REGOLAMENTO (UE) 2018/1725 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 23 ottobre 2018

sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE

(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, paragrafo 2,

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]),

deliberando secondo la procedura legislativa ordinaria ([2]),

considerando quanto segue:

(1) La protezione delle persone fisiche in relazione al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. Tale diritto è garantito altresì dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

(2) Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([3]) conferisce alle persone fisiche diritti giuridicamente tutelati, precisa gli obblighi dei titolari del trattamento in seno alle istituzioni e agli organi dell'Unione e istituisce un'autorità di controllo indipendente, il Garante europeo della protezione dei dati, incaricata di sorvegliare il trattamento dei dati personali effettuato dalle istituzioni e dagli organi dell'Unione. Non si applica, però, al trattamento dei dati personali nel corso di un'attività delle istituzioni e degli organi dell'Unione che esuli dall'ambito di applicazione del diritto dell'Unione.

(3) Il 27 aprile 2016 sono stati adottati il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([4]) e la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio ([5]). Il regolamento stabilisce norme generali per la protezione delle persone fisiche in relazione al trattamento dei dati personali e per la libera circolazione dei dati personali nell'Unione, mentre la direttiva prevede norme specifiche per la protezione delle persone fisiche in relazione al trattamento dei dati personali e per la libera circolazione dei dati personali nell'Unione nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia.

(4) Il regolamento (UE) 2016/679 reca gli adeguamenti del regolamento (CE) n. 45/2001 necessari per assicurare un quadro di protezione dei dati solido e coerente nell'Unione e per consentirne l'applicazione parallelamente al regolamento (UE) 2016/679.

(5) È nell'interesse di un approccio coerente alla protezione dei dati in tutta l'Unione e della libera circolazione dei dati personali all'interno dell'Unione allineare per quanto possibile le norme sulla protezione dei dati per le istituzioni, gli organi e gli organismi dell'Unione a quelle adottate per il settore pubblico degli Stati membri. Quando le disposizioni del presente regolamento seguono gli stessi principi delle disposizioni del regolamento (UE) 2016/679,

---

([1]) GU C 288 del 31.8.2017, pag. 107.

([2]) Posizione del Parlamento europeo del 13 settembre 2018 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio dell'11 ottobre 2018.

([3]) Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati (GU L 8 del 12.1.2001, pag. 1).

([4]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([5]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016, pag. 89).

conformemente alla giurisprudenza della Corte di giustizia dell'Unione europea («Corte di giustizia») le disposizioni dei due regolamenti dovrebbero essere interpretate in modo omogeneo, in particolare in considerazione del fatto che il regime del presente regolamento dovrebbe essere inteso come equivalente a quello del regolamento (UE) 2016/679.

(6) Le persone i cui dati personali sono trattati da istituzioni e organi dell'Unione, in qualsiasi circostanza, ad esempio in quanto impiegate presso tali istituzioni e organi, dovrebbero essere tutelate. Il presente regolamento non si dovrebbe applicare al trattamento dei dati personali delle persone decedute. Esso non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

(7) Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate.

(8) È opportuno che il presente regolamento si applichi al trattamento dei dati personali da parte di tutte le istituzioni e di tutti gli organi e gli organismi dell'Unione. Dovrebbe applicarsi al trattamento di dati personali interamente o parzialmente automatizzato e al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.

(9) Nella dichiarazione n. 21, relativa alla protezione dei dati personali nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, allegata all'atto finale della conferenza intergovernativa che ha adottato il trattato di Lisbona, la conferenza riconosce che potrebbero rivelarsi necessarie, in considerazione della specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di dati personali nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia in base all'articolo 16 TFUE. Un capo distinto del presente regolamento contenente norme generali dovrebbe pertanto applicarsi al trattamento dei dati personali operativi, quali i dati personali trattati a fini di indagine penale da parte di organi o organismi dell'Unione nell'esercizio di attività nei settori della cooperazione giudiziaria e in materia penale e della cooperazione di polizia.

(10) La direttiva (UE) 2016/680 stabilisce norme armonizzate per la protezione e la libera circolazione dei dati personali trattati a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Al fine di assicurare lo stesso livello di protezione per le persone fisiche mediante diritti azionabili in tutta l'Unione e di prevenire disparità che possano ostacolare lo scambio di dati personali tra gli organi o gli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE e le autorità competenti, è opportuno che le norme per la protezione e la libera circolazione dei dati personali operativi trattati da tali organi o organismi dell'Unione siano coerenti con la direttiva (UE) 2016/680.

