio mediante dichiarazione scritta, anche elettronica, 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 questo contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il consenso tacito o passivo 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 dato per l'insieme delle finalità del trattamento. Se il consenso dell'interessato è richiesto con modalità elettronica, la richiesta deve essere chiara, concisa e non disturbare inutilmente il servizio per il quale il consenso è espresso.

(25 bis bis) In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto dovrebbe essere consentito agli interessati di dare 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 dare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista.

(25 bis) È opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche di una persona fisica che siano ereditarie o acquisite, ottenuti dall'analisi di un campione biologico della persona in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) e dell'acido ribonucleico (RNA) ovvero dall'analisi di qualsiasi altro elemento che consenta di ottenere informazioni equivalenti.

(26) 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, fra cui: le informazioni raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria e della relativa prestazione di cui alla direttiva 2011/24/UE; 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; qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o l'effettivo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, ad esempio un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

(27) Lo stabilimento principale di un responsabile 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 prese in un altro stabilimento del responsabile del trattamento nell'Unione, nel qual caso quest'ultimo dovrebbe essere considerato lo stabilimento principale. Lo stabilimento principale di un responsabile del 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 effettivamente 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 l'incaricato del trattamento, per "stabilimento principale" dovrebbe intendersi il luogo in cui ha sede la sua amministrazione centrale nell'Unione e, 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 responsabile del trattamento sia dell'incaricato del trattamento, l'autorità di controllo competente capofila dovrebbe continuare ad essere l'autorità di controllo dello Stato membro in cui il responsabile del trattamento ha lo stabilimento principale, ma l'autorità di controllo dell'incaricato del trattamento dovrebbe essere considerata autorità di controllo interessata e partecipare alla procedura di cooperazione prevista dal presente regolamento. In ogni caso, le autorità di controllo dello o degli Stati membri in cui l'incaricato del trattamento ha uno o più stabilimenti non dovrebbero essere considerate autorità di controllo interessate quando il progetto di decisione riguarda soltanto il responsabile del trattamento. Se il trattamento è effettuato da un gruppo di imprese, 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.

(28) Un gruppo di imprese 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 centrale che controlla il trattamento dei dati personali in imprese a essa collegate forma con tali imprese un'entità che può essere considerata un "gruppo di imprese".

(29) I minori necessitano di una specifica protezione dei loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze, delle misure di salvaguardia e dei loro diritti in relazione al trattamento dei dati personali. Ciò riguarda in particolare 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 relativi al minore 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.

(30) Qualsiasi trattamento di dati personali dovrebbe essere lecito ed equo. Le persone fisiche dovrebbero essere a conoscenza del fatto che sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano e della misura in cui i dati sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Ciò riguarda in particolare l'informazione degli interessati sull'identità del responsabile del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento equo e trasparente con riguardo agli interessati 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 al trattamento. In particolare, le finalità specifiche del trattamento dei dati dovrebbero essere esplicite e legittime e precisate al momento della raccolta. I dati dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del trattamento; da qui l'obbligo, in particolare, di garantire che il periodo di conservazione dei dati 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 garantire che i dati non siano conservati più a lungo del necessario, il responsabile del trattamento dovrebbe fissare un termine per la cancellazione o per la verifica periodica. È opportuno prendere 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.

(31) 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 in altro atto legislativo dell'Unione o degli Stati membri, come indicato nel presente regolamento, tenuto conto della necessità di soddisfare l'obbligo legale al quale il responsabile del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali prese su richiesta dello stesso.

(31 bis) 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, e tuttavia tale base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per coloro che vi sono sottoposti, come richiesto dalla giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo.

(32) Per i trattamenti basati sul consenso dell'interessato, il responsabile 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 materia, dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole di esprimere un consenso e in quale misura. In linea con la direttiva 93/13/CEE del Consiglio[1] è opportuno prevedere una dichiarazione di consenso predisposta dal responsabile 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 messo a conoscenza almeno dell'identità del responsabile 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 ed è nell'impossibilità di rifiutare o ritirare il consenso senza subire pregiudizio.

(33) (…)

(34) Per preservare la libertà di espressione del consenso, è opportuno che il consenso non costituisca una valida base giuridica per il trattamento dei dati personali nel caso specifico in cui esista un evidente squilibrio tra l'interessato e il responsabile del trattamento, specie quando il responsabile del trattamento è un'autorità pubblica e ciò rende 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 consente di esprimere un consenso separato a trattamenti di dati differenti, 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.

(35) Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.

(35 bis) (…)

(36) È opportuno che il trattamento effettuato per adempiere un obbligo legale al quale il responsabile del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri abbia una base tratta dal diritto dell'Unione o dalla legislazione nazionale di uno Stato membro. Il presente regolamento non impone la necessità di una legislazione specifica per ogni singolo trattamento. Un atto legislativo può bastare come base per più trattamenti effettuati conformemente a un obbligo legale cui è soggetto il responsabile 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 base potrebbe precisare le condizioni generali del regolamento relative alla liceità del trattamento dei dati, definire le specifiche per stabilire il responsabile del trattamento, il tipo di dati oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito ed equo. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il responsabile 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 privato, quale un'associazione professionale, quando un interesse pubblico lo giustifichi, in particolare per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria.

(37) Il trattamento di dati personali dovrebbe essere parimenti considerato lecito quando è necessario per tutelare un interesse essenziale per la vita dell'interessato o di un'altra persona. I dati personali dovrebbero essere trattati unicamente per tutelare l'interesse vitale di un'altra persona fisica, in linea di massima, quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati 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 un'epidemia e la sua diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

(38) I legittimi interessi di un responsabile del trattamento, compreso un responsabile del trattamento a cui i dati 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 relazione con il responsabile del trattamento. Ad esempio, potrebbero sussistere legittimi interessi quando esista una relazione pertinente ed appropriata tra l'interessato e il responsabile del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del responsabile 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, 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 responsabile del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati, tale base giuridica non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'adempimento dei loro compiti. Costituisce parimenti legittimo interesse del responsabile 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.

(38 bis) I responsabili del trattamento facenti parte di un gruppo di imprese o di un istituto collegato ad un organismo centrale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo di imprese 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 di imprese, verso un'impresa situata in un paese terzo.

(39) Costituisce legittimo interesse del responsabile del trattamento interessato trattare dati 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, ad eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati 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.

(40) Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati. 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 responsabile 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 per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche 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 sono stati inizialmente raccolti, il responsabile 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 sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il responsabile 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 dato il suo consenso o il trattamento si basi su un atto legislativo 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 responsabile del trattamento dovrebbe poter sottoporre i dati 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 responsabile del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati 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 responsabile del trattamento. Tuttavia, tale trasmissione nell'interesse legittimo del responsabile del trattamento o l'ulteriore trattamento dei dati personali dovrebbero essere vietati se il trattamento non è compatibile con l'obbligo giuridico, professionale o vincolante di segretezza.

(41) 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 notevoli per i diritti e le libertà fondamentali. Tra questi dati dovrebbero essere ricompresi 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 costituirà sistematicamente un trattamento sensibile, poiché esse rientreranno 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 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 ad un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il responsabile del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto concerne 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 viene eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.

(42) La deroga al divieto di trattare categorie di dati sensibili 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 motivi di interesse pubblico lo giustifichino, in particolare il trattamento dei dati nel campo 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. Ciò può avvenire 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 per finalità di archiviazione nel pubblico interesse o finalità di ricerca scientifica e storica o finalità statistiche. La deroga dovrebbe anche consentire di trattare tali dati se necessario per accertare, esercitare o difendere un diritto, che sia in sede giudiziale, amministrativa o stragiudiziale.

(42 bis) Le categorie particolari di dati personali che necessitano di una maggiore protezione possono 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 per finalità di archiviazione nel pubblico interesse o finalità di ricerca scientifica e storica o finalità statistiche in base al diritto dell'Unione o degli Stati membri 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 ad 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 all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi.

(42 ter) 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 è soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche. In questo contesto, il concetto di "sanità pubblica" andrebbe interpretato secondo la definizione del 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: 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 ad essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati personali 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.

(43) Inoltre, è effettuato per motivi di interesse pubblico il trattamento di dati personali a cura di autorità pubbliche diretto a realizzare scopi, previsti dal diritto costituzionale o dal diritto internazionale pubblico, di associazioni religiose ufficialmente riconosciute.

(44) Se, nel corso di attività elettorali, il funzionamento del sistema democratico presuppone, in alcuni Stati membri, che i partiti politici raccolgano dati sulle opinioni politiche delle persone, può esserne consentito il trattamento di tali dati per motivi di interesse pubblico, purché siano predisposte garanzie adeguate.

(45) Se i dati che tratta non gli consentono di identificare una persona fisica, il responsabile 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 responsabile 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 in linea offerto dal responsabile del trattamento.

(46) 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 quali la pubblicità on line, in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se vengono raccolti dati personali che lo riguardano, da chi e per quale finalità. Dato che i minori necessitano di 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.

(47) 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. Pertanto il responsabile 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 responsabile 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 la richiesta dell'interessato.

(48) I principi di trattamento equo e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Il responsabile del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie a garantire un trattamento equo e trasparente, in considerazione delle 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 raccolti direttamente presso l'interessato, questi dovrebbe inoltre essere informato dell'eventuale obbligo di fornire i dati e delle conseguenze a cui va incontro 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 a macchina.

(49) L'interessato dovrebbe ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta o, se i dati non sono ottenuti presso l'interessato ma da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso. Se i dati 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. Il responsabile del trattamento, qualora intenda trattare i dati 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 stato possibile comunicare all'interessato l'origine dei dati, perché sono state utilizzate varie fonti, l'informazione dovrebbe essere fornita in via generale.

(50) Per contro, non è necessario imporre tale obbligo se l'interessato dispone già dell'informazione, se la registrazione o la comunicazione sono previste per legge o se informare l'interessato si rivela impossibile o richiederebbe risorse sproporzionate. Ciò potrebbe verificarsi in particolare con i trattamenti per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica e storica o finalità statistiche, nel qual caso si può tener conto del numero di interessati, dell'antichità dei dati e di eventuali garanzie adeguate.

(51) Una persona fisica dovrebbe avere il diritto di accedere ai dati 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 propri dati personali 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 del trattamento, ove possibile al periodo di conservazione, ai destinatari, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e alle possibili conseguenze di tale trattamento, almeno quando è basato sulla profilazione. Ove possibile, il responsabile del trattamento può 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, queste considerazioni non dovrebbero portare a negare all'interessato l'accesso a tutte le informazioni. Se il responsabile del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il responsabile in questione può chiedere all'interessato, prima che siano fornite le informazioni, di precisare le informazioni o le attività di trattamento cui la richiesta si riferisce.

(52) Il responsabile del trattamento dovrebbe prendere tutte le misure ragionevoli per verificare l’identità di un interessato che chieda l'accesso, in particolare nel contesto di servizi on line e di identificativi on line. Il responsabile del trattamento non dovrebbe conservare dati personali al solo scopo di poter rispondere a potenziali richieste.

(53) Una persona fisica dovrebbe avere il diritto di rettificare i dati personali che la riguardano e il "diritto all'oblio", se la conservazione di tali dati non è conforme al presente regolamento o al diritto dell'Unione o degli Stati membri cui è soggetto il responsabile 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 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 dato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare questo tipo di dati personali, in particolare da Internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non è più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati 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 responsabile del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica e storica o finalità statistiche o per accertare, esercitare o difendere un diritto in sede giudiziaria.

(54) Per rafforzare il "diritto all'oblio" nell'ambiente on line, è opportuno che il diritto di cancellazione sia esteso in modo da obbligare il responsabile del trattamento che ha pubblicato dati personali a informare i responsabili del trattamento che stanno trattando tali dati affinché cancellino qualsiasi link verso tali dati personali o copia o riproduzione di detti dati. Per garantire l'informazione sopramenzionata, è opportuno che il responsabile del trattamento prenda misure ragionevoli, tenuto conto della tecnologia disponibile e dei mezzi a sua disposizione, anche di natura tecnica, per informare i responsabili del trattamento che stanno trattando i dati della richiesta dell'interessato.

(54 bis) 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 o nel rendere i dati 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 non siano sottoposti a ulteriori trattamenti e non possano più essere modificati; il sistema dovrebbe indicare che il trattamento dei dati personali è stato limitato in modo da renderne evidente la limitazione.

(55) 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 a macchina e interoperabile i dati personali che lo riguardano che abbia fornito a un responsabile del trattamento e di trasmetterli a un altro responsabile del trattamento. È opportuno incoraggiare i responsabili del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati. Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali acconsentendo al trattamento o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un altro motivo legittimo diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei responsabili del trattamento che trattano dati nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi in particolare quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il responsabile del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento. Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non comporta l'obbligo per i responsabili del trattamento di adottare o mantenere sistemi di trattamento dei dati tecnicamente compatibili. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati non dovrebbe pregiudicare i diritti degli altri interessati in ottemperanza del presente regolamento. Tale diritto non dovrebbe altresì 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 concernenti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e finché i dati siano necessari all'esecuzione di tale contratto. Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati siano trasmessi direttamente da un responsabile del trattamento a un altro.

(56) Nei casi in cui 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 responsabile del trattamento, ovvero per i legittimi interessi di un responsabile del trattamento o di terzi, l'interessato dovrebbe comunque avere il diritto di opporsi al trattamento dei dati che riguardano la sua situazione particolare. È opportuno che incomba al responsabile del trattamento dimostrare che i suoi interessi legittimi preminenti possono prevalere sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato.

(57) 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 esso quello iniziale o ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione.

(58) 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 basata unicamente su un trattamento automatizzato 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 on line o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende anche 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 nella misura in cui ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito prendere 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 responsabile 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'UE o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal responsabile del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un responsabile del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, fra cui la specifica informazione dell'interessato e il diritto di ottenere l'intervento umano e che la misura non riguardi un minore, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Al fine di garantire un trattamento equo e trasparente nel rispetto dell'interessato, in considerazione delle circostanze e del contesto specifici in cui i dati personali sono trattati, è opportuno che il responsabile del trattamento utilizzi procedure matematiche o statistiche adeguate per la profilazione, metta in atto misure tecniche ed 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 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.

(58 bis) La profilazione in quanto tale 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 dovrebbe avere la possibilità di emanare orientamenti in tale contesto.

(59) 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 o 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 responsabili 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, indagine 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 interessi pubblici 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 dei diritti fondamentali dell'Unione europea e alla convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

(60) È opportuno stabilire la responsabilità generale del responsabile 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 responsabile 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, del campo di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

(60 bis) Tali rischi, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati suscettibili di cagionare un danno fisico, materiale o morale, in particolare se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati 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 dell'esercizio del controllo dei 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 o dati relativi alla salute o 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 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, per creare o utilizzare profili personali; se sono trattati dati personali di persone vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

(60 ter) La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate in funzione della natura, del campo di applicazione, del contesto e delle finalità del trattamento dei dati. Il rischio dovrebbe essere considerato in base ad una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

(60 quater) Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del responsabile del trattamento o dall'incaricato del trattamento in particolare per quanto concerne 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 segnatamente da codici di condotta approvati, certificazioni approvate, linee direttrici del comitato europeo per la protezione dei dati o attraverso le indicazioni fornite da un responsabile della protezione dei dati. Il comitato europeo per la protezione dei dati può inoltre pubblicare linee direttrici 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 questi casi per far fronte a tale rischio.

(61) La tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali richiede l'adozione di misure tecniche ed organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il responsabile 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 responsabile 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 responsabili del trattamento e gli incaricati 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.

(62) La tutela dei diritti e delle libertà degli interessati così come la responsabilità generale dei responsabili del trattamento e degli incaricati del trattamento, anche in relazione al monitoraggio e alle misure delle autorità di controllo, esigono una chiara attribuzione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un responsabile del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri responsabili del trattamento o quando l'operazione viene eseguita per conto del responsabile del trattamento.

(63) Quando un responsabile del trattamento o un incaricato del trattamento non stabilito nell'Unione tratta dati personali di interessati che si trovano nell'Unione e le sue attività di trattamento sono finalizzate 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, quest'ultimo inteso all'interno dell'Unione, è opportuno che tale responsabile del trattamento o incaricato del trattamento designi un rappresentante, tranne se il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati ai sensi dell'articolo 9, paragrafo 1, o il trattamento di dati relativi alle condanne penali e ai reati di cui all'articolo 9 bis, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, del campo di applicazione e delle finalità del trattamento, o se il responsabile del trattamento è un'autorità pubblica o un organismo pubblico. Il rappresentante dovrebbe agire per conto del responsabile del trattamento o dell'incaricato del trattamento e può essere interpellato da qualsiasi autorità di controllo. Il rappresentante dovrebbe essere esplicitamente autorizzato mediante mandato scritto del responsabile del trattamento o dell'incaricato 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 responsabile del trattamento o dell'incaricato del trattamento ai sensi del presente regolamento. Tale rappresentante dovrebbe svolgere i suoi compiti nel rispetto del mandato conferitogli dal responsabile del trattamento dei dati, anche per quanto concerne 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 coercitive in caso di inadempienza da parte del responsabile del trattamento.