(11) Le norme generali del capo del presente regolamento relativo al trattamento dei dati personali operativi dovrebbero applicarsi fatte salve le norme specifiche applicabili al trattamento dei dati personali operativi da parte degli organi o degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE. Tali norme specifiche dovrebbero essere considerate come *lex specialis* rispetto alle disposizioni del capo del presente regolamento relativo al trattamento dei dati personali operativi (*lex specialis derogat legi generali*). Al fine di ridurre la frammentazione giuridica, le norme specifiche sulla protezione dei dati applicabili al trattamento dei dati personali operativi da parte degli organi o degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE dovrebbero essere coerenti con i principi alla base del capo del presente regolamento relativo al trattamento dei dati personali operativi, nonché con le disposizioni del presente regolamento relative al controllo indipendente, ai ricorsi giurisdizionali, alla responsabilità e alle sanzioni.

(12) Il capo del presente regolamento relativo al trattamento dei dati personali operativi dovrebbe applicarsi agli organi e agli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE, come compiti principali o accessori, a fini di prevenzione, accertamento, indagine o perseguimento di reati. Tuttavia, esso non dovrebbe applicarsi a Europol o alla Procura europea finché gli atti giuridici che istituiscono Europol e la Procura europea non siano stati modificati al fine di rendere loro applicabile il capo del presente regolamento relativo al trattamento dei dati personali operativi, nella versione adattata.

(13) La Commissione dovrebbe effettuare un riesame del presente regolamento, in particolare del capo del presente regolamento relativo al trattamento dei dati personali operativi. La Commissione dovrebbe altresì svolgere un riesame di altri atti giuridici adottati sulla base dei trattati che disciplinano il trattamento dei dati personali operativi

da parte degli organi o degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE. A seguito di tale riesame, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche in relazione al trattamento dei dati personali, la Commissione dovrebbe poter presentare opportune proposte legislative, compresi gli adeguamenti del capo del presente regolamento relativo al trattamento dei dati personali operativi, al fine di applicarlo a Europol e alla Procura europea. Gli adeguamenti dovrebbero tener conto delle disposizioni relative al controllo indipendente, ai ricorsi giurisdizionali, alla responsabilità e alle sanzioni.

(14) Il trattamento dei dati personali amministrativi, quali i dati relativi al personale, da parte degli organi o degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE dovrebbe essere disciplinato dal presente regolamento.

(15) Il presente regolamento dovrebbe applicarsi al trattamento dei dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea (TUE). Il presente regolamento non dovrebbe applicarsi al trattamento dei dati personali da parte delle missioni di cui all'articolo 42, paragrafo 1, e agli articoli 43 e 44 TUE, che attuano la politica di sicurezza e di difesa comune. Ove opportuno, dovrebbero essere presentate opportune proposte al fine di regolamentare ulteriormente il trattamento dei dati personali nel settore della politica di sicurezza e di difesa comune.

(16) È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori oggettivi, tra cui i costi e il tempo necessari per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.

(17) L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è intesa a precludere altre misure di protezione dei dati.

(18) Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (cookies) o a identificativi di altro tipo, come i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle.

(19) Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbero pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso. Tuttavia, l'interessato dovrebbe avere il diritto di revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento basata sul consenso espresso prima della revoca. Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto giuridico per il trattamento dei dati personali in un caso specifico in cui esista un evidente squilibrio tra l'interessato e il titolare del trattamento e sia pertanto improbabile

che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista.

(20) Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente in relazione alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che le riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso non autorizzato ai dati personali e alle attrezzature impiegate per il trattamento o l'utilizzo non autorizzato degli stessi, nonché per impedirne la comunicazione non autorizzata al momento della trasmissione.

(21) Conformemente al principio di responsabilizzazione, le istituzioni e gli organi dell'Unione, quando trasmettono dati personali all'interno della stessa istituzione o dello stesso organo dell'Unione e il destinatario non fa parte del titolare del trattamento o ad altre istituzioni o altri organi dell'Unione, dovrebbero verificare se tali dati personali sono necessari per il legittimo esercizio dei compiti che rientrano nelle competenze del destinatario. In particolare, a seguito della richiesta di trasmissione di dati personali da parte di un destinatario, il titolare del trattamento dovrebbe verificare la sussistenza di un motivo pertinente per effettuare in modo lecito il trattamento e la competenza del destinatario. Il titolare del trattamento dovrebbe anche effettuare una valutazione provvisoria della necessità della trasmissione dei dati. Qualora emergano dubbi su tale necessità, il titolare del trattamento dovrebbe chiedere ulteriori spiegazioni al destinatario. Il destinatario dovrebbe provvedere a che si possa successivamente verificare la necessità del trasferimento dei dati.