(63 bis) Per garantire che siano rispettati i requisiti del presente regolamento riguardo al trattamento che l'incaricato del trattamento deve eseguire per conto del responsabile del trattamento, quando affida delle attività di trattamento a un incaricato del trattamento il responsabile del trattamento dovrebbe ricorrere unicamente a incaricati del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche ed organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. L'applicazione da parte dell'incaricato 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 del responsabile del trattamento. L'esecuzione dei trattamenti su commissione dovrebbe essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli l'incaricato del trattamento al responsabile 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 dell'incaricato del trattamento nel contesto del trattamento da eseguire e del rischio per i diritti e le libertà dell'interessato. Il responsabile del trattamento e l'incaricato 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 responsabile del trattamento, l'incaricato del trattamento dovrebbe, a scelta del responsabile del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto l'incaricato del trattamento preveda un requisito di conservazione dei dati.

(64) (…)

(65) Per dimostrare che si conforma al presente regolamento, il responsabile del trattamento o l'incaricato del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Bisognerebbe obbligare tutti i responsabili del trattamento e gli incaricati 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.

(66) Per mantenere la sicurezza e prevenire trattamenti contrari al presente regolamento, il responsabile del trattamento o l'incaricato 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, come la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque trattati, che potrebbero cagionare in particolare un danno fisico, materiale o morale.

(66 bis) Per migliorare il rispetto del presente regolamento nei casi in cui i trattamenti possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile 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 è effettuato nel rispetto del presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indica che i trattamenti presentano un rischio elevato che il responsabile 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.

(67) Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o morali 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, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale o qualsiasi altro danno economico o sociale alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il responsabile 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 responsabile del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilità, 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, la notifica dovrebbe essere corredata di una giustificazione motivata e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

(67 bis nuovo) Le persone fisiche dovrebbero essere informate senza ingiustificato ritardo se la violazione dei dati personali è suscettibile di presentare un rischio elevato per i loro diritti e le loro libertà affinché possano prendere le precauzioni del caso. La notifica dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Le notifiche agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile, in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti (come le autorità incaricate dell'applicazione della legge). Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la notifica agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni ripetute o analoghe potrebbe giustificare tempi più lunghi.

(68) Occorre verificare se sono state messe in atto tutte le misure tecnologiche ed 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 ad un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

(68 bis) (…)

(69) 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 della 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, nei casi in cui una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione.

(70) La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Tale obbligo comporta oneri amministrativi e finanziari senza per questo aver mai veramente 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, campo di applicazione, contesto e finalità. Questi tipi di trattamenti possono essere quelli che, in particolare, comportano l'utilizzo di nuove tecnologie o che sono di nuovo tipo e per i quali il responsabile del trattamento non ha effettuato preventivamente una valutazione d'impatto sulla protezione dei dati, o che si rivelano necessari alla luce del tempo trascorso dal trattamento iniziale.

(70 bis) In tali casi è opportuno che il responsabile del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio elevato, tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio, che verta in particolare anche sulle misure, sulle garanzie e sui meccanismi per attenuare tale rischio nonché per assicurare la protezione dei dati personali e per dimostrare la conformità al presente regolamento.

(71) 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 nei casi in cui tali trattamenti rendono 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 sono trattati per prendere 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 ad una valutazione d'impatto sulla protezione dei dati.

(72) 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 responsabili 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.

(73) In vista dell'adozione della legge nazionale 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.

(74) Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi previsti per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il responsabile 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 di dati 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 a norma dell'articolo 33, in particolare le misure previste per attenuare il rischio per i diritti e le libertà delle persone fisiche.

(74 bis) L'incaricato del trattamento, se necessario e su richiesta, dovrebbe assistere il responsabile 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.

(74 ter) 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 attenui il rischio per l'interessato.

(75) 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 responsabile del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati, il responsabile del trattamento o l'incaricato 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 responsabile 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 responsabile del trattamento o dall'incaricato del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del responsabile del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente.

(76) Le associazioni o altre organizzazioni rappresentanti le categorie di responsabili del trattamento o di incaricati del trattamento dovrebbero essere incoraggiate ad 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 responsabili del trattamento e degli incaricati del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche.

(76 bis) Nell'elaborare un codice di condotta, o nel modificare o prorogare tale codice, le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o di incaricati del trattamento dovrebbero consultare le parti interessate pertinenti, compresi, quando possibile, gli interessati, e tener conto delle osservazioni ricevute e delle opinioni espresse in risposta a tali consultazioni.

(77) Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione, sigilli e marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi.

(78) I flussi transfrontalieri 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 responsabili del trattamento e incaricati del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali il livello di tutela delle persone fisiche garantito 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 responsabili del trattamento e incaricati 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 possono soltanto essere effettuati nel pieno rispetto del presente regolamento. Il trasferimento è ammesso soltanto se, fatte salve le altre disposizioni del presente regolamento, il responsabile del trattamento o l'incaricato del trattamento rispetta le condizioni di cui al capo V.

(79) 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'UE e includano un adeguato livello di protezione per i diritti fondamentali degli interessati.

(80) La Commissione può decidere, con effetto nell'intera Unione, che taluni paesi terzi, o 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 dei paesi terzi o delle organizzazioni internazionali che si ritiene offrano tale livello di protezione. In questi casi, i trasferimenti di dati personali verso tali paesi possono avere luogo senza ulteriori autorizzazioni. La Commissione può inoltre decidere, dopo aver fornito una comunicazione e una motivazione completa al paese terzo, di revocare una tale decisione.

(81) 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 ed obiettivi come specifiche attività di trattamento e il campo di applicazione delle norme giuridiche e degli atti legislativi applicabili in vigore nel paese terzo. Il paese terzo dovrebbe offrire garanzie atte ad assicurare un adeguato livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione, segnatamente quando i dati 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 europee e agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e di ricorso effettivo in sede amministrativa e giudiziale.

(81 bis) Al di là degli impegni internazionali che il paese terzo o l'organizzazione internazionale hanno assunto, la Commissione dovrebbe tenere altresì 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 europeo per la protezione dei dati.

(81 ter) È opportuno che la Commissione controlli il funzionamento delle decisioni sul livello di protezione in un paese terzo, o in un territorio o settore specifico all'interno di un paese terzo, o un'organizzazione internazionale, comprese le 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 queste ultime decisioni e riferire eventuali riscontri pertinenti al comitato ai sensi del regolamento (UE) n. 182/2011, come stabilito a norma del presente regolamento, al Parlamento europeo e al Consiglio.

(82) La Commissione può riconoscere che un paese terzo, o 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 o organizzazione internazionale dovrebbe essere vietato, a meno che non siano soddisfatti i requisiti di cui agli articoli da 42 a 44. 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.

(83) In mancanza di una decisione di adeguatezza, il responsabile del trattamento o l'incaricato 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'UE, 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.

(84) La possibilità che il responsabile del trattamento o l'incaricato del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione o da un'autorità di controllo non dovrebbe precludere ai responsabili del trattamento o agli incaricati del trattamento la possibilità di includere tali clausole tipo in un contratto più ampio, anche in un contratto tra l'incaricato del trattamento e un altro incaricato 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 responsabili del trattamento e gli incaricati del trattamento dovrebbero essere incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le clausole tipo di protezione.

(85) Un gruppo societario 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 societario o gruppo d'imprese, 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.

(86) 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 ad 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 ad essere consultato dal pubblico o dalle persone aventi un legittimo interesse. In quest'ultimo caso, il trasferimento non dovrebbe riguardare la totalità dei dati o delle categorie di dati contenuti nel registro; inoltre, quando il registro è destinato ad 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.

(87) 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 parimenti 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 dare 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 esprimere il proprio consenso ai fini dell'esecuzione di un compito derivante dalle convenzioni di Ginevra e/o al fine di operare per la fedele applicazione del diritto internazionale umanitario applicabile nei conflitti armati potrebbe essere considerato necessario per importanti motivi di interesse pubblico o nell'interesse vitale dell'interessato.

(88) 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 preminenti del responsabile del trattamento, a meno che non prevalgano gli interessi o i diritti e le libertà dell'interessato e qualora il responsabile del trattamento abbia valutato tutte le circostanze relative al trasferimento. Il responsabile del trattamento dovrebbe considerare con particolare attenzione la natura dei dati, 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 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 motivi di trasferimento è applicabile. Per finalità di ricerca scientifica e storica o per finalità statistiche, è opportuno tener conto delle legittime aspettative della società nei confronti di un miglioramento delle conoscenze. Il responsabile del trattamento informa l'autorità di controllo e l'interessato in merito al trasferimento.

(89) In ogni caso, se la Commissione non ha preso alcuna decisione circa il livello adeguato di protezione dei dati di un paese terzo, il responsabile del trattamento o l'incaricato del trattamento dovrebbe ricorrere a soluzioni che diano all'interessato diritti effettivi e azionabili in relazione al trattamento dei loro dati personali nell'Unione, dopo il trasferimento, così da continuare a beneficiare dei diritti fondamentali e delle garanzie.

(90) Alcuni paesi terzi adottano leggi, regolamenti e altri strumenti legislativi finalizzati a disciplinare direttamente le attività di trattamento dati 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 divulgazione di dati personali da parte di un responsabile del trattamento o di un incaricato 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 strumenti legislativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della tutela delle persone fisiche garantita 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 divulgazione è necessaria per un rilevante motivo di interesse pubblico riconosciuto dal diritto dell'Unione o di uno Stato membro cui è soggetto il responsabile del trattamento.

(91) 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 divulgazioni 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 scontrarsi con poteri insufficienti per prevenire e correggere, regimi giuridici incoerenti e 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 nel rispetto delle disposizioni del presente regolamento, comprese quelle contemplate dal capo V.

(92) La designazione 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 tutela delle persone fisiche con riguardo al trattamento dei loro dati personali. Gli Stati membri possono istituire più di una autorità di controllo, al fine di rispecchiare la loro struttura costituzionale, organizzativa e amministrativa.

(92 bis) L'indipendenza delle autorità di controllo non dovrebbe significare che tali autorità non possano essere assoggettate ad un meccanismo di controllo o monitoraggio con riguardo alle loro spese finanziarie. Né implica che le autorità di controllo non possano essere assoggettate a controllo giurisdizionale.

(93) 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 europeo per la protezione dei dati e la Commissione.

(94) 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 i compiti 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.

(95) 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 i membri siano nominati dal parlamento e/o dal governo o dal capo di Stato dello Stato membro, sulla base di una proposta del governo o di un membro del governo, o del parlamento o di una sua camera, o da un organismo indipendente incaricato ai sensi del diritto dello Stato membro della nomina attraverso una procedura trasparente. 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 professionale 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 dello Stato membro, che sia soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo.

(95 bis) Ogni autorità di controllo dovrebbe avere la competenza, nel territorio del proprio Stato membro, ad esercitare i poteri e ad assolvere i compiti ad essa attribuiti a norma del presente regolamento. Ciò dovrebbe comprendere in particolare il trattamento nell'ambito delle attività di uno stabilimento del responsabile del trattamento o dell'incaricato 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 responsabile del trattamento o da un incaricato del trattamento non stabilito nell'Unione europea riguardante interessati non residenti nel suo territorio. Questo dovrebbe includere il trattamento dei reclami proposti dall'interessato, lo svolgimento di indagini sull'applicazione del regolamento, la promozione della sensibilizzazione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali.

(96) Spetterebbe alle autorità di controllo 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.

(97) Qualora il trattamento dei dati personali abbia luogo nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione e il responsabile del trattamento o l'incaricato del trattamento sia stabilito in più di uno Stato membro o qualora il trattamento effettuato nell'ambito delle attività dello stabilimento unico di un responsabile del trattamento o incaricato 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 responsabile del trattamento o dell'incaricato del trattamento o dello stabilimento unico del responsabile del trattamento o dell'incaricato del trattamento dovrebbe fungere da autorità capofila. Essa dovrebbe cooperare con le altre autorità interessate perché il responsabile del trattamento o l'incaricato 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 pubblicazione di linee direttrici su qualsiasi questione relativa all'applicazione del presente regolamento, il comitato europeo per la protezione dei dati può pubblicare linee direttrici 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.

(97 bis) L'autorità capofila dovrebbe essere competente per l'adozione di decisioni vincolanti riguardanti misure di applicazione dei poteri di cui gode a norma delle disposizioni 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.

(97 ter) 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 responsabile del trattamento o dell'incaricato del trattamento ed essere vincolante per il responsabile del trattamento e l'incaricato del trattamento. Il responsabile del trattamento o l'incaricato 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 responsabile del trattamento o dell'incaricato del trattamento per quanto riguarda le attività di trattamento nell'Unione.

(97 quater) Ogni autorità di controllo che non agisce in qualità di autorità di controllo capofila dovrebbe essere competente a trattare casi locali in cui il responsabile del trattamento o l'incaricato 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 che coinvolge soltanto interessati in tale singolo Stato membro, ad esempio quando l'oggetto riguardi il trattamento di dati 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 nell'ambito del meccanismo di sportello unico a norma dell'articolo 54 bis 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 responsabile del trattamento o dell'incaricato del trattamento, al fine di garantire l'effettiva applicazione di una decisione nei confronti del responsabile del trattamento o dell'incaricato 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 del meccanismo di sportello unico a norma dell'articolo 54 bis.

(98) Le norme sull'autorità di controllo capofila e sul meccanismo di sportello unico a norma dell'articolo 54 bis 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 ad esercitare i poteri ad 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.

(99) (…)

(100) 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 interno, il potere di intentare un'azione e/o 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 legati 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 dal diritto nazionale, 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 nazionale, quale l'obbligo di ottenere un'autorizzazione giudiziaria preliminare. Ogni misura giuridicamente vincolante dell'autorità di controllo dovrebbe avere forma scritta, essere chiara ed 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 ad un ricorso effettivo. Ciò non dovrebbe precludere requisiti supplementari ai sensi del diritto processuale nazionale. L'adozione di tale decisione giuridicamente vincolante implica che essa può essere soggetta a controllo giurisdizionale nello Stato membro dell'autorità di controllo che ha adottato la decisione.

(101) (…)

(101 bis) 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.

(101 ter) Nei casi in cui un'altra autorità di controllo agisca in qualità di autorità di controllo capofila per le attività di trattamento del responsabile del trattamento o dell'incaricato del trattamento, ma il concreto oggetto di un reclamo o la possibile violazione riguardi solo attività di trattamento del responsabile del trattamento o dell'incaricato 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 responsabile 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; o 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 che deve essere oggetto di valutazione tenuto conto dei pertinenti obblighi giuridici ai sensi della legislazione nazionale.

(102) Le attività di sensibilizzazione delle autorità di controllo nei confronti del pubblico dovrebbero comprendere misure specifiche per i responsabili del trattamento e gli incaricati del trattamento, comprese le micro, piccole e medie imprese, e le persone fisiche in particolare nel contesto educativo.

(103) 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 mancata risposta da parte dell'autorità di controllo che riceve una richiesta entro un mese dal ricevimento della stessa.

(104) Ciascuna autorità di controllo dovrebbe partecipare, se del caso, alle operazioni congiunte tra autorità di controllo. L'autorità di controllo che riceve una richiesta dovrebbe darvi seguito entro un termine definito.

(105) 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.

(106) In applicazione del meccanismo di coerenza il comitato europeo per la protezione dei dati 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 europeo per la protezione dei dati dovrebbe altresì avere il potere di adottare decisioni giuridicamente vincolanti in caso di 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 definiti 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.

(107) (…)

(108) 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. Pertanto, un'autorità di controllo può adottare misure provvisorie debitamente giustificate nel proprio territorio, con un periodo di validità determinato che non supera i tre mesi.

(109) L'applicazione di tale meccanismo dovrebbe essere un requisito ai fini della 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.

(110) Per promuovere l'applicazione coerente del presente regolamento, il comitato europeo per la protezione dei dati dovrebbe essere istituito come un organismo indipendente dell'Unione. Per conseguire i suoi obiettivi, il comitato europeo per la protezione dei dati dovrebbe essere dotato di personalità giuridica. Il comitato europeo per la protezione dei dati 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 dal responsabile 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 per quanto la riguarda e che il garante europeo della protezione dei dati vi partecipi con diritti di voto specifici. Il comitato europeo per la protezione dei dati dovrebbe contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, anche dando 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 adempiere i suoi compiti in piena indipendenza.

(110 bis) Il comitato europeo per la protezione dei dati 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 europeo per la protezione dei dati dal presente regolamento dovrebbe svolgere i suoi compiti esclusivamente secondo le istruzioni del presidente del comitato europeo per la protezione dei dati e riferire a quest'ultimo.

(111) 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 in conformità dell'articolo 47 della Carta dei diritti fondamentali 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 suoi diritti di interessato. A seguito di reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nella fattispecie. 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.

(112) 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 ad un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei dati personali e siano costituiti secondo il diritto di uno Stato membro, 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 dello Stato membro. Gli Stati membri possono prevedere che tale organismo, organizzazione o associazione debba avere il diritto, indipendentemente dall'eventuale mandato dell'interessato, in tale Stato membro, di proporre reclamo e/o 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 non conforme alle disposizioni del presente regolamento. L'organismo, l'organizzazione o l'associazione possono non essere autorizzati a chiedere il risarcimento del danno per conto di un interessato indipendentemente dal mandato dell'interessato.

(113) Qualsiasi persona fisica o giuridica ha diritto di proporre un ricorso per l'annullamento delle decisioni del comitato europeo per la protezione dei dati dinanzi alla Corte di giustizia dell'Unione europea (la "Corte di giustizia"), alle condizioni previste all'articolo 263 del TFUE. In quanto destinatari di tali decisioni, le autorità di controllo interessate che intendono impugnarle, devono proporre ricorso entro due mesi dalla data in cui esse sono state loro notificate, conformemente all'articolo 263 del TFUE. Ove le decisioni del comitato europeo per la protezione dei dati si riferiscano direttamente e individualmente a un responsabile del trattamento, a un incaricato 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 europeo per la protezione dei dati, conformemente all'articolo 263 del TFUE. Fatto salvo tale diritto ai sensi dell'articolo 263 del 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, questo diritto non comprende altre misure delle 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 ad 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 europeo per la protezione dei dati viene impugnata dinanzi ad un'autorità giurisdizionale nazionale ed è in questione la validità della decisione del comitato europeo per la protezione dei dati, tale autorità giurisdizionale nazionale non ha il potere di invalidare la decisione del comitato europeo per la protezione dei dati, ma deve deferire la questione di validità alla Corte di giustizia ai sensi dell'articolo 267 del TFUE quale interpretato dalla Corte di giustizia, ogni qualvolta ritenga la decisione non valida. Tuttavia, un'autorità giurisdizionale nazionale non può deferire una questione relativa alla validità di una decisione del comitato europeo per la protezione dei dati 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 del TFUE.

(113 bis) 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 delle attività dello stesso responsabile del trattamento o dello stesso incaricato del trattamento o lo stesso titolo siano sottoposte ad un'autorità giurisdizionale competente in un altro Stato membro, questa 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 le azioni 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 consenta 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.

(114) (…)

(115) (…)

(116) Nelle azioni contro un responsabile del trattamento o incaricato del trattamento, il ricorrente dovrebbe poter avviare un’azione legale dinanzi all'autorità giurisdizionale dello Stato membro in cui il responsabile del trattamento o l’incaricato del trattamento ha uno stabilimento o in cui risiede l’interessato, salvo che il responsabile del trattamento sia un'autorità pubblica di uno Stato membro che agisce nell’esercizio dei suoi poteri pubblici.

(117) (…)

(118) Il responsabile del trattamento o l'incaricato del trattamento dovrebbe risarcire i danni cagionati 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 dell'Unione europea 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. Quando si fa riferimento ad un trattamento non conforme al presente regolamento, esso comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni specifiche di diritto nazionale relative al presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i responsabili del trattamento o gli incaricati del trattamento siano coinvolti nello stesso trattamento, ogni responsabile del trattamento o incaricato del trattamento dovrebbe rispondere per l'intero ammontare del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto nazionale, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni responsabile del trattamento o incaricato 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 responsabile del trattamento o l'incaricato del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri responsabili del trattamento o incaricati del trattamento coinvolti nello stesso trattamento.

(118 bis) Qualora il presente regolamento preveda disposizioni specifiche in materia di giurisdizione, in particolare riguardo a procedimenti che prevedono il ricorso giurisdizionale, compreso per risarcimento, contro un responsabile del trattamento o un incaricato del trattamento, disposizioni generali in materia di giurisdizione quali quelle di cui al regolamento (UE) n. 1215/2012 non dovrebbero pregiudicare l'applicazione di dette disposizioni specifiche.

(118 ter) Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni e sanzioni amministrative pecuniarie per violazione del regolamento, oltre 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 costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un monito anziché imposta una sanzione pecuniaria. Si dovrebbe prestare tuttavia dovuta attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure prese 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 responsabile del trattamento o dell'incaricato del trattamento, all'adesione ad un codice di condotta e eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni e di sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali adeguate in conformità dei principi generali del diritto dell'Unione e della Carta dei diritti fondamentali, inclusi l'effettiva tutela giurisdizionale e il giusto processo.

(119) Gli Stati membri possono 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.

(120) 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 dovrebbe specificare detti illeciti e indicare il limite massimo e i criteri per fissare la relativa sanzione amministrativa pecuniaria, che va stabilita dall'autorità di controllo competente in misura proporzionata alla situazione specifica, 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 pecuniarie sono imposte a imprese, per queste finalità le imprese dovrebbero essere intese quali definite agli articoli 101 e 102 del TFUE. Se le sanzioni pecuniarie sono imposte 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.

(120 bis) (nuovo) I sistemi giudiziari di Danimarca ed Estonia non consentono l'imposizione 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 è imposta dalle competenti autorità giurisdizionali nazionali quale sanzione penale e in Estonia la sanzione pecuniaria è imposta dall'autorità di controllo nell'ambito 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 imposte dovrebbero essere effettive, proporzionate e dissuasive.

(120 bis) 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 dalla legislazione nazionale.

(121) La legislazione degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese la libertà di stampa, 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 garantito dall'articolo 11 della Carta dei diritti fondamentali dell'Unione europea. 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 questi diritti fondamentali. Gli Stati membri dovrebbero adottare tali esenzioni e deroghe con riferimento alle disposizioni concernenti i principi generali, i diritti dell'interessato, il responsabile del trattamento e l'incaricato del trattamento, il trasferimento di dati a paesi terzi o a organizzazioni internazionali, le autorità di controllo indipendenti, la cooperazione e la coerenza nonché situazioni di trattamento dei dati specifiche. Nel caso in cui tali esenzioni o deroghe differiscano da uno Stato membro all'altro, dovrebbe applicarsi il diritto nazionale dello Stato membro cui è soggetto il responsabile 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.

(121 bis) 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 comunicati da detta autorità o organismo se la comunicazione 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 questo 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, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico non pregiudica in alcun modo il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali ai sensi delle disposizioni di diritto unionale e nazionale 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 definito per legge incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali.

(122) (…)

(123) (…)

(124) 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.

(125) Il trattamento di dati personali per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche 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 per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche è da effettuarsi quando il responsabile del trattamento ha valutato la fattibilità di conseguire tali finalità trattando dati che non consentono o non consentono più di identificare l'interessato, purché esistano garanzie adeguate (come ad esempio la pseudonimizzazione dei dati). Gli Stati membri dovrebbero prevedere garanzie adeguate per il trattamento di dati personali per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche. Gli Stati membri dovrebbero essere autorizzati a fornire, a specifiche condizioni e in presenza di adeguate garanzie per gli interessati, specifiche e deroghe relative ai requisiti in materia di informazione, alla rettifica, alla cancellazione, al diritto all'oblio, alla limitazione del trattamento e al diritto alla portabilità dei dati, nonché al diritto di opporsi in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e 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.

(125 bis)(…)

(125 bis bis) Combinando informazioni provenienti dai registri, i ricercatori possono ottenere nuove conoscenze di grande utilità nel caso, per esempio, di malattie diffuse come le malattie cardiovascolari, il cancro, la depressione, ecc.. 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 sull'impatto a lungo termine di numerose condizioni sociali, ad esempio la disoccupazione, l'istruzione, permette di combinare tali informazioni con altre condizioni di vita. I risultati delle ricerche ottenuti sulla base dei 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, ecc.. 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 degli Stati membri o dell'Unione.

(125 ter) Qualora i dati personali siano trattati per finalità 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 disporre che i dati personali possano essere ulteriormente trattati 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.

(126) 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, del trattato sul funzionamento dell'Unione europea. 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 divulgazione 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.

(126 bis) Qualora i dati personali siano trattati per finalità 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.

(126 ter) 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.

(126 quater) 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. Questi risultati statistici possono essere ulteriormente usati per finalità diverse, anche per finalità di ricerca scientifica. Per finalità statistiche si intende qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici. 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 non siano utilizzati a sostegno di misure o decisioni riguardanti persone specifiche.

(126 quinquies) 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, del trattato sul funzionamento dell'Unione europea, mentre le statistiche nazionali dovrebbero essere conformi anche al diritto nazionale. Il 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, fornisce ulteriori specificazioni in merito al segreto statistico per quanto concerne le statistiche europee.

(127) Per quanto riguarda il potere delle autorità di controllo di ottenere, dal responsabile del trattamento o dall'incaricato 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.

(128) 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 del trattato sul funzionamento dell'Unione europea.

(129) 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 dati nell'Unione, dovrebbe essere delegato alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea. 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.

(130) 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, 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 Commissione5. A tal fine, la Commissione dovrebbe contemplare misure specifiche per le micro, piccole e medie imprese.

(131) È opportuno applicare la procedura d'esame per l'adozione di atti di esecuzione su: clausole contrattuali tipo tra i responsabili del trattamento e gli incaricati del trattamento e tra incaricati del trattamento, codici di condotta; norme tecniche e meccanismi di certificazione; adeguato livello di protezione offerto da un paese terzo, o da un territorio o settore di trattamento dati all'interno del paese terzo, o da un'organizzazione internazionale; adozione di clausole tipo di protezione dei dati; formati e procedure per lo scambio di informazioni per via elettronica tra i responsabili del trattamento, gli incaricati del trattamento e le autorità di controllo per norme vincolanti d'impresa; assistenza reciproca; modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato europeo per la protezione dei dati in considerazione della portata generale di tali atti.

(132) È opportuno che la Commissione adotti atti di esecuzione immediatamente applicabili quando gli elementi a disposizione indicano che un paese terzo, o un territorio o settore di trattamento dati all'interno del paese terzo, o un'organizzazione internazionale non garantisce un livello di protezione adeguato e ciò è reso necessario da imperativi motivi di urgenza.

---

5 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 (GU L 55 del 28.2.2011, pag. 13).

(133) Poiché gli obiettivi del presente regolamento, segnatamente garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati nell'Unione, non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(134) 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 dia nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il responsabile 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.

(135) 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, compresi gli obblighi del responsabile 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.

(136) (…)

(137) (…)

(138) (…)

(139) (…)

CAPO I
DISPOSIZIONI GENERALI

Articolo 1

Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e norme relative alla libera circolazione di tali dati.

2. Il presente regolamento tutela i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

2 bis. (…)

3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 2

Campo 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) (…)

   c) effettuati dagli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del titolo V, capo 2, del trattato sull'Unione europea;

   d) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico;

e) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati, esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.

2 bis. 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 strumenti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 90 bis.

3. 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

Campo di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato 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 responsabile del trattamento o incaricato 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 controllo del loro comportamento, quest'ultimo inteso all'interno dell'Unione europea.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un responsabile del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto nazionale di uno Stato membro in virtù del diritto internazionale pubblico.

Articolo 4

Definizioni

Ai fini del presente regolamento s'intende per:

1) "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile, l'"interessato"; si considera identificabile la persona 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 on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) (…)

3) "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 memorizzazione, 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 bis) "limitazione di trattamento": contrassegno dei dati personali memorizzati con l'obiettivo di limitarne il trattamento in futuro;

3 bis bis) "profilazione": qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati 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;

3 ter) "pseudonimizzazione": il trattamento dei dati personali in modo tale che i dati non possano più essere attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive, sempre che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire la non attribuzione a una persona identificata o identificabile;

4) "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;

5) "responsabile del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi 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 del trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il responsabile del trattamento o i criteri specifici applicabili alla sua nomina possono essere designati dal diritto dell'Unione o degli Stati membri;

6) "incaricato del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del responsabile del trattamento;

7) "destinatario": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi 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 in materia di protezione dei dati applicabili secondo le finalità del trattamento;

7 bis) "terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che non sia l'interessato, il responsabile del trattamento, l'incaricato del trattamento e le persone autorizzate al trattamento dei dati sotto l'autorità diretta del responsabile o dell'incaricato;

8) "consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile con la quale l'interessato accetta, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

9) "violazione dei dati personali": 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, memorizzati o comunque trattati;

10) "dati genetici": tutti i dati personali riguardanti le caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni uniche sulla fisiologia o sulla salute di detta persona, ottenuti in particolare dall'analisi di un campione biologico della persona in questione;

11) "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;

12) "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;

12 bis) (…)

13) "stabilimento principale":

a) per quanto riguarda un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, a meno che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano prese in un altro stabilimento del responsabile del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni; in questo caso lo stabilimento che ha preso siffatte decisioni è considerato lo stabilimento principale;

b) con riferimento a un incaricato del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione e, se l'incaricato del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento dell'incaricato del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento dell'incaricato del trattamento nella misura in cui l'incaricato del trattamento è soggetto a obblighi specifici ai sensi del presente regolamento;

14) "rappresentante": la persona fisica o giuridica stabilita nell'Unione che, designata dal responsabile del trattamento o dall'incaricato del trattamento per iscritto ai sensi dell'articolo 25, li rappresenta per quanto concerne gli obblighi rispettivi a norma del presente regolamento;

15) "impresa": ogni 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;

16) "gruppo di imprese": un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

17) "norme vincolanti d'impresa": le politiche in materia di protezione dei dati personali applicate da un responsabile del trattamento o incaricato del trattamento stabilito nel territorio di uno Stato membro dell'Unione al trasferimento o al complesso di trasferimenti di dati personali a un responsabile del trattamento o incaricato del trattamento in uno o più paesi terzi, nell'ambito di un gruppo di imprese o di un gruppo di imprese che svolge un'attività economica comune;

18) (…)

19) "autorità di controllo": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 46;

19 bis) "autorità di controllo interessata": un'autorità di controllo interessata dal trattamento in quanto:

a) il responsabile del trattamento o l'incaricato del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono in tale Stato membro sono o sono probabilmente influenzati in modo sostanziale dal trattamento, oppure

c) un reclamo è stato proposto a tale autorità di controllo;

19 ter) "trattamento transfrontaliero di dati personali":

a) trattamento che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un responsabile del trattamento o incaricato del trattamento nell'Unione e in cui il responsabile del trattamento o l'incaricato del trattamento è stabilito in più di uno Stato membro; oppure

b) trattamento che ha luogo nell'ambito delle attività di un unico stabilimento di un responsabile del trattamento o incaricato del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale sugli interessati in più di uno Stato membro;

19 quater) "obiezione pertinente e motivata":

un'obiezione sul fatto che vi sia o meno una violazione del presente regolamento, oppure, ove del caso, che l'azione prevista in relazione al responsabile del trattamento o incaricato del trattamento sia conforme al presente regolamento. L'obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove del caso, alla libera circolazione dei dati personali all'interno dell'Unione;

20) "servizio della società dell'informazione": i servizi di cui all'articolo 1, paragrafo 1, lettera b), della 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 e delle regole relative ai servizi della società dell'informazione;

21) "organizzazione internazionale": un'organizzazione e gli organismi di diritto internazionale pubblico ad 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

1. I dati personali devono essere:

   a) trattati in modo lecito, equo e trasparente nei confronti dell'interessato ("liceità, equità e trasparenza");

   b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità; un ulteriore trattamento dei dati personali per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche non è, conformemente all'articolo 83, paragrafo 1, considerato incompatibile con le finalità iniziali ("limitazione della finalità");

   c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati");

   d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

   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 per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche, conformemente all'articolo 83, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal regolamento a tutela dei diritti e delle libertà dell'interessato ("limitazione della conservazione");

e ter) trattati in modo 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");

e sexies)(…)

f) (…)

2. Il responsabile del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo ("responsabilità").

Articolo 6

Liceità del trattamento

1. Il trattamento dei dati personali 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 prese su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il responsabile 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 responsabile del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del responsabile 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. Ciò non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. (…)

2 bis. (nuovo) Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento dei dati personali, in adempimento all'articolo 6, paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito ed equo 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 degli Stati membri cui è soggetto il responsabile 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 responsabile del trattamento. Tale base potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra l'altro le condizioni generali relative alla liceità del trattamento dei dati da parte del responsabile del trattamento, il tipo di dati oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati 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 ed equo, anche per le altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri deve perseguire un obiettivo di interesse pubblico ed essere proporzionato all'obiettivo legittimo perseguito.

3 bis. Laddove il trattamento per una finalità diversa da quella per la quale i dati 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 21, paragrafo 1, lettere da a bis) a g), al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati sono stati inizialmente raccolti, il responsabile del trattamento, tra le altre cose, tiene conto:

a) di ogni nesso tra le finalità per cui i dati 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 responsabile 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 9 bis;

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.

4. (…)

5. (…)

Articolo 7

Condizioni per il consenso

1. Qualora il trattamento sia basato sul consenso, il responsabile del trattamento deve essere in grado di dimostrare che l'interessato ha espresso il proprio consenso al trattamento dei propri dati personali.

1 bis. (…)

2. Se il consenso dell'interessato è espresso nel contesto di una dichiarazione scritta che riguarda anche altre materie, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte della dichiarazione cui l'interessato abbia dato il consenso e 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 viene informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente espresso, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, dipenda dal consenso al trattamento di dati 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 di minori al di sotto dei 16 anni - o, se previsto dal diritto degli Stati membri, di un'età inferiore ma non al di sotto di 13 anni - è lecito soltanto se e nella misura in cui tale consenso è espresso o autorizzato dal titolare della responsabilità genitoriale sul minore.

1 bis. Il responsabile del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia espresso o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili.

2. 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.

3. (…)

4. (…)

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, l'appartenenza sindacale, come pure trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona o dati relativi alla salute o alla vita sessuale e all'orientamento sessuale.

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

   a) l'interessato ha espresso 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, oppure

   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del responsabile 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 adeguate garanzie per i diritti fondamentali e gli interessi dell'interessato, oppure

   c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona qualora l'interessato si trovi nell'incapacità fisica o giuridica di esprimere il proprio consenso, oppure

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 persegua 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 non siano comunicati a terzi senza il consenso dell'interessato, oppure

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato, oppure

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali, oppure

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, oppure

h) il trattamento è necessario per finalità di prevenzione medica 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 4, oppure

h ter) 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, oppure

i) il trattamento è necessario per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche in conformità dell'articolo 83, paragrafo 1, sulla base del diritto dell'Unione o degli Stati membri, 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.

j) (…)

3. (…)

4. 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.