(22) Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sulla necessità delle istituzioni e degli organi dell'Unione di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, sulla necessità di adempiere a un obbligo legale al quale è soggetto il titolare del trattamento o su qualsiasi altra base legittima a norma del presente regolamento, incluso il consenso dell'interessato o la necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso. Il trattamento di dati personali per l'esercizio dei compiti svolti da istituzioni e organi dell'Unione nell'interesse pubblico comprende il trattamento dei dati personali necessari alla gestione e al funzionamento di tali istituzioni e organi. Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

(23) Il diritto dell'Unione di cui al presente regolamento dovrebbe essere chiaro e preciso, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità dei requisiti previsti dalla Carta e dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

(24) Le norme interne di cui al presente regolamento dovrebbero essere atti di applicazione generale chiari e precisi intesi a produrre effetti giuridici nei confronti degli interessati. Esse dovrebbero essere adottate al più alto livello di gestione delle istituzioni e degli organi dell'Unione, nell'ambito delle rispettive competenze e per questioni connesse al loro funzionamento, e dovrebbero essere pubblicate nella *Gazzetta ufficiale dell'Unione europea*. L'applicazione di tali norme dovrebbe essere prevedibile per le persone che vi sono sottoposte conformemente ai requisiti previsti dalla Carta e dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Le norme interne potrebbero assumere la forma di decisioni, in particolare ove adottate dalle istituzioni dell'Unione.

(25) Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali. Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile. L'ulteriore trattamento a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, dovrebbe tener conto, tra l'altro, di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo, della natura dei dati personali, delle conseguenze dell'ulteriore trattamento previsto per gli interessati e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

(26) Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di esprimere un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio ([1]) è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.

(27) I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe riguardare, in particolare, la creazione di profili di personalità e la raccolta di dati personali relativi ai minori quando sono proposti servizi direttamente a un minore sui siti web delle istituzioni e degli organi dell'Unione, quali i servizi di comunicazione interpersonale o la vendita di biglietti online, e il trattamento dei dati personali si basa sul consenso.

(28) I destinatari stabiliti nell'Unione diversi dalle istituzioni e dagli organi dell'Unione che desiderino che le istituzioni e gli organi dell'Unione trasmettano loro dati personali dovrebbero dimostrare che i dati sono necessari per l'esecuzione di un loro compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sono investiti. In alternativa, tali destinatari dovrebbero dimostrare che la trasmissione è necessaria al fine specifico di servire l'interesse pubblico e il responsabile del trattamento dovrebbe stabilire se sussistono motivi per presumere che gli interessi legittimi dell'interessato possano subire pregiudizio. In tali casi, il responsabile del trattamento dovrebbe chiaramente soppesare i vari interessi in conflitto al fine di valutare se la trasmissione di dati personali richiesta sia

([1]) Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori (GU L 95 del 21.4.1993, pag. 29).

proporzionata. Il fine specifico di servire l'interesse pubblico potrebbe riguardare la trasparenza delle istituzioni e degli organi dell'Unione. Nel rispetto del principio della trasparenza e della buona amministrazione, le istituzioni e gli organi dell'Unione dovrebbero dimostrare tale necessità quando danno origine a una trasmissione. I requisiti previsti dal presente regolamento per la trasmissione a destinatari stabiliti nell'Unione diversi dalle istituzioni e dagli organi dell'Unione dovrebbero essere intesi come complementari alle condizioni per il trattamento lecito.

(29) Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che non siano soddisfatte le condizioni specifiche di cui al presente regolamento. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, fermo restando che l'utilizzo dei termini «origine razziale» nel presente regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte. Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto se trattate attraverso un dispositivo tecnico specifico che consenta l'identificazione univoca o l'autenticazione di una persona fisica. Oltre ai requisiti specifici per il trattamento dei dati sensibili, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro per i casi in cui l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.