5. 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 9 bis

Trattamento dei dati 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, può avvenire soltanto sotto il controllo dei pubblici poteri o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda adeguate garanzie per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali può essere tenuto soltanto sotto il controllo dei pubblici poteri.

Articolo 10

Trattamento che non richiede l'identificazione

1. Se le finalità per cui un responsabile del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il responsabile 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, in tali casi, il responsabile 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 18 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 11

Informazioni e comunicazioni trasparenti

1. (…)

2. (…)

Articolo 12

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il responsabile del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 14 e 14 bis e le comunicazioni di cui agli articoli da 15 a 20 e 32 relative al trattamento dei dati personali 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, se del caso in formato elettronico. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

1 bis. Il responsabile del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 20. Nei casi di cui all'articolo 10, paragrafo 2, il responsabile 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 20, salvo che il responsabile del trattamento dimostri che non è in grado di identificare l'interessato.

2. Il responsabile del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo ad una richiesta ai sensi degli articoli da 15 a 20 senza ingiustificato ritardo e al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato per un massimo di altri due mesi, se necessario, tenuto conto della complessità della richiesta e del numero di richieste. Qualora si applichi la proroga, l'interessato è informato dei motivi del ritardo entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta in formato elettronico, le informazioni sono fornite, ove possibile, in formato elettronico, salvo indicazione diversa dell'interessato.

3. Se non ottempera alla richiesta dell'interessato, il responsabile 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.

4. Le informazioni fornite ai sensi degli articoli 14 e 14 bis ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 20 e 32 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il responsabile del trattamento può addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta, oppure può rifiutare di soddisfare la richiesta. In tali casi, incombe al responsabile del trattamento dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

4 bis. Fatto salvo l'articolo 10, qualora il responsabile del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 19, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

4 ter. Le informazioni da fornire agli interessati a norma degli articoli 14 e 14 bis 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 a macchina.

4 quater. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 86 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

5. (…)

6. (…)

Articolo 13

Diritti relativi ai destinatari

(...)

SEZIONE 2

INFORMAZIONE E ACCESSO AI DATI

Articolo 14

Informazioni da fornire qualora i dati siano raccolti presso l'interessato

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il responsabile del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:

   a) l'identità e le coordinate di contatto del responsabile del trattamento e del suo eventuale rappresentante; il responsabile del trattamento include anche le coordinate di contatto dell'eventuale responsabile della protezione dei dati;

   b) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

   c) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal responsabile del trattamento o da terzi;

d) se del caso, i destinatari o le categorie di destinatari dei dati personali;

e) se del caso, l'intenzione del responsabile 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 42 o 43, o all'articolo 44, paragrafo 1, lettera h), 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.

1 bis. Oltre alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il responsabile del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento equo e trasparente:

a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;

b) …

c) …

d) …

e) l'esistenza del diritto dell'interessato di chiedere al responsabile 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 o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

e bis) 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;

f) il diritto di proporre reclamo ad un'autorità di controllo;

g) se la comunicazione di dati personali è un obbligo statutario o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati nonché le possibili conseguenze della mancata comunicazione di tali dati;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 20, paragrafi 1 e 3, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

1 ter. Qualora il responsabile del trattamento intenda trattare ulteriormente i dati 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 finalità diversa e tutte le informazioni pertinenti di cui al paragrafo 1 bis.

2. (…)

3. (…)

4. (…)

5. I paragrafi 1, 1 bis e 1 ter non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

6. (…)

7. (…)

8. (…)

Articolo 14 bis

Informazioni da fornire qualora i dati non siano stati ottenuti presso l'interessato

1. Qualora i dati non siano stati ottenuti presso l'interessato, il responsabile del trattamento fornisce all'interessato le seguenti informazioni:

   a) l'identità e le coordinate di contatto del responsabile del trattamento e del suo eventuale rappresentante; il responsabile del trattamento include anche le coordinate di contatto dell'eventuale responsabile della protezione dei dati;

   b) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

   b bis) le categorie di dati personali in questione;

   c) (…)

   d) se del caso, i destinatari o le categorie di destinatari dei dati personali;

   d bis) se del caso, l'intenzione del responsabile 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 42 o 43, o all'articolo 44, paragrafo 1, lettera h), 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 responsabile del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento equo e trasparente nei confronti dell'interessato:

   b) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare questo periodo;

   b bis) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal responsabile del trattamento o da terzi;

c) (…)

e) l'esistenza del diritto dell'interessato di chiedere al responsabile 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;

e bis) 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;

f) il diritto di proporre reclamo ad un'autorità di controllo;

g) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 20, paragrafi 1 e 3, 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 responsabile del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:

a) entro un termine ragionevole dall'ottenimento dei dati, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati vengono trattati, oppure

b) nel caso in cui i dati siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato, oppure

c) in caso di prevista comunicazione ad un altro destinatario, al più tardi al momento della prima divulgazione dei dati.

3 bis. Qualora il responsabile del trattamento intenda trattare ulteriormente i dati 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 finalità diversa e tutte le informazioni pertinenti di cui al paragrafo 2.

4. I paragrafi da 1 a 3 bis non si applicano se e nella misura in cui:

a) l'interessato dispone già delle informazioni, oppure

b) comunicare tali informazioni risulta impossibile o implicherebbe risorse sproporzionate; in particolare per il trattamento per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche, fatte salve le condizioni e le garanzie di cui all'articolo 83, paragrafo 1, o nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di archiviazione nel pubblico interesse o delle finalità di ricerca scientifica e storica o delle finalità statistiche; in tali casi, il responsabile del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni, oppure

c) l'ottenimento o la divulgazione sono espressamente previsti dal diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato, oppure

d) qualora i dati debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo statutario di segretezza.

Articolo 15

Diritto di accesso dell'interessato

1. L'interessato ha il diritto di ottenere dal responsabile del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, se è in corso tale trattamento, l'accesso ai dati 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 questo periodo;

e) l'esistenza del diritto dell'interessato di chiedere al responsabile 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 ad 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 20, paragrafi 1 e 3, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

1 bis. Qualora i dati personali siano trasferiti ad 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 42 relative al trasferimento.

1 ter. Il responsabile del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il responsabile del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta in formato elettronico, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in formato elettronico, come d'uso comune.

2. (…)

2 bis. Il diritto di ottenere una copia di cui al paragrafo 1 ter non può ledere i diritti e le libertà altrui.

3. (…)

4. (…)

SEZIONE 3

RETTIFICA E CANCELLAZIONE

Articolo 16

Diritto di rettifica

L'interessato ha il diritto di ottenere dal responsabile del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità per le quali i dati sono stati trattati, 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 responsabile del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il responsabile del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

   a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

   b) l'interessato ritira 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 motivo legittimo per trattare i dati;

   c) l'interessato si oppone al trattamento dei dati personali ai sensi dell'articolo 19, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento dei dati personali ai sensi dell'articolo 19, paragrafo 2;

   d) sono stati trattati illecitamente;

   e) i dati devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento;

   f) i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

1 bis. (…)

2. (…)

2 bis. Il responsabile 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 prende le misure ragionevoli, anche tecniche, per informare i responsabili del trattamento che stanno trattando i dati 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 dei dati personali 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 dei dati personali previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e h ter), e dell'articolo 9, paragrafo 4;

d) per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche conformemente all'articolo 83, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di archiviazione nel pubblico interesse o delle finalità di ricerca scientifica e storica o finalità statistiche;

e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

4. (…)
5. (…)
6. (…)
7. (…)
8. (…)
9. (…)

Articolo 17 bis

Diritto di limitazione di trattamento

1. L’interessato ha il diritto di ottenere dal responsabile del trattamento la limitazione del trattamento dei dati personali quando:

   a) l’interessato contesta l’esattezza dei dati, per il periodo necessario al responsabile del trattamento per effettuare le opportune verifiche;

   a ter) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati e chiede invece che ne sia limitato l'utilizzo;

   b) benché il responsabile 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, oppure

   c) l'interessato si è opposto al trattamento ai sensi dell'articolo 19, paragrafo 1, in attesa della verifica se i motivi legittimi del responsabile del trattamento prevalgano su quelli dell'interessato.

2. Se il trattamento dei dati personali è limitato a norma del paragrafo 1, tali dati possono essere 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 responsabile del trattamento prima che detta limitazione sia revocata.

Articolo 17 ter

Obbligo di notifica in caso di rettifica, cancellazione o limitazione dei dati

Il responsabile del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati le eventuali rettifiche, cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 17 bis, salvo che ciò si riveli impossibile o implichi risorse sproporzionate. Il responsabile del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Articolo 18

Diritto alla portabilità dei dati

1. (…)

2. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile a macchina i dati personali che lo riguardano forniti ad un responsabile del trattamento e ha il diritto di trasmettere tali dati a un altro responsabile del trattamento senza impedimenti da parte del responsabile 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 bis. (nuovo) 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 da un responsabile del trattamento all'altro, se tecnicamente fattibile.

2 bis. L'esercizio di tale diritto lascia impregiudicato l'articolo 17. Il diritto di cui al paragrafo 2 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 responsabile del trattamento.

2 bis bis. Il diritto di cui al paragrafo 2 non può ledere i diritti e le libertà altrui.

3. (…)

SEZIONE 4

DIRITTO DI OPPOSIZIONE E PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE

Articolo 19

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 responsabile del trattamento non tratta più i dati personali salvo che egli dimostri l'esistenza di motivi legittimi preminenti 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.

2 bis. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

2 ter. (nuovo) 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.

2 ter. 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.

2 bis bis. Qualora i dati personali siano trattati per finalità di ricerca scientifica e storica o per finalità statistiche a norma dell'articolo 83, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento dei dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

3. (…)

Articolo 20

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 allo stesso modo significativamente sulla sua persona.

1 bis. 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 responsabile del trattamento, oppure

b) sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, oppure

c) si basi sul consenso esplicito dell'interessato.

1 ter. Nei casi di cui al paragrafo 1 bis, lettere a) e c), il responsabile 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 responsabile del trattamento, di esprimere la propria opinione e di contestare la decisione.

2. (…)

3. Le decisioni di cui al paragrafo 1 bis 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.

4. (…)

5. (…)

SEZIONE 5

Limitazioni

Articolo 21

Limitazioni

1. Il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento o l'incaricato del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 20 e 32, 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 20, 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 bis) la sicurezza nazionale;

a ter) la difesa;

a) la sicurezza pubblica;

b) 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;

c) 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;

c bis) la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari;

d) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;

e) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere a bis), a ter), a), b), c) e d);

f) la tutela dell'interessato o dei diritti e delle libertà altrui;

g) l'esecuzione delle azioni civili.

2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, ove appropriato:

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 responsabile del trattamento o delle categorie di responsabili;
f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, del campo 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
RESPONSABILE DEL TRATTAMENTO E INCARICATO DEL TRATTAMENTO

SEZIONE 1
OBBLIGHI GENERALI

Articolo 22

Responsabilità del responsabile del trattamento

1. Tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

2. (…)

2 bis. 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 responsabile del trattamento.

2 ter. L'applicazione dei codici di condotta approvati ai sensi dell'articolo 38 o di un meccanismo di certificazione approvato ai sensi dell'articolo 39 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del responsabile del trattamento.

3. (…)

4. (…)

Articolo 23

Protezione dei dati fin dalla progettazione e protezione di default

1. Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi di varia probabilità e gravità 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 responsabile del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare i principi di protezione dei dati, quali la minimizzazione, in modo efficace 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 responsabile del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, di default, solo i dati personali necessari per ogni specifica finalità del trattamento; ciò vale per la quantità dei dati raccolti, l'estensione del trattamento, il periodo di conservazione e l'accessibilità. In particolare dette misure garantiscono che, di default, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

2 bis. Un meccanismo di certificazione approvato ai sensi dell'articolo 39 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2.

3. (…)

4. (…)

Articolo 24

Corresponsabili del trattamento

1. Allorché due o più responsabili del trattamento determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali, essi sono corresponsabili del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito al rispetto 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 14 e 14 bis, a meno che e nella misura in cui le rispettive responsabilità dei responsabili del trattamento siano determinate dal diritto dell'Unione o degli Stati membri cui essi sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

2. 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 responsabile del trattamento.

3. L'accordo riflette adeguatamente i rispettivi ed effettivi ruoli dei corresponsabili del trattamento e i loro rapporti con gli interessati, e il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Articolo 25

Rappresentanti di responsabili del trattamento non stabiliti nell'Unione

1. Ove si applichi l'articolo 3, paragrafo 2, il responsabile del trattamento o l'incaricato del trattamento designa per iscritto un rappresentante nell'Unione.

2. Quest'obbligo non si applica:

   a) (…);

   b) 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 il trattamento di dati relativi a condanne penali e a reati di cui all'articolo 9 bis, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, del campo di applicazione e delle finalità del trattamento, oppure

c) alle autorità pubbliche o agli organismi pubblici.

d) (…)

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 controllato.

3 bis. Ai fini della conformità con il presente regolamento, il rappresentante è autorizzato dal responsabile del trattamento o dall'incaricato del trattamento ad essere interpellato, in aggiunta o in sostituzione del responsabile del trattamento o dell'incaricato del trattamento, in particolare dalle autorità di controllo e dagli interessati, per tutte le questioni riguardanti il trattamento di dati personali.

4. La designazione di un rappresentante a cura del responsabile del trattamento o dell'incaricato del trattamento fa salve le azioni legali che potrebbero essere promosse contro lo stesso responsabile del trattamento o incaricato del trattamento.

Articolo 26

Incaricato del trattamento

1. Qualora un trattamento debba essere effettuato per conto del responsabile del trattamento, quest'ultimo ricorre unicamente a incaricati del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

1 bis. L'incaricato del trattamento non ricorre ad un altro incaricato senza il previo consenso scritto, specifico o generale, del responsabile del trattamento. In quest'ultimo caso l'incaricato del trattamento dovrebbe sempre informare il responsabile del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri incaricati del trattamento, dando così l'opportunità al responsabile del trattamento di obiettare a tali modifiche.

2. L'esecuzione dei trattamenti su commissione è disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli l'incaricato del trattamento al responsabile del trattamento, in cui siano stipulati 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 responsabile del trattamento, e che preveda in particolare che l'incaricato del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del responsabile 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 degli Stati membri cui è soggetto l'incaricato del trattamento; in tal caso, l'incaricato del trattamento informa il responsabile del trattamento circa tale obbligo giuridico prima del trattamento dei dati, 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 statutario di riservatezza;

c) prenda tutte le misure richieste ai sensi dell'articolo 30;

d) rispetti le condizioni di cui ai paragrafi 1 bis e 2 bis per ricorrere a un altro incaricato del trattamento;

e) tenuto conto della natura del trattamento, assista il responsabile del trattamento con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del responsabile del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il responsabile del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 30 a 34, tenendo conto della natura del trattamento e delle informazioni a disposizione dell'incaricato del trattamento;

g) su scelta del responsabile del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi di trattamento di dati e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la memorizzazione dei dati;

h) metta a disposizione del responsabile del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca agli audit, comprese le ispezioni, realizzati dal responsabile del trattamento o da un altro revisore da questi incaricato. L'incaricato del trattamento informa immediatamente il responsabile del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o le disposizioni dell'Unione o degli Stati membri concernenti la protezione dei dati.

2 bis. Quando un incaricato del trattamento ricorre ad un altro incaricato del trattamento per l'esecuzione di specifiche attività di trattamento per conto del responsabile del trattamento, su tale altro incaricato 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 responsabile del trattamento e l'incaricato del trattamento di cui al paragrafo 2, 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 incaricato del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, l'incaricato iniziale conserva nei confronti del responsabile del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro incaricato.

2 bis bis. L'applicazione da parte dell'incaricato del trattamento di un codice di condotta approvato ai sensi dell'articolo 38 o di un meccanismo di certificazione approvato ai sensi dell'articolo 39 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 2 bis.

2 bis ter. Fatto salvo un contratto individuale tra il responsabile del trattamento e l'incaricato del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 2 e 2 bis può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 2 ter e 2 quater, anche laddove siano parte di una certificazione concessa al responsabile del trattamento o all'incaricato del trattamento ai sensi degli articoli 39 e 39 bis.

2 ter. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 2 e 2 bis e secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.

2 quater. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 2 e 2 bis in conformità del meccanismo di coerenza di cui all'articolo 57.

3. Il contratto o altro atto giuridico di cui ai paragrafi 2 e 2 bis è stipulato in forma scritta, anche in formato elettronico.

4. Fatti salvi gli articoli 77, 79 e 79 ter, se un incaricato del trattamento determina le finalità e i mezzi del trattamento dei dati in violazione del presente regolamento, è considerato un responsabile del trattamento relativamente al trattamento in questione.

5. (…)

Articolo 27

Trattamento sotto l'autorità del responsabile del trattamento e dell'incaricato del trattamento

L'incaricato del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 28

Registri delle attività di trattamento

1. Ogni responsabile del trattamento e il suo eventuale rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Il registro contiene le seguenti informazioni:

   a) il nome e le coordinate di contatto del responsabile del trattamento e di ogni corresponsabile del trattamento, del rappresentante del responsabile del trattamento e dell'eventuale responsabile della protezione dei dati;

   b) (…)

   c) le finalità del trattamento;

d) una descrizione delle categorie di interessati e delle categorie di dati personali;

e) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi;

f) se del caso, i trasferimenti di dati verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'articolo 44, paragrafo 1, lettera h), la documentazione delle garanzie adeguate;

g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

h) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 30, paragrafo 1.