(30) Le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale. Pertanto il presente regolamento dovrebbe prevedere condizioni armonizzate per il trattamento di categorie particolari di dati personali relativi alla salute in relazione a esigenze specifiche, in particolare qualora il trattamento di tali dati sia svolto da persone vincolate dal segreto professionale per talune finalità connesse alla salute. Il diritto dell'Unione dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali delle persone fisiche.

(31) Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche. In tale contesto, la nozione di «sanità pubblica» dovrebbe essere interpretata secondo la definizione del regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio ([1]): tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità.

(32) Se i dati personali che tratta non gli consentono di identificare una persona fisica, il titolare del trattamento non dovrebbe essere obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione del presente regolamento. Tuttavia, il titolare del trattamento non dovrebbe rifiutare le ulteriori informazioni fornite dall'interessato al fine di sostenere l'esercizio dei suoi diritti. L'identificazione dovrebbe includere l'identificazione digitale di un interessato, ad esempio mediante un meccanismo di autenticazione quali le stesse credenziali, utilizzate dall'interessato per l'accesso (log in) al servizio online offerto dal titolare del trattamento.

(33) Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici dovrebbe essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie dovrebbero assicurare che siano state predisposte misure tecniche e organizzative al fine di garantire, in particolare, il principio della minimizzazione dei dati. L'ulteriore trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è da

([1]) Regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativo alle statistiche comunitarie in materia di sanità pubblica e di salute e sicurezza sul luogo di lavoro (GU L 354 del 31.12.2008, pag. 70).

effettuarsi quando il titolare del trattamento ha valutato la fattibilità di conseguire tali finalità trattando dati personali che non consentono o non consentono più di identificare l'interessato, purché esistano garanzie adeguate (come ad esempio la pseudonimizzazione dei dati personali). Le istituzioni e gli organi dell'Unione dovrebbero prevedere garanzie adeguate nel diritto dell'Unione, ed eventualmente nelle norme interne adottate dalle istituzioni e dagli organi dell'Unione relative a questioni connesse al loro funzionamento, per il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

(34) 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 o cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici. Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza indebito ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

(35) I principi di trattamento corretto e trasparente implicano che l'interessato sia informato dell'esistenza del trattamento e delle sue finalità. Il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati. Inoltre l'interessato dovrebbe essere informato dell'esistenza di una profilazione e delle conseguenze della stessa. In caso di dati personali raccolti direttamente presso l'interessato, questi dovrebbe inoltre essere informato dell'eventuale obbligo di fornire i dati personali e delle conseguenze in cui incorre se si rifiuta di fornirli. Tali informazioni potrebbero essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico.

(36) L'interessato dovrebbe ricevere le informazioni relative al trattamento di dati personali che lo riguardano al momento della raccolta presso l'interessato o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso. Se i dati personali possono essere legittimamente comunicati a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali. Il titolare del trattamento, qualora intenda trattare i dati personali per una finalità diversa da quella per cui sono stati raccolti, dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie. Qualora non sia possibile comunicare all'interessato l'origine dei dati personali perché sono state utilizzate varie fonti, dovrebbe essere fornita un'informazione di carattere generale.

(37) Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che lo riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce.

(38) L'interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che lo riguardano e il «diritto all'oblio» se la conservazione di tali data violi il presente regolamento o il diritto dell'Unione cui è soggetto il titolare del trattamento. L'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in

particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da Internet. L'interessato dovrebbe poter esercitare tale diritto nonostante il fatto che non è più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

(39) Per rafforzare il «diritto all'oblio» nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento che ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali. Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a sua disposizione, comprese le misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali.

(40) Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web. Negli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

(41) Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati. Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili. Qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente regolamento. Inoltre tale diritto non dovrebbe pregiudicare il diritto dell'interessato di ottenere la cancellazione dei dati personali e le limitazioni di tale diritto di cui al presente regolamento e non dovrebbe segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto. Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro.

(42) Qualora i dati personali possano essere lecitamente trattati, essendo il trattamento necessario per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, l'interessato dovrebbe comunque avere il diritto di opporsi al trattamento dei dati personali che riguardano la sua situazione particolare. È opportuno che incomba al titolare del trattamento dimostrare che i suoi interessi legittimi cogenti prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato.

(43) L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che può includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali le pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica,

la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.

Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore. Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e che impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero trattamenti che risultino in 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.