2 bis. Ogni incaricato del trattamento e il suo eventuale rappresentante tengono un registro di tutte le categorie di attività di trattamento dei dati personali svolte per conto di un responsabile del trattamento, contenente:

a) nome e coordinate di contatto dell'incaricato o degli incaricati del trattamento, di ogni responsabile del trattamento per conto del quale agisce l'incaricato del trattamento, del rappresentante del responsabile del trattamento o dell'incaricato del trattamento e dell'eventuale responsabile della protezione dei dati;

b) (…)

c) le categorie dei trattamenti effettuati per conto di ogni responsabile del trattamento;

d) se del caso, i trasferimenti di dati verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'articolo 44, paragrafo 1, lettera h), la documentazione delle garanzie adeguate;

e) ove possibile, una descrizione generale delle misure di sicurezza tecniche ed organizzative di cui all'articolo 30, paragrafo 1.

3 bis. I registri di cui ai paragrafi 1 e 2 bis sono tenuti in forma scritta, anche in formato elettronico.

3. Su richiesta, il responsabile del trattamento, l'incaricato del trattamento e l'eventuale rappresentante del responsabile del trattamento o dell'incaricato del trattamento mettono il registro a disposizione dell'autorità di controllo.

4. Gli obblighi di cui ai paragrafi 1 e 2 bis 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 il trattamento di dati relativi a condanne penali e a reati di cui all'articolo 9 bis.

5. (…)

6. (…)

Articolo 29

Cooperazione con l'autorità di controllo

1. Il responsabile del trattamento, l'incaricato del trattamento e il loro eventuale rappresentante cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

2. (…).

SEZIONE 2
SICUREZZA DEI DATI

Articolo 30

Sicurezza del trattamento

1. Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, 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 responsabile del trattamento e l'incaricato del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono tra l'altro, se del caso:

   a) la pseudonimizzazione e la cifratura dei dati personali;

   b) la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;

   c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;

   d) una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

1 bis. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati da trattamenti di dati derivanti in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, memorizzati o comunque trattati.

2. (…)

2 bis. L'applicazione di un codice di condotta approvato ai sensi dell'articolo 38 o di un meccanismo di certificazione approvato ai sensi dell'articolo 39 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1.

2 ter. Il responsabile del trattamento e l'incaricato del trattamento fanno sì che chiunque agisca sotto l'autorità del responsabile del trattamento o dell'incaricato del trattamento e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

3. (…)

4. (…)

Articolo 31

Notificazione di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il responsabile del trattamento notifica la violazione all'autorità di controllo competente ai sensi dell'articolo 51 senza ingiustificato ritardo, 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 non sia effettuata entro 72 ore, la notifica all'autorità di controllo è corredata di una giustificazione motivata.

1 bis. (…)

2. L'incaricato del trattamento informa il responsabile del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve come minimo:

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 in questione;

b) indicare il nome e le coordinate di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) (…)

d) descrivere le probabili conseguenze della violazione dei dati personali;

e) descrivere le misure adottate o di cui si propone l'adozione da parte del responsabile del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

f) (…)

3 bis. 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.

4. Il responsabile del trattamento documenta qualsiasi violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto del presente articolo.

5. (…)

6. (…)

Articolo 32

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 responsabile del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'articolo 31, paragrafo 3, lettere b), d) ed e).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se:

a) il responsabile del trattamento ha utilizzato le misure tecniche ed organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura, oppure

b) il responsabile 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, oppure

c) detta comunicazione richiederebbe sforzi sproporzionati. In una simile circostanza, 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 responsabile 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 presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

5. (…)

6. (…)

SEZIONE 3
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI E CONSULTAZIONE PREVENTIVA

Articolo 33

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, il campo di applicazione, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile 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.

1 bis. Il responsabile del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, chiede un parere al responsabile della protezione dei dati, qualora ne sia designato uno.

2. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei seguenti casi:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione, e da cui discendono decisioni che hanno effetti giuridici o incidono allo stesso modo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 9 bis;

c) la sorveglianza sistematica di una zona accessibile al pubblico su larga scala.

d) (…)

e) (…)

2 bis. 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 europeo per la protezione dei dati.

2 ter. 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 europeo per la protezione dei dati.

2 quater. Prima di adottare gli elenchi di cui ai paragrafi 2 bis e 2 ter, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 57 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al controllo 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.

3. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, se del caso, l'interesse legittimo perseguito dal responsabile del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;

d) 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.

3 bis. Nel valutare l'impatto del trattamento effettuato dai relativi responsabili o incaricati si tiene debito conto del rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 38, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

4. Se del caso, il responsabile 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.

5. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto degli Stati membri cui il responsabile del trattamento è soggetto una base giuridica attraverso un atto legislativo che disciplina 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 1, 2 e 3 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

6. (…)

7. (…)

8. Se necessario, il responsabile del trattamento procede a un riesame per valutare se il trattamento dei dati personali è effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando vi sia un cambiamento del rischio rappresentato dai trattamenti.

Articolo 34

Consultazione preventiva

1. (…)

2. Il responsabile del trattamento, prima di procedere al trattamento dei dati personali, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati di cui all'articolo 33 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal responsabile del trattamento per attenuare il rischio.

3. Se ritiene che il trattamento previsto di cui al paragrafo 2 non sia conforme al presente regolamento, in particolare qualora il responsabile del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo, entro un periodo massimo di otto settimane dalla richiesta di consultazione, fornisce una consulenza per iscritto al responsabile del trattamento dei dati, e ove applicabile all'incaricato del trattamento, e può avvalersi dei poteri di cui all'articolo 53. Questo periodo può essere prorogato di ulteriori sei settimane, tenendo conto della complessità del trattamento previsto. Qualora si applichi la proroga, il responsabile del trattamento e, ove applicabile, l'incaricato del trattamento ne sono informati, incluso dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Tali periodi possono essere sospesi fino all'ottenimento da parte dell'autorità di controllo delle informazioni eventualmente richieste ai fini della consultazione.

4. (…)

5. (…)

6. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 2, il responsabile del trattamento trasmette all'autorità di controllo:

   a) se del caso, le rispettive responsabilità del responsabile del trattamento, dei corresponsabili e coincaricati del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo di imprese;

   b) le finalità e i mezzi del trattamento previsto;

   c) le misure e le garanzie previste per tutelare i diritti e le libertà degli interessati a norma del presente regolamento;

   d) se del caso, le coordinate di contatto del responsabile della protezione dei dati;

   e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 33;

   f) ogni altra informazione richiesta dall'autorità di controllo.

7. 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 di dati personali.

7 bis. Nonostante il paragrafo 2, il diritto degli Stati membri può richiedere che i responsabili del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento di dati personali da parte di un responsabile del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento dei dati con riguardo alla protezione sociale e alla sanità pubblica.

8. (…)

9. (…)

SEZIONE 4
RESPONSABILE DELLA PROTEZIONE DEI DATI

Articolo 35

Designazione del responsabile della protezione dei dati

1. Il responsabile del trattamento e l'incaricato del trattamento designano sistematicamente un responsabile della protezione dei dati quando:
   a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali, oppure

   b) le attività principali del responsabile del trattamento o dell'incaricato del trattamento consistono in trattamenti che, per loro natura, campo di applicazione e/o finalità, richiedono il controllo regolare e sistematico degli interessati su larga scala, oppure

   c) le attività principali del responsabile del trattamento o dell'incaricato del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 9 bis.

2. Un gruppo di imprese 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 responsabile del trattamento o l'incaricato 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 responsabile del trattamento, l'incaricato del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o di incaricati 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 responsabili del trattamento o gli incaricati 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 pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti di cui all'articolo 37.

6. (…)

7. (…)

8. Il responsabile della protezione dei dati può essere un membro del personale del responsabile del trattamento o dell'incaricato del trattamento oppure adempiere ai suoi compiti in base a un contratto di servizi.

9. Il responsabile del trattamento o l'incaricato del trattamento pubblica le coordinate di contatto del responsabile della protezione dei dati e le comunica all'autorità di controllo.

10. (…)

11. (…)

Articolo 36

Posizione del responsabile della protezione dei dati

1. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati sia prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il responsabile del trattamento o l'incaricato del trattamento sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 37 fornendogli le risorse necessarie per adempiere a tali compiti nonché l'accesso ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

2 bis. (nuovo) 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.

3. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione dei propri compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal responsabile del trattamento o dall'incaricato del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente ai massimi superiori gerarchici del responsabile del trattamento o dell'incaricato del trattamento.

4. 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.

4 bis. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il responsabile del trattamento o l'incaricato del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 37

Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

a) informare e consigliare il responsabile del trattamento o l'incaricato del trattamento nonché i dipendenti che trattano dati personali 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, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del responsabile del trattamento o dell'incaricato 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 gli audit connessi;

c) (…)

d) (…)

e) (…)

f) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 33;

g) cooperare con l'autorità di controllo;

h) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento di dati personali, tra cui la consultazione preventiva di cui all'articolo 34, ed effettuare, se del caso, consultazioni su qualunque altra questione.

2. (…)

2 bis. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del medesimo.

SEZIONE 5
CODICI DI CONDOTTA E CERTIFICAZIONE

Articolo 38

Codici di condotta

1. Gli Stati membri, le autorità di controllo, il comitato europeo per la protezione dei dati e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità settoriali e delle esigenze specifiche delle micro, piccole e medie imprese.

1 bis. Le associazioni e gli altri organismi rappresentanti le categorie di responsabili del trattamento o incaricati del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione delle disposizioni del presente regolamento, ad esempio:

a) il trattamento equo e trasparente dei dati;

a bis) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;

b) la raccolta dei dati;

b ter) la pseudonimizzazione dei dati personali;

c) l'informazione del pubblico e degli interessati;

d) l'esercizio dei diritti degli interessati;

e) l'informazione e la protezione del minore e il modo in cui è ottenuto il consenso del titolare della responsabilità genitoriale sul minore;

e sexies) le misure e le procedure di cui agli articoli 22 e 23 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 30;

e septies) la notificazione di una violazione dei dati personali alle autorità di controllo e la comunicazione di detta violazione all'interessato;

f) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali;

g) (…)

h) le procedure stragiudiziali e di altro tipo per comporre le controversie tra responsabili del trattamento e interessati in materia di trattamento dei dati personali, fatti salvi i diritti degli interessati ai sensi degli articoli 73 e 75.

1 bis ter. Oltre ai responsabili del trattamento o agli incaricati del trattamento soggetti al presente regolamento, possono applicare i codici di condotta approvati ai sensi del paragrafo 2 e aventi validità generale a norma del paragrafo 4 anche i responsabili del trattamento o gli incaricati del trattamento non 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 42, paragrafo 2, lettera d). Detti responsabili del trattamento o incaricati del trattamento assumono l'impegno vincolante ed esecutivo, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

1 ter. Il codice di condotta a norma del paragrafo 1 bis contiene i meccanismi che consentono all'organismo di cui all'articolo 38 bis, paragrafo 1, di effettuare il controllo obbligatorio del rispetto delle norme del codice da parte dei responsabili del trattamento o degli incaricati del trattamento che si impegnano ad aderirvi, fatti salvi i compiti e i poteri dell'autorità di controllo competente ai sensi degli articoli 51 o 51 bis.

2. Le associazioni e gli altri organismi di cui al paragrafo 1 bis che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice all'autorità di controllo competente ai sensi dell'articolo 51. L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice o del codice modificato o prorogato e lo approva, se ritiene che offra garanzie sufficientemente adeguate.

2 bis. Qualora il parere di cui al paragrafo 2 confermi che il codice di condotta o il codice modificato o prorogato è conforme al presente regolamento e viene quindi approvato, e se il codice stesso non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice.

2 ter. Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvarlo l'autorità di controllo competente ai sensi dell'articolo 51 lo sottopone, tramite la procedura di cui all'articolo 57, al comitato europeo per la protezione dei dati, il quale formula un parere sulla conformità al presente regolamento del progetto di codice o del codice modificato o prorogato o, nel caso di cui al paragrafo 1 bis ter, sulla previsione di adeguate garanzie.

3. Qualora il parere di cui al paragrafo 2 ter confermi che i codici di condotta o i codici modificati o prorogati sono conformi al presente regolamento o, nel caso di cui al paragrafo 1 bis ter, forniscono adeguate garanzie, il comitato europeo per la protezione dei dati trasmette il suo parere alla Commissione.

4. La Commissione può decidere con atto di esecuzione che i codici di condotta approvati e le modifiche o proroghe dei codici di condotta approvati esistenti che le sono stati sottoposti ai sensi del paragrafo 3 hanno validità generale all'interno dell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.

5. La Commissione provvede ad un'appropriata divulgazione dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 4.

5 bis. Il comitato europeo per la protezione dei dati raccoglie in un registro tutti i codici di condotta approvati e le relative modifiche e li rende pubblici con qualsiasi mezzo appropriato.

Articolo 38 bis

Controllo dei codici di condotta approvati

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 52 e 53, il controllo della conformità con un codice di condotta ai sensi dell'articolo 38 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 tal fine se:
   a) riguardo al contenuto del codice ha dimostrato in modo convincente all'autorità di controllo competente di essere indipendente e competente;

   b) ha istituito procedure che gli consentono di valutare l'ammissibilità dei responsabili del trattamento e degli incaricati del trattamento in questione ad applicare il codice, di controllare che detti responsabili e incaricati ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento;

   c) ha istituito procedure e strutture atte a trattare i reclami concernenti violazioni del codice o il modo in cui il codice è stato o è attuato da un responsabile del trattamento o un incaricato del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico;

d) dimostra 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 europeo per la protezione dei dati il progetto di criteri per l'accreditamento dell'organismo di cui al paragrafo 1, ai sensi del meccanismo di coerenza di cui all'articolo 57.

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 prende, stanti adeguate garanzie, le opportune misure in caso di violazione del codice da parte di un responsabile del trattamento o incaricato del trattamento, tra cui la sospensione o l'esclusione dal codice del responsabile del trattamento o dell'incaricato 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 non sono conformi al presente regolamento.

6. Il presente articolo non si applica al trattamento di dati personali effettuato da autorità pubbliche e da organismi pubblici.

Articolo 39

Certificazione

1. Gli Stati membri, le autorità di controllo, il comitato europeo per la protezione dei dati 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 responsabili del trattamento e dagli incaricati del trattamento. Si tiene conto delle esigenze specifiche delle micro, piccole e medie imprese.

1 bis. I meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 2 bis, oltre ad essere applicati dai responsabili del trattamento e dagli incaricati del trattamento soggetti al presente regolamento, possono essere istituiti anche al fine di dimostrare la previsione di adeguate garanzie da parte dei responsabili del trattamento o incaricati 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 42, paragrafo 2, lettera e). Detti responsabili del trattamento o incaricati del trattamento assumono l'impegno vincolante ed esecutivo, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

1 ter. La certificazione è volontaria e accessibile tramite una procedura trasparente.

2. La certificazione ai sensi del presente articolo non riduce la responsabilità del responsabile del trattamento o dell'incaricato del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri dell'autorità di controllo competente a norma degli articoli 51 o 51 bis.

2 bis. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 39 bis o dall'autorità di controllo competente in base ai criteri approvati dalla stessa o, ai sensi dell'articolo 57, dal comitato europeo per la protezione dei dati. In quest'ultimo caso i criteri approvati dal comitato europeo per la protezione dei dati possono risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.

3 (nuovo). Il responsabile del trattamento o l'incaricato del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione di cui all'articolo 39 bis o, se del caso, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.

4. La certificazione è rilasciata al responsabile del trattamento o incaricato del trattamento per un periodo massimo di 3 anni e può essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti. È revocata, se del caso, dagli organismi di certificazione di cui all'articolo 39 bis o dall'autorità di controllo competente, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

5. Il comitato europeo per la protezione dei dati 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 39 bis

Organismo di certificazione e relativa procedura

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 52 e 53, la certificazione è rilasciata e rinnovata da un organismo di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati dopo averne informato l'autorità di controllo al fine di consentire, se del caso, l'esercizio dei suoi poteri a norma dell'articolo 53, paragrafo 1 ter, lettera f bis). Ogni Stato membro stabilisce se tali organismi di certificazione siano accreditati:

   a) dall'autorità di controllo competente ai sensi degli articoli 51 o 51 bis, e/o

   b) dall'organismo nazionale di accreditamento designato in virtù del 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 conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 51 o 51 bis.