(44) Gli atti giuridici adottati sulla base dei trattati o le norme interne adottate dalle istituzioni e dagli organi dell'Unione relative a questioni connesse al loro funzionamento possono imporre limitazioni a specifici principi e ai diritti di informazione, accesso e rettifica o cancellazione dei dati personali, al diritto alla portabilità dei dati, alla riservatezza dei dati delle comunicazioni elettroniche nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento, ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica e per la prevenzione, l'indagine e il perseguimento di reati o l'esecuzione di sanzioni penali. Ciò comprende la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, la tutela della vita umana, in particolare in risposta a catastrofi di origine naturale o umana, la sicurezza interna delle istituzioni e degli organi dell'Unione, altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare gli obiettivi della politica estera e di sicurezza comune dell'Unione o un interesse economico o finanziario rilevante dell'Unione o di uno Stato membro, e la tenuta di registri pubblici per ragioni di interesse pubblico generale o la tutela dell'interessato o dei diritti e delle libertà altrui, compresi la protezione sociale, la sanità pubblica e gli scopi umanitari.

(45) È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

(46) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o èa loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

(47) La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

(48) La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle prescrizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. I principi della protezione dei dati fin dalla progettazione e di default dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici.

(49) Il regolamento (UE) 2016/679 prevede che i titolari del trattamento dimostrino il rispetto degli obblighi ad essi incombenti attraverso l'adesione a meccanismi di certificazione approvati. Allo stesso modo, le istituzioni e gli organi dell'Unione dovrebbero essere in grado di dimostrare la conformità al presente regolamento ottenendo la certificazione in conformità dell'articolo 42 del regolamento (UE) 2016/679.

(50) La protezione dei diritti e delle libertà degli interessati così come la responsabilità generale dei titolari del trattamento e dei responsabili del trattamento esigono una chiara ripartizione delle responsabilità nell'ambito del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento è eseguita per conto del titolare del trattamento.

(51) Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino le prescrizioni del presente regolamento, anche per la sicurezza del trattamento. L'applicazione da parte dei responsabili del trattamento diversi dalle istituzioni e dagli organi dell'Unione di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento. L'esecuzione dei trattamenti da parte di un responsabile del trattamento diverso da un'istituzione o un organo dell'Unione dovrebbe essere disciplinata da un contratto o, nel caso in cui istituzioni e organi dell'Unione agiscano in qualità di responsabili del trattamento, da un contratto o da altro atto giuridico a norma del diritto dell'Unione che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e delle responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato. Il titolare del trattamento e il responsabile del trattamento dovrebbero poter scegliere di usare un contratto individuale o clausole contrattuali tipo che sono adottate direttamente dalla Commissione oppure dal Garante europeo della protezione dei dati e successivamente dalla Commissione. Dopo il completamento del trattamento per conto del titolare del trattamento, il responsabile del trattamento dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali, salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione di tali dati personali.

(52) Per dimostrare che si conformano al presente regolamento, i titolari del trattamento dovrebbero tenere un registro delle attività di trattamento effettuate sotto la propria responsabilità e i responsabili del trattamento dovrebbero tenere un registro delle categorie di attività di trattamento effettuate sotto la propria responsabilità. Le istituzioni e gli organi dell'Unione dovrebbero essere obbligati a cooperare con il Garante europeo della protezione dei dati e a mettere, su richiesta, i propri registri a sua disposizione affinché possano servire per monitorare detti trattamenti. Salvo i casi in cui ciò non sia appropriato date le dimensioni di un'istituzione o un organo dell'Unione, è opportuno che le istituzioni e gli organi dell'Unione possano istituire un registro centrale in cui registrare le proprie attività di trattamento. Per motivi di trasparenza, dovrebbero poter rendere pubblico tale registro.

(53) Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura

dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione non autorizzata a dati personali trasmessi, conservati o comunque elaborati che potrebbero cagionare in particolare un danno fisico, materiale o immateriale, o l'accesso a tali dati.

(54) Le istituzioni e gli organi dell'Unione dovrebbero garantire la riservatezza delle comunicazioni elettroniche come disposto dall'articolo 7 della Carta. In particolare le istituzioni e gli organi dell'Unione dovrebbero garantire la sicurezza delle proprie reti di comunicazione elettronica. Dovrebbero proteggere le informazioni relative alle apparecchiature terminali degli utenti che accedono ai loro siti web e alle applicazioni per dispositivi mobili a disposizione del pubblico in ottemperanza alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([1]) e proteggere inoltre i dati personali conservati in elenchi di utenti.