2. L'organismo di certificazione di cui al paragrafo 1 può essere accreditato a tal fine solo se:

   a) riguardo al contenuto della certificazione ha dimostrato in modo convincente all'autorità di controllo competente di essere indipendente e competente;

a bis) si è impegnato a rispettare i criteri di cui all'articolo 39, paragrafo 2 bis, e approvati dall'autorità di controllo competente ai sensi degli articoli 51 o 51 bis o, ai sensi dell'articolo 57, dal comitato europeo per la protezione dei dati;

b) ha istituito procedure per il rilascio, il riesame periodico e il ritiro delle certificazioni, dei sigilli e dei marchi di protezione dei dati;

c) ha istituito procedure e strutture atte a trattare i reclami concernenti violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal responsabile del trattamento o dall'incaricato del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico;

d) dimostra 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'accreditamento degli organi di certificazione di cui al paragrafo 1 ha luogo in base ai criteri approvati dall'autorità di controllo competente ai sensi degli articoli 51 o 51 bis o, ai sensi dell'articolo 57, dal comitato europeo per la protezione dei dati. In caso di accreditamento ai sensi del paragrafo 1, lettera b), 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. L'organismo di certificazione di cui al paragrafo 1 è responsabile della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del responsabile del trattamento o dell'incaricato del trattamento riguardo alla conformità al presente regolamento. L'accreditamento è rilasciato per un periodo massimo di 5 anni e può essere rinnovato alle stesse condizioni purché l'organismo 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 e i criteri di cui all'articolo 39, paragrafo 2 bis, sono resi pubblici dall'autorità di controllo in forma facilmente accessibile. Le autorità di controllo provvedono a trasmetterli anche al comitato europeo per la protezione dei dati. Il comitato europeo per la protezione dei dati raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

6 bis. Fatte salve le disposizioni del capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento rilasciato all'organismo di certificazione 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 non sono conformi al presente regolamento.

7. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 86 al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati di cui all'articolo 39, paragrafo 1.

7 bis. (…)

8. La Commissione può stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere i meccanismi di certificazione e i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.

CAPO V

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

Articolo 40

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, è ammesso soltanto se il responsabile del trattamento e l'incaricato 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 tutela delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Articolo 41

Trasferimento previa 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, o un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscano 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), come anche l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le regole professionali e le misure di sicurezza, ivi comprese le regole 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 precedente 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 che siano rispettate le norme in materia di protezione dei dati, comprensiva di adeguati poteri sanzionatori, per assistere e consigliare gli 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 che un paese terzo, o un territorio o uno o più settori specifici all'interno del paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2. 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 campo di applicazione geografico e settoriale e, se del caso, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b). L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.

3 bis. (…)

4. (…)

4 bis. 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 e delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE.

5. Se le informazioni disponibili ne danno indicazione, in particolare in seguito al riesame di cui al paragrafo 3, la Commissione decide che un paese terzo, o un territorio o settore specifico all'interno del paese terzo, o un'organizzazione internazionale non garantisce più un livello di protezione adeguato ai sensi del paragrafo 2 e quindi revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 senza effetto retroattivo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 87, paragrafo 2, o, in casi di estrema urgenza, secondo la procedura di cui all'articolo 87, paragrafo 3.

5 bis. 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.

6. Una decisione ai sensi del paragrafo 5 lascia impregiudicato il trasferimento di dati personali verso il paese terzo, o il territorio o settore specifico all'interno del paese terzo, o verso l'organizzazione internazionale in questione, a norma degli articoli da 42 a 44.

7. 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.

8. Le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al paragrafo 3 o 5.

Articolo 42

Trasferimento in presenza di garanzie adeguate

1. In mancanza di una decisione ai sensi dell'articolo 41, paragrafo 3, il responsabile del trattamento o l'incaricato del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha offerto garanzie adeguate e a condizione che siano disponibili diritti azionabili degli interessati e mezzi di ricorso effettivi per gli interessati.

2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

oa) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici, o

a) le norme vincolanti d'impresa in conformità dell'articolo 43, o

b) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 87, paragrafo 2, o

c) 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 87, paragrafo 2, o

d) un codice di condotta approvato a norma dell'articolo 38, insieme all'impegno vincolante ed esecutivo da parte del responsabile del trattamento o dell'incaricato del trattamento nel paese terzo ad applicare le garanzie adeguate, compreso per quanto riguarda i diritti degli interessati, o

e) un meccanismo di certificazione approvato a norma dell'articolo 39, insieme all'impegno vincolante ed esecutivo da parte del responsabile del trattamento o dell'incaricato del trattamento nel paese terzo ad applicare le garanzie adeguate, compreso per quanto riguarda i diritti degli interessati.

2 bis. 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 responsabile del trattamento o l'incaricato del trattamento e il responsabile del trattamento, l'incaricato del trattamento o il destinatario dei dati 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 degli interessati.

3. (…)

4. (…)

5. (…)

5 bis. L'autorità di controllo applica il meccanismo di coerenza di cui all'articolo 57 nei casi di cui al paragrafo 2 bis.

5 ter. Le autorizzazioni emesse 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.

Articolo 43

Trasferimento in presenza di 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 57, a condizione che queste:

   a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo di imprese o gruppi 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;

   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 d'imprese in questione 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 di default, alla base giuridica del trattamento e al trattamento di specifiche categorie di dati personali sensibili, 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 dei suoi dati personali 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 20, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 75, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;

f) il fatto che il responsabile del trattamento o l'incaricato 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 responsabile del trattamento o l'incaricato del trattamento può essere esonerato in tutto o in parte da tale responsabilità dimostrando 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 14 e 14 bis;

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 e il controllo della formazione e della gestione dei reclami;

hh) le procedure di reclamo;

i) i meccanismi all'interno del gruppo 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 al consiglio dell'impresa controllante o del gruppo di imprese e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;

j) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;

k) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera i);

l) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e

m) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

2 bis. (…)

3. (…)

4. La Commissione può specificare il formato e le procedure per lo scambio di informazioni tra responsabili del trattamento, incaricati 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 87, paragrafo 2.

Articolo 43 bis (nuovo)

Trasferimento o divulgazione non autorizzati dal diritto dell'Unione

1. Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la divulgazione di dati personali da parte di un responsabile del trattamento o di un incaricato 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 motivi di trasferimento a norma del presente capo.

Articolo 44

Deroghe in specifiche situazioni

1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 41, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 42, 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 a condizione che:

   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, oppure

   b) il trasferimento sia necessario all’esecuzione di un contratto concluso tra l’interessato e il responsabile del trattamento ovvero all’esecuzione di misure precontrattuali prese su istanza dell’interessato, oppure

   c) il trasferimento sia necessario per la conclusione o l’esecuzione di un contratto stipulato tra il responsabile del trattamento e un'altra persona fisica o giuridica a favore dell’interessato, oppure

   d) il trasferimento sia necessario per importanti motivi di interesse pubblico, oppure

   e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria, oppure

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 dare il proprio consenso, oppure

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 purché sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri, oppure

h) se non è possibile basare il trasferimento su una disposizione degli articoli 41 o 42, comprese le norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni a norma delle lettere da a) a g) 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 preminenti del responsabile del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il responsabile del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia offerto garanzie adeguate per la protezione dei dati personali. Il responsabile del trattamento informa l'autorità di controllo in merito al trasferimento. In aggiunta alle informazioni di cui agli articoli 14 e 14 bis, il responsabile del trattamento informa l'interessato del trasferimento e degli interessi legittimi preminenti perseguiti dal responsabile del trattamento.

2. Il trasferimento di cui al paragrafo 1, lettera g), non può riguardare la totalità dei dati personali o intere categorie di dati personali contenute nel registro. Se il registro è destinato ad essere consultato da persone aventi un legittimo interesse, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora ne siano i destinatari.

3. (…)

4. Il paragrafo 1, lettere a), b), c) e h), non si applica alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

5. L'interesse pubblico di cui al paragrafo 1, lettera d), deve essere riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il responsabile del trattamento.

5 bis. 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 responsabile del trattamento o l'incaricato del trattamento attesta nel registro di cui all'articolo 28 la valutazione e le garanzie adeguate di cui al paragrafo 1, lettera h).

7. (…).

Articolo 45

Cooperazione internazionale per la protezione dei dati personali

1. 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 pratiche in materia di protezione dei dati personali, compresi i conflitti di giurisdizione con paesi terzi.

2. (…)

CAPO VI
AUTORITÀ DI CONTROLLO INDIPENDENTI

SEZIONE 1
INDIPENDENZA

Articolo 46

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 dei dati personali e di agevolare la libera circolazione dei dati personali all'interno dell'Unione.

1 bis. 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.

2. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità al comitato europeo per la protezione dei dati e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 57.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo entro la data di cui all'articolo 91, paragrafo 2, e comunica senza ritardo ogni successiva modifica.

Articolo 47

Indipendenza

1. Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei compiti e nell'esercizio dei poteri che le sono stati conferiti 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. 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 professionale incompatibile, remunerata o meno.

4. (…)

5. Ogni Stato membro provvede affinché ogni autorità di controllo sia dotata di risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei suoi compiti e l'esercizio dei suoi poteri, compresi quelli nell'ambito dell'assistenza reciproca, della cooperazione e della partecipazione al comitato europeo per la protezione dei dati.

6. Ogni Stato membro provvede affinché ogni autorità di controllo scelga e disponga di proprio personale, soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo.

7. Gli Stati membri garantiscono che ogni autorità di controllo sia soggetta a un controllo finanziario che non ne pregiudichi l'indipendenza. Gli Stati membri garantiscono che ogni autorità di controllo disponga di bilanci annuali, separati e pubblici che possono far parte del bilancio generale statale o nazionale.

Articolo 48

Condizioni generali per i membri dell'autorità di controllo

1. Gli Stati membri dispongono che ciascun membro dell'autorità di controllo debba essere nominato tramite una procedura trasparente:
   - dal parlamento, o
   - dal governo, o
   - dal capo di Stato dello Stato membro interessato, o
   - da un organismo indipendente incaricato ai sensi del diritto dello Stato membro della nomina.

2. Il membro o i membri possiedono le qualifiche, l'esperienza e le competenze, in particolare nel settore della protezione dei dati personali, richieste per l'esercizio delle loro funzioni e dei loro poteri.

3. Il mandato dei membri cessa alla scadenza del termine o in caso di dimissioni o di provvedimento d'ufficio, a norma del diritto dello Stato membro interessato.

4. Un membro può essere rimosso solo in casi di colpa grave o se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni.

Articolo 49

Norme sull'istituzione dell'autorità di controllo

1. Ogni Stato membro prevede con legge:

   a) l'istituzione di ogni autorità di controllo;

   b) le qualifiche e le condizioni di ammissibilità richieste per essere nominato membro di ogni autorità di controllo;

   c) le norme e le procedure per la nomina dei membri di ogni autorità di controllo;

d) la durata del mandato del membro o dei membri di ogni autorità di controllo, che non può essere inferiore a quattro anni, salvo per le prime nomine dopo l'entrata in vigore del presente regolamento, 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 vantaggi incompatibili con tali obblighi durante e dopo il mandato e le regole che disciplinano la cessazione del rapporto di lavoro.

g) (…)

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, l'obbligo del segreto professionale si applica in particolare alle segnalazioni da parte di persone fisiche di violazioni del presente regolamento.

Articolo 50

Segreto professionale

(…)

SEZIONE 2
COMPETENZA, COMPITI E POTERI

Articolo 51

Competenza

1. Ogni autorità di controllo è competente ad assolvere i compiti e a esercitare i poteri a essa assegnati a norma del presente regolamento nel territorio del suo Stato membro.

2. Se il trattamento è effettuato da autorità pubbliche o organismi privati che agiscono sulla base dell'articolo 6, paragrafo 1, lettere c) o e), è competente l'autorità di controllo dello Stato membro interessato. In tal caso, non si applica l'articolo 51 bis.

3. Le autorità di controllo non sono competenti per il controllo dei trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali.

Articolo 51 bis

Competenza dell'autorità di controllo capofila

1. Fatto salvo l'articolo 51, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del responsabile del trattamento o incaricato del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri del suddetto responsabile del trattamento o incaricato del trattamento, conformemente alla procedura di cui all'articolo 54 bis.

2 bis. In deroga al paragrafo 1, ogni autorità di controllo è competente per il trattamento dei reclami ad essa proposti o per il trattamento 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.

2 ter. Nei casi indicati al paragrafo 2 bis, l'autorità di controllo informa senza indugio l'autorità di controllo capofila sulla 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 conformemente alla procedura di cui all'articolo 54 bis, tenendo conto dell'esistenza o meno di uno stabilimento del responsabile del trattamento o incaricato del trattamento nello Stato membro dell'autorità di controllo che l'ha informata.

2 quater. Qualora l'autorità di controllo capofila decida di trattare il caso, si applica la procedura di cui all'articolo 54 bis. 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 preparazione del progetto di decisione di cui all'articolo 54 bis, paragrafo 2.

2 quinquies. 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 55 e 56.

3. L'autorità di controllo capofila è l'unico interlocutore del responsabile del trattamento o dell'incaricato del trattamento in merito al trattamento transfrontaliero da parte di tale responsabile del trattamento o incaricato del trattamento.

Articolo 52

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;

a bis) promuove la sensibilizzazione e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento dei dati personali. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;

a ter) fornisce consulenza, a norma del diritto nazionale, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali;

a quater) promuove la sensibilizzazione dei responsabili del trattamento e degli incaricati del trattamento riguardo agli obblighi imposti loro dal presente regolamento;

a quinquies) 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;

b) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 76, 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;

c) 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;

d) 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;

e) sorveglia gli sviluppi che presentano un interesse, se ed in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le pratiche commerciali;

f) adotta le clausole contrattuali tipo di cui all'articolo 26, paragrafo 2 quater, e all'articolo 42, paragrafo 2, lettera c);

f bis) redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 33, paragrafo 2 bis;

g) offre consulenza sui trattamenti di cui all'articolo 34, paragrafo 3;

g bis) incoraggia l'elaborazione di codici di condotta ai sensi dell'articolo 38 e fornisce un parere su tali codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma dell'articolo 38, paragrafo 2;

g ter) incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati a norma dell'articolo 39, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 39, paragrafo 2 bis;

g quater) ove del caso, effettua un riesame periodico delle certificazioni rilasciate in conformità dell'articolo 39, paragrafo 4;

h) definisce e pubblica i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 38 bis e di un organismo di certificazione ai sensi dell'articolo 39 bis;

h bis) effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 38 bis e di un organismo di certificazione ai sensi dell'articolo 39 bis;

h ter) autorizza le clausole contrattuali e le disposizioni di cui all'articolo 42, paragrafo 2 bis;

i) approva le norme vincolanti d'impresa ai sensi dell'articolo 43;

j) contribuisce alle attività del comitato europeo per la protezione dei dati;

j ter) tiene registri interni delle violazioni del presente regolamento e delle misure adottate, in particolare degli avvertimenti emessi e delle sanzioni imposte;

k) svolge qualsiasi altro compito legato alla protezione dei dati personali.

2. (…)

3. (…)

4. Ogni autorità di controllo agevola la proposizione di reclami di cui al paragrafo 1, lettera b), tramite provvedimenti quali, ad esempio, un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.

5. Ogni autorità di controllo svolge i propri compiti senza spese né per l'interessato né, eventualmente, per il responsabile della protezione dei dati.

6. 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 rifiutare di soddisfare la richiesta. Incombe all'autorità di controllo dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Articolo 53

Poteri

1. Ogni autorità di controllo ha i seguenti poteri di indagine:

a) ingiungere al responsabile del trattamento e all'incaricato del trattamento e, se del caso, al rappresentante del responsabile del trattamento o dell'incaricato del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;

a bis) condurre indagini sotto forma di verifiche sulla protezione dei dati;

a ter) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 39, paragrafo 4;

b) (…)

c) (…)

d) notificare al responsabile del trattamento o all'incaricato del trattamento le presunte violazioni del presente regolamento;

d bis) ottenere, dal responsabile del trattamento o dall'incaricato del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'adempimento dei suoi compiti;

d ter) ottenere accesso a tutti i locali del responsabile del trattamento e dell'incaricato del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale dello Stato membro.

1 ter. Ogni autorità di controllo ha i seguenti poteri correttivi:

a) rivolgere avvertimenti al responsabile del trattamento o all'incaricato del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;

b) rivolgere moniti al responsabile del trattamento o all'incaricato del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;

c bis) ingiungere al responsabile del trattamento o all'incaricato del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti derivantigli dal presente regolamento;

d) ingiungere al responsabile del trattamento o all'incaricato del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine;

d bis) ingiungere al responsabile del trattamento di comunicare all'interessato una violazione dei dati personali;

e) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

f) ordinare la rettifica, la limitazione o la cancellazione di dati a norma degli articoli 16, 17 e 17 bis e la notificazione di tali misure ai destinatari cui sono stati trasmessi i dati ai sensi dell'articolo 17, paragrafo 2 bis, e dell'articolo 17 ter;

f bis) (nuovo) ritirare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 39 e 39 bis, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;

g) irrogare una sanzione amministrativa pecuniaria ai sensi dell'articolo 79, oltre alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso;

h) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

i) (…)

j) (…)

1 quater. Ogni autorità di controllo ha i seguenti poteri autorizzativi e consultivi:

a) fornire consulenza al responsabile del trattamento, conformemente alla procedura di consultazione preventiva di cui all'articolo 34;

a bis) formulare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto nazionale, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali;

a ter) autorizzare il trattamento di cui all'articolo 34, paragrafo 7 bis, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare;

a quater) formulare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 38, paragrafo 2;

a quinquies) accreditare gli organismi di certificazione a norma dell'articolo 39 bis;

a sexies) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 39, paragrafo 2 bis;

b) adottare le clausole tipo di protezione dei dati di cui all'articolo 26, paragrafo 2 quater, e all'articolo 42, paragrafo 2, lettera c);

c) autorizzare le clausole contrattuali di cui all'articolo 42, paragrafo 2 bis, lettera a);

c bis) autorizzare gli accordi amministrativi di cui all'articolo 42, paragrafo 2 bis, lettera d);

d) approvare le norme vincolanti d'impresa ai sensi dell'articolo 43.

2. L'esercizio da parte di un'autorità di controllo dei poteri attribuitile 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 dei diritti fondamentali dell'Unione europea.

3. Ogni Stato membro prevede 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.

4. Ogni Stato membro può prevedere per legge che la sua autorità di controllo abbia ulteriori poteri rispetto a quelli di cui ai paragrafi 1, 1 ter e 1 quater. L'esercizio di tali poteri non pregiudica il funzionamento effettivo delle disposizioni del capo VII.

Articolo 54

Relazione di attività

Ogni autorità di controllo elabora una relazione annuale sulla propria attività, in cui può figurare un elenco dei tipi di violazioni notificate e di sanzioni imposte. La relazione è trasmessa al parlamento nazionale, al governo e alle altre autorità designate dal diritto nazionale ed è messa a disposizione del pubblico, della Commissione e del comitato europeo per la protezione dei dati.

CAPO VII
COOPERAZIONE E COERENZA

SEZIONE 1
COOPERAZIONE

Articolo 54 bis

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 nello sforzo per raggiungere un consenso. L'autorità di controllo capofila e le autorità di controllo interessate si scambiano tutte le informazioni utili.

1 bis. L'autorità di controllo capofila può chiedere in qualunque momento alle altre autorità di controllo interessate di fornire assistenza reciproca a norma dell'articolo 55 e può condurre operazioni congiunte a norma dell'articolo 56, in particolare per lo svolgimento di indagini o il controllo dell'attuazione di una misura concernente un responsabile del trattamento o incaricato del trattamento stabilito in un altro Stato membro.

2. 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.

3. Se una delle altre autorità di controllo interessate esprime un'obiezione pertinente e motivata al progetto di decisione entro un termine di quattro settimane dopo essere stata consultata conformemente al paragrafo 2, l'autorità di controllo capofila, ove non dia seguito all'obiezione o la ritenga non pertinente o non motivata, sottopone la questione al meccanismo di coerenza di cui all'articolo 57.

3 bis. L'autorità di controllo capofila, qualora intenda dare seguito all'obiezione formulata, 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 3 entro un termine di due settimane.

4. Se nessuna delle altre autorità di controllo interessate ha espresso obiezioni al progetto di decisione trasmesso dall'autorità di controllo capofila entro il termine di cui ai paragrafi 3 e 3 bis, l'autorità di controllo capofila e le autorità di controllo interessate sono considerate d'accordo con tale progetto di decisione e sono vincolate da esso.

4 bis. L'autorità di controllo capofila adotta la decisione e la notifica allo stabilimento principale o allo stabilimento unico del responsabile del trattamento o incaricato del trattamento, a seconda dei casi, e informa le altre autorità di controllo interessate e il comitato europeo per la protezione dei dati circa 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.

4 ter. In deroga al paragrafo 4 bis, se un reclamo è archiviato o respinto, l'autorità di controllo cui è stato proposto il reclamo adotta la decisione e la notifica al reclamante e ne informa il responsabile del trattamento.

4 ter b. Se l'autorità di controllo capofila e le autorità di controllo interessate convengono di archiviare o respingere 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 concernente azioni in relazione al responsabile del trattamento e la notifica allo stabilimento principale o allo stabilimento unico del responsabile del trattamento o dell'incaricato 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 concernente l'archiviazione o il rigetto di detto reclamo e la notifica a detto reclamante e ne informa il responsabile del trattamento o l'incaricato del trattamento.

4 quater. Dopo aver ricevuto la notifica della decisione dell'autorità di controllo capofila a norma dei paragrafi 4 bis e 4 ter b, il responsabile del trattamento o incaricato 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 responsabile del trattamento o incaricato del trattamento notifica le misure adottate per conformarsi alla decisione all'autorità di controllo capofila, che ne informa le altre autorità di controllo interessate.

4 quinquies. 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 61.

5. L'autorità di controllo capofila e le altre autorità di controllo interessate si scambiano reciprocamente per via elettronica, con modulo standard, le informazioni richieste a norma del presente articolo.

Articolo 55

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, al più tardi 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 cui è presentata una richiesta di assistenza non può rifiutare di darvi seguito, salvo che:

   a) non sia competente per trattare l'oggetto della richiesta o per le misure cui deve dare esecuzione, oppure

   b) l'intervento richiesto sia incompatibile con le disposizioni del presente regolamento o con il diritto dell'Unione o degli Stati membri cui è soggetta l'autorità di controllo che riceve la richiesta.

5. L'autorità di controllo che riceve la richiesta informa l'autorità di controllo richiedente dell'esito o, se del caso, dei progressi o delle misure adottate per rispondere alla richiesta. In caso di rifiuto della richiesta ai sensi del paragrafo 4, ne spiega i motivi.

6. Di norma le autorità di controllo forniscono per via elettronica, con modulo standard, le informazioni richieste da altre autorità di controllo.

7. Non è imposta alcuna spesa per le misure prese a seguito di una richiesta di assistenza reciproca. Le autorità di controllo possono concordare con altre autorità di controllo norme per l'indennizzo da parte di altre autorità di controllo di 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 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 51, paragrafo 1. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 61, paragrafo 1, e che sia necessaria una decisione vincolante d'urgenza da parte del comitato europeo per la protezione dei dati a norma dell'articolo 61, paragrafo 2.

9. (…)

10. La Commissione può specificare il formato e le procedure per l'assistenza reciproca di cui al presente articolo e le modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato europeo per la protezione dei dati, in particolare il modulo standard di cui al paragrafo 6. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.

Articolo 56

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. Nell'eventualità che il responsabile del trattamento o incaricato 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, a seconda del caso. Conformemente all'articolo 51 bis, paragrafi 1 o 2 quater, l'autorità di controllo competente 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, nel rispetto del diritto del proprio Stato membro 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 nazionale dell'autorità di controllo ospite.

3 bis. 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.

3 ter. 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 quest'ultimo gli importi corrisposti agli aventi diritto per conto di detti terzi.

3 quater. Fatto salvo l'esercizio dei suoi diritti nei confronti di terzi e fatta eccezione per il paragrafo 3 ter, ciascuno Stato membro rinuncia, nel caso previsto al paragrafo 1, a chiedere il risarcimento dei danni da esso subiti ad un altro Stato membro.

4. (…)

5. 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, le altre autorità di controllo possono adottare misure provvisorie nel territorio del loro Stato membro ai sensi dell'articolo 51. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 61, paragrafo 1, e che siano necessari un parere o una decisione vincolante d'urgenza da parte del comitato europeo per la protezione dei dati a norma dell'articolo 61, paragrafo 2.

6. (…)

SEZIONE 2

COERENZA

Articolo 57

Meccanismo di coerenza

1. 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 specificato nella presente sezione.

Articolo 58

Parere del comitato europeo per la protezione dei dati

1. Il comitato europeo per la protezione dei dati emette un parere ogniqualvolta un'autorità di controllo competente intende adottare una delle misure in appresso. A tal fine l'autorità di controllo competente comunica il progetto di decisione al comitato europeo per la protezione dei dati, quando la decisione:

   c) è finalizzata a stabilire un elenco di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 33, paragrafo 2 bis, oppure

   c bis) riguarda una questione di cui all'articolo 38, paragrafo 2 ter, concernente la conformità al presente regolamento di un progetto di codice di condotta o una modifica o proroga di un codice di condotta, oppure

   c ter) è finalizzata ad approvare i criteri per l'accreditamento di un organismo ai sensi dell'articolo 38 bis, paragrafo 3, o di un organismo di certificazione ai sensi dell'articolo 39 bis, paragrafo 3, oppure

   d) è finalizzata a determinare clausole tipo di protezione dei dati di cui all'articolo 42, paragrafo 2, lettera c), e all'articolo 26, paragrafo 2 quater, oppure

e) è finalizzata ad autorizzare clausole contrattuali di cui all'articolo 42, paragrafo 2 bis, lettera a), oppure

f) è finalizzata ad approvare norme vincolanti d'impresa ai sensi dell'articolo 43.

2. Qualsiasi autorità di controllo, il presidente del comitato europeo per la protezione dei dati 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 europeo per la protezione dei dati 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 55 o alle operazioni congiunte ai sensi dell'articolo 56.

3. Nei casi di cui ai paragrafi 1 e 2, il comitato europeo per la protezione dei dati 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 europeo per la protezione dei dati. 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 6, il membro che non abbia formulato obiezioni entro un termine ragionevole indicato dal presidente è considerato d'accordo con il progetto di decisione.

4. (…)

5. Senza ingiustificato ritardo, le autorità di controllo e la Commissione comunicano per via elettronica, con modulo standard, al comitato europeo per la protezione dei dati 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.

6. Il presidente del comitato europeo per la protezione dei dati informa, senza ingiustificato ritardo, per via elettronica:

   a) i membri del comitato europeo per la protezione dei dati e la Commissione di tutte le informazioni utili che sono state comunicate al comitato con modulo standard. Se necessario, il segretariato del comitato europeo per la protezione dei dati fornisce una traduzione delle informazioni utili;

   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.

7. (…)

7 bis. Entro il termine di cui al paragrafo 3 l'autorità di controllo competente non adotta il suo progetto di decisione di cui al paragrafo 1.

7 ter. (…)

8. L'autorità di controllo di cui al paragrafo 1 tiene nella massima considerazione il parere del comitato europeo per la protezione dei dati e, entro due settimane dal ricevimento del parere, comunica per via elettronica, con modulo standard, al presidente del comitato europeo per la protezione dei dati se mantiene o se modificherà il progetto di decisione e, se del caso, il progetto di decisione modificato.

9. Se entro il termine di cui al paragrafo 8 l'autorità di controllo interessata informa il presidente del comitato europeo per la protezione dei dati, fornendo le pertinenti motivazioni, che non intende conformarsi al parere del comitato, in tutto o in parte, si applica l'articolo 58 bis, paragrafo 1.

Articolo 58 bis

Composizione delle controversie da parte del comitato europeo per la protezione dei dati

1. Al fine di garantire l'applicazione corretta e coerente del presente regolamento nei singoli casi, il comitato europeo per la protezione dei dati adotta una decisione vincolante nei seguenti casi:

a) se, in un caso di cui all'articolo 54 bis, paragrafo 3, un'autorità di controllo interessata ha espresso un'obiezione pertinente e motivata a un progetto di decisione dell'autorità capofila o l'autorità capofila ha rigettato un'obiezione in quanto non pertinente e/o non motivata. La decisione vincolante riguarda tutte le questioni oggetto dell'obiezione pertinente e motivata, in particolare in caso di violazione del regolamento;

b) se vi sono opinioni contrastanti in merito alla competenza delle autorità di controllo interessate per lo stabilimento principale;

d) se un'autorità di controllo competente non richiede il parere del comitato europeo per la protezione dei dati nei casi di cui all'articolo 58, paragrafo 1, o non si conforma al parere del comitato europeo per la protezione dei dati emesso a norma dell'articolo 58. In tal caso qualsiasi autorità di controllo interessata o la Commissione può comunicare la questione al comitato europeo per la protezione dei dati.

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. Questo 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 mancanza di una maggioranza dei membri del comitato, la decisione è adottata mediante 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. (…)

6. Il presidente del comitato europeo per la protezione dei dati 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 europeo per la protezione dei dati dopo che l'autorità di controllo ha notificato la decisione definitiva di cui al paragrafo 7.

7. 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 senza ingiustificato ritardo e al più tardi entro un mese dalla notifica della decisione da parte del comitato europeo per la protezione dei dati. L'autorità di controllo capofila o, se del caso, l'autorità di controllo a cui è stato proposto il reclamo, informa il comitato europeo per la protezione dei dati circa la data in cui la decisione definitiva è notificata rispettivamente al responsabile del trattamento o all'incaricato del trattamento e all'interessato. La decisione definitiva delle autorità di controllo interessate è adottata ai sensi dell'articolo 54 bis, paragrafi 4 bis, 4 ter e 4 ter b. La decisione finale fa riferimento alla decisione di cui al paragrafo 1 e precisa che la decisione di cui al paragrafo 1 sarà pubblicata sul sito web del comitato europeo per la protezione dei dati conformemente al paragrafo 6. La decisione finale deve accludere la decisione di cui al paragrafo 1.

Articolo 59

Parere della Commissione

(...)

Articolo 60

Sospensione di un progetto di misura

(...)

Articolo 61

Procedura d'urgenza

1. In circostanze eccezionali, qualora ritenga che urga intervenire per tutelare i diritti e le libertà degli interessati, un'autorità di controllo interessata può, in deroga al meccanismo di coerenza di cui agli articoli 57, 58 e 58 bis, o alla procedura di cui all'articolo 54 bis, 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 europeo per la protezione dei dati 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 europeo per la protezione dei dati, 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 europeo per la protezione dei dati qualora un'autorità di controllo competente non abbia adottato misure adeguate in una situazione in cui urge intervenire per tutelare 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 58, paragrafo 3, e all'articolo 58 bis, 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 europeo per la protezione dei dati.

Articolo 62

Scambio di informazioni

1. La Commissione può adottare atti di esecuzione di portata generale per:

   a) (…)

   b) (…)

   c) (…)

   d) specificare le modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato europeo per la protezione dei dati, in particolare il modulo standard di cui all'articolo 58.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 87, paragrafo 2.

2. (…)

3. (…)

Articolo 63

Applicazione

(…)

SEZIONE 3

COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Articolo 64

Comitato europeo per la protezione dei dati

1 bis. Il comitato europeo per la protezione dei dati è istituito come organismo dell'Unione ed è dotato di personalità giuridica.

1 ter. Il comitato europeo per la protezione dei dati è rappresentato dal suo presidente.

2. Il comitato europeo per la protezione dei dati è composto dal responsabile di un'autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.

3. 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 nazionale di tale Stato membro.

4. La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato europeo per la protezione dei dati senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato europeo per la protezione dei dati comunica alla Commissione le attività del comitato europeo per la protezione dei dati.

5. Nei casi relativi all'articolo 58 bis, 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 in sostanza a quelli del presente regolamento.

Articolo 65

Indipendenza

1. Nell'adempimento dei suoi compiti o nell'esercizio dei suoi poteri ai sensi degli articoli 66 e 67, il comitato europeo per la protezione dei dati opera con indipendenza.

2. Fatte salve le richieste della Commissione di cui all'articolo 66, paragrafo 1, lettera b), e paragrafo 2, nell'adempimento dei suoi compiti o nell'esercizio dei suoi poteri il comitato europeo per la protezione dei dati non sollecita né accetta istruzioni da alcuno.

Articolo 66

Compiti del comitato europeo per la protezione dei dati

1. Il comitato europeo per la protezione dei dati garantisce l'applicazione coerente del presente regolamento. A tal fine, di propria iniziativa o, se del caso, su richiesta della Commissione:

a bis) monitora e assicura l'applicazione corretta del presente regolamento nei casi previsti all'articolo 57, paragrafo 3, fatti salvi i compiti delle autorità nazionali di controllo;

a) consiglia la Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, comprese eventuali proposte di modifica del presente regolamento;

a bis) consiglia la Commissione sul formato e le procedure per lo scambio di informazioni tra responsabili del trattamento, incaricati del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa;

a ter) (nuovo) pubblica linee direttrici, raccomandazioni e migliori pratiche 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;

b) 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 direttrici, raccomandazioni e migliori pratiche al fine di promuovere l'applicazione coerente del presente regolamento;

(b bis) (nuovo) pubblica linee direttrici, raccomandazioni e migliori pratiche conformemente all'articolo 66, paragrafo 1, lettera b), per precisare ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione ai sensi dell'articolo 20, paragrafo 2;

(b ter) (nuovo) pubblica linee direttrici, raccomandazioni e migliori pratiche conformemente all'articolo 66, paragrafo 1, lettera b), per accertare la violazione di dati personali e determinare l'ingiustificato ritardo di cui all'articolo 31, paragrafi 1 e 2, e le circostanze particolari in cui il responsabile del trattamento o l'incaricato del trattamento è tenuto a notificare la violazione dei dati personali;

(b quater) (nuovo) pubblica linee direttrici, raccomandazioni e migliori pratiche conformemente all'articolo 66, paragrafo 1, lettera b), 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 32, paragrafo 1;

(b quinquies) (nuovo) pubblica linee direttrici, raccomandazioni e migliori pratiche conformemente all'articolo 66, paragrafo 1, lettera b), al fine di precisare ulteriormente i criteri e i requisiti dei trasferimenti di dati basati sulle norme vincolanti d'impresa applicate, rispettivamente, dai responsabili del trattamento e dagli incaricati del trattamento, nonché gli ulteriori requisiti per garantire la protezione dei dati personali degli interessati di cui all'articolo 43;

(b sexies) (nuovo) pubblica linee direttrici, raccomandazioni e migliori pratiche conformemente all'articolo 66, paragrafo 1, lettera b), al fine di precisare ulteriormente i criteri e i requisiti dei trasferimenti di dati sulla base dell'articolo 44, paragrafo 1;

b bis) elabora per le autorità di controllo linee direttrici concernenti l'applicazione delle misure di cui all'articolo 53, paragrafi 1, 1 ter e 1 quater, e la fissazione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 79;

c) valuta l'applicazione pratica delle linee direttrici, raccomandazioni e migliori pratiche di cui alle lettere b) e b bis);

c bis 0)pubblica linee direttrici, raccomandazioni e migliori pratiche conformemente al paragrafo 1, lettera b), per stabilire procedure comuni per le segnalazioni da parte di persone fisiche di violazioni del presente regolamento ai sensi dell'articolo 49, paragrafo 2;

c bis) 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 38 e 39;

c ter) effettua l'accreditamento di organismi di certificazione e il suo riesame periodico a norma dell'articolo 39 bis e tiene un registro pubblico di organismi accreditati a norma dell'articolo 39 bis, paragrafo 6, e dei responsabili o incaricati del trattamento accreditati, stabiliti in paesi terzi a norma dell'articolo 39, paragrafo 4;

c quinquies) specifica i requisiti di cui dell'articolo 39 bis, paragrafo 3, ai fini dell'accreditamento degli organismi di certificazione ai sensi dell'articolo 39;

c quinquies bis) trasmette alla Commissione un parere in merito ai requisiti di certificazione di cui all'articolo 39 bis, paragrafo 7;

c quinquies ter) trasmette alla Commissione un parere in merito alle icone di cui all'articolo 12, paragrafo 4 ter;

c sexies) trasmette alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale, come pure per valutare se il paese terzo o il territorio o l'organizzazione internazionale o il settore specifico non garantiscano più un livello adeguato di protezione. A tal fine, la Commissione fornisce al comitato europeo per la protezione dei dati tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, il territorio o il settore di trattamento all'interno del paese terzo o l'organizzazione internazionale;

d) esprime pareri sui progetti di decisione delle autorità di controllo conformemente al meccanismo di coerenza di cui al paragrafo 2 e sulle questioni presentate conformemente all'articolo 57, paragrafo 4;

e) promuove la cooperazione e l'effettivo scambio di informazioni e pratiche tra le autorità di controllo a livello bilaterale e multilaterale;

f) 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;

g) promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle pratiche in materia di protezione dei dati tra autorità di controllo di tutto il mondo;

g ter) emette pareri sui codici di condotta redatti a livello di Unione a norma dell'articolo 38, paragrafo 4;

i) mantiene 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 europeo per la protezione dei dati, la Commissione può indicare un termine, tenuto conto dell'urgenza della questione.