(55) Una violazione dei dati personali, se non affrontata in modo adeguato e tempestivo, potrebbe provocare danni fisici, materiali o immateriali alle persone fisiche. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificarla al Garante europeo della protezione dei dati, senza indebito o ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. Qualora il ritardo sia giustificato, si dovrebbero comunicare quanto prima le informazioni meno sensibili o meno specifiche sulla violazione invece di risolvere completamente l'incidente sottostante prima di procedere alla notifica.

(56) Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con il Garante europeo della protezione dei dati, nel rispetto degli orientamenti impartiti da questo o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge.

(57) Il regolamento (CE) n. 45/2001 ha introdotto l'obbligo generale in capo al titolare del trattamento di notificare il trattamento dei dati personali al responsabile della protezione dei dati. Salvo i casi in cui ciò non sia appropriato date le dimensioni dell'istituzione o dell'organo dell'Unione, il responsabile della protezione dei dati deve tenere un registro dei trattamenti notificati. Oltre a tale obbligo generale, è opportuno istituire meccanismi e procedure efficaci per monitorare i trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali procedure dovrebbero essere altresì poste in essere, in particolare, quando i tipi di trattamenti comportano l'utilizzo di nuove tecnologie o sono di nuovo tipo in relazione a cui il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati o laddove se ne riveli la necessità alla luce del tempo trascorso dal trattamento iniziale. In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio elevato, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio, assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento.

(58) Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il titolare del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno consultare il Garante europeo della protezione dei dati prima dell'inizio delle attività di trattamento. Tale rischio elevato potrebbe scaturire da certi tipi di trattamento e dall'estensione e frequenza del trattamento, da cui potrebbe derivare altresì un danno o un'interferenza con i diritti e le libertà della persona fisica. Il Garante europeo della protezione dei dati che riceve una richiesta di consultazione dovrebbe darvi seguito entro un termine determinato. Tuttavia, la mancanza di reazione

([1]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

del Garante europeo della protezione dei dati entro tale termine dovrebbe far salvo ogni intervento dello stesso 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, dovrebbe essere possibile presentare al Garante europeo della protezione dei dati il risultato di una valutazione d'impatto sulla protezione dei dati effettuata riguardo al trattamento in questione, in particolare le misure previste per attenuare il rischio per i diritti e le libertà delle persone fisiche.

(59) Il Garante europeo della protezione dei dati dovrebbe essere informato circa le misure amministrative e consultato in merito alle norme interne adottate dalle istituzioni e dagli organi dell'Unione relative a questioni connesse al loro funzionamento quando prevedono il trattamento di dati personali, stabiliscono le condizioni per le limitazioni dei diritti degli interessati o fissano garanzie adeguate per i diritti dell'interessato, al fine di garantire la conformità del trattamento previsto al presente regolamento, in particolare riguardo all'attenuazione dei rischi per l'interessato.

(60) Il regolamento (UE) 2016/679 ha istituito il comitato europeo per la protezione dei dati quale organo indipendente dell'Unione dotato di personalità giuridica. Il comitato dovrebbe contribuire all'applicazione coerente del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680 in tutta l'Unione, fornendo anche consulenza alla Commissione. Nel contempo il Garante europeo della protezione dei dati dovrebbe continuare a esercitare le proprie funzioni di controllo e consulenza in relazione a tutte le istituzioni e tutti gli organi dell'Unione, di propria iniziativa o su richiesta. Per garantire la coerenza delle norme sulla protezione dei dati in tutta l'Unione, la Commissione, all'atto della preparazione di proposte o raccomandazioni, dovrebbe sforzarsi di consultare il garante europeo della protezione dei dati. La Commissione dovrebbe avere l'obbligo di condurre una consultazione a seguito dell'adozione di atti legislativi o durante la preparazione di atti delegati e atti di esecuzione di cui agli articoli 289, 290 e 291 TFUE e a seguito dell'adozione di raccomandazioni e proposte relative ad accordi con paesi terzi e organizzazioni internazionali di cui all'articolo 218 TFUE se questi incidono sul diritto alla protezione dei dati personali. In tali casi la Commissione dovrebbe avere l'obbligo di consultare il Garante europeo della protezione dei dati, tranne qualora il regolamento (UE) 2016/679 stabilisca la consultazione obbligatoria del comitato europeo per la protezione dei dati, ad esempio per le decisioni di adeguatezza o gli atti delegati riguardanti le icone standardizzate e i requisiti dei meccanismi di certificazione. Qualora l'atto in questione sia di particolare rilevanza per la tutela dei diritti e delle libertà fondamentali delle persone fisiche in relazione al trattamento di dati personali, la Commissione dovrebbe altresì poter consultare il comitato europeo per la protezione dei dati. In tali casi il Garante europeo della protezione dei dati, in quanto membro del comitato europeo per la protezione dei dati, dovrebbe coordinare le proprie attività con quest'ultimo al fine di emettere un parere congiunto. Il Garante europeo della protezione dei dati e, ove applicabile, il comitato europeo per la protezione dei dati dovrebbero fornire la propria consulenza per iscritto entro otto settimane. Tale termine dovrebbe essere più breve in caso di urgenza o ove altrimenti appropriato, ad esempio quando la Commissione elabora atti delegati o di esecuzione.

(61) In conformità dell'articolo 75 del regolamento (UE) 2016/679, il Garante europeo della protezione dei dati dovrebbe assicurare il segreteriato del comitato europeo per la protezione dei dati.

(62) In tutte le istituzioni e tutti gli organi dell'Unione un responsabile della protezione dei dati dovrebbe garantire che l'applicazione del presente regolamento e consigliare i titolari del trattamento e i responsabili del trattamento nell'assolvimento dei loro obblighi. Il responsabile della protezione dei dati dovrebbe essere una persona con il livello necessario di conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, che dovrebbe essere determinato, in particolare, in base ai trattamenti di dati effettuati dal titolare o dal responsabile del trattamento e alla protezione richiesta per i dati personali interessati. Tali responsabili della protezione dei dati dovrebbero poter adempiere le funzioni e i compiti loro incombenti in maniera indipendente.

(63) È opportuno che, quando i dati personali sono trasferiti da istituzioni e organi dell'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, sia garantito il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento. Le stesse garanzie dovrebbero applicarsi nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali possono essere effettuati soltanto nel pieno rispetto del presente regolamento e dei diritti e delle libertà fondamentali sanciti dalla Carta. Il trasferimento potrebbe aver luogo soltanto se, fatte salve le altre disposizioni del presente regolamento, il titolare del trattamento o il responsabile del trattamento rispetta le condizioni stabilite dalle disposizioni del presente regolamento in relazione al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

(64) A norma dell'articolo 45 del regolamento (UE) 2016/679 o dell'articolo 36 della direttiva (UE) 2016/680, la Commissione può riconoscere che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale offre un livello adeguato di protezione dei dati. In tali casi, i trasferimenti di dati personali verso tale paese terzo o organizzazione internazionale da parte di un'istituzione o di un organo dell'Unione possono avere luogo senza ulteriori autorizzazioni.

(65) In mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento dovrebbe provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato. Tali adeguate garanzie possono consistere nell'applicazione di clausole tipo di protezione dei dati adottate dalla Commissione, clausole tipo di protezione dei dati adottate dal Garante europeo della protezione dei dati o clausole contrattuali autorizzate dal Garante europeo della protezione dei dati. Quando il responsabile del trattamento non è un'istituzione o un organo dell'Unione, tali adeguate garanzie possono anche consistere in norme vincolanti d'impresa, codici di condotta e meccanismi di certificazione utilizzati per i trasferimenti internazionali a norma del regolamento (UE) 2016/679. Tali garanzie dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi, fra cui il ricorso effettivo in sede amministrativa o giudiziale e la richiesta di risarcimento, nell'Unione o in un paese terzo. Esse dovrebbero riguardare, in particolare, la conformità 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 istituzioni e organi dell'Unione 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 del Garante europeo della protezione dei dati dovrebbe essere ottenuta quando le garanzie sono offerte nell'ambito di accordi amministrativi giuridicamente non vincolanti.