3. Il comitato europeo per la protezione dei dati trasmette pareri, linee direttrici, raccomandazioni e migliori pratiche alla Commissione e al comitato di cui all'articolo 87, e li pubblica.

4. (…)

4 bis. Se del caso, il comitato europeo per la protezione dei dati consulta le parti interessate e offre loro la possibilità di esprimere commenti entro un termine ragionevole. Fatto salvo l'articolo 72, il comitato europeo per la protezione dei dati rende pubblici i risultati della procedura di consultazione.

Articolo 67

Relazioni

1. (…)

2. Il comitato europeo per la protezione dei dati redige una relazione annuale sulla tutela delle persone fisiche con riguardo al trattamento dei dati personali nell'Unione e, se del caso, nei paesi terzi e nelle organizzazioni internazionali. La relazione è pubblicata e viene trasmessa al Parlamento europeo, al Consiglio e alla Commissione.

3. La relazione annuale include la valutazione dell'applicazione pratica delle linee direttrici, raccomandazioni e migliori pratiche di cui all'articolo 66, paragrafo 1, lettera c), nonché delle decisioni vincolanti di cui all'articolo 57, paragrafo 3.

Articolo 68

Procedura

1. Il comitato europeo per la protezione dei dati decide a maggioranza semplice dei suoi membri, salvo se diversamente previsto dal presente regolamento.

2. Il comitato europeo per la protezione dei dati adotta il proprio regolamento interno deliberando a maggioranza di due terzi dei suoi membri e fissa le modalità del proprio funzionamento.

Articolo 69

Presidenza

1. Il comitato europeo per la protezione dei dati 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 70

Compiti del presidente

1. Il presidente ha il compito di:

   a) convocare le riunioni del comitato europeo per la protezione dei dati e stabilirne l'ordine del giorno;

   a bis) notificare le decisioni adottate dal comitato europeo per la protezione dei dati a norma dell'articolo 58 bis all'autorità di controllo capofila e alle autorità di controllo interessate;

   b) garantire l'adempimento tempestivo dei compiti del comitato europeo per la protezione dei dati, in particolare in relazione al meccanismo di coerenza di cui all'articolo 57.

2. Il comitato europeo per la protezione dei dati fissa nel proprio regolamento interno la ripartizione dei compiti tra presidente e vicepresidenti.

Articolo 71

Segreteria

1. Il comitato europeo per la protezione dei dati dispone di una segreteria messa a disposizione dal garante europeo della protezione dei dati.

1 bis. La segreteria svolge i propri compiti seguendo esclusivamente le istruzioni del presidente del comitato europeo per la protezione dei dati.

1 ter. Il personale del garante europeo della protezione dei dati coinvolto nell'assolvimento dei compiti assegnati al comitato europeo per la protezione dei dati 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.

1 quater. Se del caso, il comitato europeo per la protezione dei dati e il garante europeo della protezione dei dati stabiliscono e pubblicano un memorandum 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 assegnati al comitato europeo per la protezione dei dati dal presente regolamento.

2. La segreteria presta assistenza analitica, amministrativa e logistica al comitato europeo per la protezione dei dati.

3. La segreteria è incaricata in particolare:

a) della gestione ordinaria del comitato europeo per la protezione dei dati;

b) della comunicazione tra i membri del comitato europeo per la protezione dei dati, il suo presidente e la Commissione, e della comunicazione con le altre istituzioni e il pubblico;

c) dell'uso di mezzi elettronici per la comunicazione interna ed esterna;

d) della traduzione delle informazioni rilevanti;

e) della preparazione delle riunioni del comitato europeo per la protezione dei dati e del relativo seguito;

f) 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 europeo per la protezione dei dati.

Articolo 72

Riservatezza

1. Se il comitato europeo per la protezione dei dati lo ritiene necessario, le sue deliberazioni possono avere carattere riservato, come previsto dal suo regolamento interno.

2. L'accesso ai documenti trasmessi ai membri del comitato europeo per la protezione dei dati, agli esperti e ai rappresentanti di terzi è disciplinato dal regolamento (CE) n. 1049/2001.

3. (…)

CAPO VIII

RICORSI, RESPONSABILITÀ E SANZIONI

Articolo 73

Diritto di proporre reclamo all'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento dei dati personali che lo riguardano non sia conforme al presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure nel luogo della presunta violazione.

2. (…)

3. (…)

4. (…)

5. 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 74.

Articolo 74

Diritto a un ricorso giurisdizionale contro l'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 contro 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 competente ai sensi degli articoli 51 e 51 bis non abbia trattato un reclamo o non lo abbia informato entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 73.

3. Le azioni contro l'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

3 bis. Qualora siano promosse azioni contro una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato europeo per la protezione dei dati nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

4. (…)

5. (…)

Articolo 75

Diritto a un ricorso giurisdizionale effettivo contro il responsabile del trattamento o l'incaricato 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 73, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento in seguito a un trattamento dei suoi dati personali non conforme al presente regolamento.

2. Le azioni contro il responsabile del trattamento o l'incaricato del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il responsabile del trattamento o l'incaricato 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 responsabile del trattamento o l'incaricato del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

3. (…)

4. (…)

Articolo 76

Rappresentanza degli interessati

1. L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione, che siano debitamente costituiti secondo il diritto di uno Stato membro, che non abbiano scopo di lucro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della tutela 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 73, 74 e 75 nonché, se previsto dal diritto dello Stato membro, il diritto di ottenere il risarcimento di cui all'articolo 77.

2. Gli Stati membri possono prevedere che un organismo, organizzazione o associazione di cui al paragrafo 1, indipendentemente dal mandato conferito dall'interessato, abbia in tale Stato membro il diritto di proporre reclamo all'autorità di controllo competente, conformemente all'articolo 73, e di esercitare i diritti di cui agli articoli 74 e 75, qualora ritenga che i diritti di un interessato siano stati violati in seguito a un trattamento dei dati personali non conforme al presente regolamento.

3. (…)

4. (…)

5. (…)

Articolo 76 bis

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 responsabile del trattamento o dello stesso incaricato 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 responsabile del trattamento o dello stesso incaricato del trattamento siano pendenti presso un'autorità giurisdizionale in un altro Stato membro, qualunque autorità giurisdizionale competente successivamente adita può sospendere le azioni.

2 bis. 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 77

Diritto al risarcimento e responsabilità

1. Chiunque subisca un danno materiale o immateriale cagionato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal responsabile del trattamento o dall'incaricato del trattamento.

2. Un responsabile del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento non conforme al presente regolamento. Un incaricato del trattamento risponde per il danno cagionato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti agli incaricati del trattamento o ha agito in modo esterno o contrario alle legittime istruzioni del responsabile del trattamento.

3. Il responsabile del trattamento o l'incaricato del trattamento è esonerato dalla responsabilità, in conformità del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più responsabili del trattamento o incaricati del trattamento oppure un responsabile del trattamento e un incaricato del trattamento siano coinvolti nello stesso trattamento e siano, in conformità ai paragrafi 2 e 3, responsabili dell'eventuale danno cagionato dal trattamento, ogni responsabile del trattamento o incaricato del trattamento risponde per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un responsabile del trattamento o un incaricato del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale responsabile del trattamento o incaricato del trattamento ha il diritto di reclamare dagli altri responsabili del trattamento o incaricati 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 nazionale dello Stato membro di cui all'articolo 75, paragrafo 2.

Articolo 78

Sanzioni

(…)

Articolo 79

Condizioni generali per irrogare sanzioni amministrative pecuniarie

1 bis. Ogni autorità di controllo garantisce che le sanzioni amministrative pecuniarie irrogate ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 3 (nuovo), 3 bis (nuovo) e 3 bis bis (nuovo) siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. (…)

2 bis. Le sanzioni amministrative pecuniarie sono irrogate, in funzione delle circostanze di ogni singolo caso, oltre alle misure di cui all'articolo 53, paragrafo 1 ter , lettere da a) a f bis) e h), o in luogo di tali misure. Al momento di decidere se irrogare 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 in considerazione della natura, del campo di applicazione o della finalità del trattamento in questione nonché del numero di interessati lesi dal danno e del livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) (…)

d) le misure prese dal responsabile del trattamento o dall'incaricato del trattamento per attenuare il danno subito dagli interessati;

e) il grado di responsabilità del responsabile del trattamento o dell'incaricato del trattamento considerate le misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 23 e 30;

f) eventuali precedenti violazioni pertinenti commesse dal responsabile del trattamento o dall'incaricato del trattamento;

g) (nuovo) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g bis) (nuovo) 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 responsabile del trattamento o l'incaricato del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente imposti provvedimenti di cui all'articolo 53, paragrafo 1 ter, nei confronti del responsabile del trattamento o dell'incaricato 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 38 o ai meccanismi di certificazione approvati ai sensi dell'articolo 39;

k) (…)

m) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i vantaggi finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

2 ter. Se, in relazione allo stesso trattamento o a trattamenti collegati, un responsabile del trattamento o un incaricato del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non può superare l'importo precisato per la violazione più grave.

3. (…)

3 (nuovo). In conformità del paragrafo 2 bis, 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 responsabile del trattamento e dell'incaricato del trattamento a norma degli articoli 8, 10, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 39 e 39 bis;

a bis) gli obblighi dell'organismo di certificazione a norma degli articoli 39 e 39 bis;

a ter) gli obblighi dell'organismo di controllo a norma dell'articolo 38 bis, paragrafo 4;

3 bis (nuovo). In conformità del paragrafo 2 bis, 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 20;

b bis) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 40 a 44;

b ter) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

c) la mancata osservanza 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 di cui all'articolo 53, paragrafo 1 ter, o il negato accesso in violazione dell'articolo 53, paragrafo 1.

3 bis bis (nuovo). In conformità del paragrafo 2 bis, la mancata osservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 53, paragrafo 1 ter, 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.

3 ter. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 53, paragrafo 1 ter, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere irrogate sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

4. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile 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.

5. Se il sistema giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, l'articolo 79 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 entro la data di cui all'articolo 91, paragrafo 2, e comunicano senza ritardo ogni successiva modifica.

6. (…)

7. (…)

Articolo 79 ter

Sanzioni

1. Gli Stati membri determinano le sanzioni per le violazioni del presente regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 79, e prendono tutti i provvedimenti necessari per la loro applicazione. Tali sanzioni sono effettive, proporzionate e dissuasive.

2. (…)

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro la data di cui all'articolo 91, paragrafo 2, e comunica senza ritardo ogni successiva modifica.

CAPO IX
DISPOSIZIONI RELATIVE A SPECIFICHE SITUAZIONI DI TRATTAMENTO DEI DATI

Articolo 80

Trattamento di dati personali e libertà d'espressione e di informazione

1. Gli Stati membri conciliano con legge il diritto alla protezione dei dati personali ai sensi del presente regolamento e il diritto alla libertà d'espressione e di informazione, incluso il trattamento di dati personali a scopi giornalistici o di espressione accademica, artistica o letteraria.

2. Ai fini del trattamento dei dati personali effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono esenzioni o deroghe rispetto alle disposizioni di cui ai capi II (principi), III (diritti dell'interessato), IV (responsabile del trattamento e incaricato 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 80 bis

Trattamento dei dati personali 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 divulgati 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 80 bis bis

Trattamento di dati personali e riutilizzo delle informazioni del settore pubblico

(…)

Articolo 80 ter

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 81

Trattamento dei dati personali per finalità connesse alla salute

(…)

Articolo 81 bis

Trattamento di dati genetici

(…)

Articolo 82

Trattamento dei dati nei rapporti di lavoro

1. Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la tutela 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 concerne la trasparenza del trattamento, il trasferimento di dati nell'ambito di un gruppo di imprese e i sistemi di monitoraggio sul posto di lavoro.

2 bis. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro la data di cui all'articolo 91, paragrafo 2, e comunica senza ritardo ogni successiva modifica.

3. (…)

Articolo 83

Garanzie e deroghe per il trattamento di dati personali per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche

1. Il trattamento di dati personali per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche 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. Queste misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in questo modo. Qualora le finalità possano essere conseguite trattando ulteriormente dati che non consentano o non consentano più di identificare l'interessato, tali finalità devono essere conseguite in questo modo.

2. Se i dati personali sono trattati per finalità di ricerca scientifica e storica o per finalità statistiche, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 17 bis e 19, fatte salve le condizioni e le garanzie di cui al paragrafo 1, 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, 17 bis, 17 ter, 18 e 19, fatte salve le condizioni e le garanzie di cui al paragrafo 1, 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 84

Obblighi di segretezza

1. Gli Stati membri possono adottare norme specifiche per stabilire i poteri delle autorità di controllo di cui all'articolo 53, paragrafo 1, lettere d bis) e d ter), in relazione ai responsabili del trattamento o agli incaricati 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 responsabile del trattamento o l'incaricato del trattamento ha ricevuto o ha ottenuto nel corso di un'attività protetta da segreto professionale.

2. Ogni Stato membro notifica alla Commissione le norme adottate ai sensi del paragrafo 1 entro la data di cui all'articolo 91, paragrafo 2, e comunica senza ritardo ogni successiva modifica.

Articolo 85

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 dei dati personali, tali corpus possono continuare ad applicarsi purché siano conformi alle disposizioni del presente regolamento.

2. Le chiese e le associazioni religiose che applicano i corpus completi di norme di cui al paragrafo 1 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 86

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 4 quater, e all'articolo 39 bis, paragrafo 7, è conferita alla Commissione per un periodo indeterminato a decorrere dalla data di entrata in vigore del presente regolamento.

3. La delega di potere di cui all'articolo 12, paragrafo 4 quater, e all'articolo 39 bis, paragrafo 7, 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 4 quater, e all'articolo 39 bis, paragrafo 7, 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 87

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 88

Abrogazione della direttiva 95/46/CE

1. La direttiva 95/46/CE è abrogata a decorrere dalla data di cui all'articolo 91, paragrafo 2.

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 89

Rapporto con la direttiva 2002/58/CE

Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento dei dati personali 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 89 ter

Rapporto con accordi precedentemente conclusi

Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali relativi al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali conclusi dagli Stati membri prima dell'entrata in vigore del presente regolamento e conformi al diritto dell'Unione applicabile prima dell'entrata in vigore del presente regolamento.

Articolo 90

Valutazione

1. La Commissione trasmette al Parlamento europeo e al Consiglio, a scadenze regolari, relazioni di valutazione e sul riesame del presente regolamento.

2. Nel contesto di tali valutazioni la Commissione esamina, in particolare, l'applicazione e il funzionamento delle disposizioni:

   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 41, paragrafo 3, e alle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE;

   b) del capo VII su cooperazione e coerenza.

2 bis. Ai fini del paragrafo 1 la Commissione può richiedere informazioni agli Stati membri e alle autorità di controllo.

2 ter. 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.

3. Le prime relazioni sono trasmesse entro quattro anni dall'entrata in vigore del presente regolamento, le successive sono trasmesse ogni quattro anni. Le relazioni sono pubblicate.

4. 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 90 bis (nuovo)

Riesame di altri strumenti dell'UE in materia di protezione dei dati

Se del caso, la Commissione presenta proposte legislative di modifica di altri strumenti giuridici dell'UE in materia di protezione dei dati personali, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche con riguardo al trattamento dei dati personali. Ciò riguarda in particolare le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione e le norme sulla libera circolazione di tali dati.

Articolo 91

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 [*due anni dalla data di cui al paragrafo 1*]. *****

**** GU: inserire data***

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*