(66) La possibilità che il titolare del trattamento o il responsabile del trattamento utilizzi clausole tipo di protezione dei dati adottate dalla Commissione o dal Garante europeo della protezione dei dati non dovrebbe precludere ai titolari del trattamento o ai responsabili del trattamento la possibilità di includere tali clausole tipo in un contratto più ampio, anche in un contratto tra il responsabile del trattamento e un altro responsabile del trattamento, né di aggiungere altre clausole o garanzie supplementari, purché non contraddicano, direttamente o indirettamente, le clausole contrattuali tipo adottate dalla Commissione o dal Garante europeo della protezione dei dati o ledano i diritti o le libertà fondamentali degli interessati. I titolari del trattamento e i responsabili del trattamento dovrebbero essere incoraggiati a fornire garanzie supplementari attraverso impegni contrattuali che integrino le clausole tipo di protezione dei dati.

(67) Alcuni paesi terzi adottano leggi, regolamenti e altri atti normativi finalizzati a disciplinare direttamente le attività di trattamento delle istituzioni e degli organi dell'Unione. Essi possono includere le sentenze di autorità giurisdizionali o le decisioni di autorità amministrative di paesi terzi che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento e non sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione. L'applicazione extraterritoriale di tali leggi, regolamenti e altri atti normativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della protezione delle persone fisiche assicurata nell'Unione con il presente regolamento. I trasferimenti dovrebbero quindi essere consentiti solo se ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi. Ciò vale, tra l'altro, quando la comunicazione è necessaria per un rilevante motivo di interesse pubblico riconosciuto dal diritto dell'Unione.

(68) È opportuno prevedere in situazioni specifiche la possibilità di trasferire dati in alcune circostanze se l'interessato ha esplicitamente acconsentito, se il trasferimento è occasionale e necessario in relazione a un contratto o un'azione legale, che sia in sede giudiziale, amministrativa o stragiudiziale, compresi i procedimenti dinanzi alle autorità di regolamentazione. È altresì opportuno prevedere la possibilità di trasferire dati se sussistono motivi di rilevante interesse pubblico previsti dal diritto dell'Unione o se i dati sono trasferiti da un registro stabilito per legge e destinato a essere consultato dal pubblico o dalle persone aventi un interesse legittimo. In quest'ultimo caso, il trasferimento non dovrebbe riguardare la totalità dei dati personali o delle categorie di dati contenuti nel registro, salvo se il diritto dell'Unione lo autorizza; inoltre, quando il registro è destinato a essere consultato dalle persone aventi un interesse legittimo, i dati dovrebbero essere trasferiti soltanto su richiesta di queste o, se ne sono destinatarie, tenendo pienamente conto degli interessi e dei diritti fondamentali dell'interessato.

(69) 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 istituzioni e organi dell'Unione e autorità garanti della concorrenza, amministrazioni fiscali o doganali, autorità di controllo finanziario e servizi competenti in materia di sicurezza sociale o sanità pubblica, ad esempio in caso di ricerca di contatti per malattie contagiose o al fine di ridurre e/o eliminare il doping nello sport. Il trasferimento di dati personali dovrebbe essere

altresì considerato lecito quando è necessario per salvaguardare un interesse che è essenziale per gli interessi vitali dell'interessato o di un'altra persona, comprese la vita o l'integrità fisica, qualora l'interessato si trovi nell'incapacità di prestare il proprio consenso. In mancanza di una decisione di adeguatezza, il diritto dell'Unione 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. Qualunque trasferimento a un'organizzazione internazionale umanitaria di dati personali di un interessato che si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso ai fini dell'esecuzione di un compito derivante dalle convenzioni di Ginevra o al fine di rispettare il diritto internazionale umanitario applicabile nei conflitti armati potrebbe essere considerato necessario per importanti motivi di interesse pubblico o nell'interesse vitale dell'interessato.

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

(71) Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo nazionali e il Garante europeo della protezione dei dati possono non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività che esulano dalla loro competenza territoriale. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati dall'insufficienza di poteri per prevenire o correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. Pertanto è opportuno promuovere una più stretta cooperazione tra il Garante europeo della protezione dei dati e le autorità di controllo nazionali affinché possano scambiare informazioni con le loro controparti internazionali.

(72) L'istituzione, mediante il regolamento (CE) n. 45/2001, del Garante europeo della protezione dei dati, cui è conferito il potere di eseguire compiti ed esercitare poteri in totale indipendenza, è un elemento essenziale della protezione delle persone fisiche in relazione al trattamento dei loro dati personali. Il presente regolamento dovrebbe rafforzarne e chiarirne ulteriormente il ruolo e l'indipendenza. Il Garante europeo della protezione dei dati dovrebbe essere una persona che offra ogni garanzia di indipendenza e che possieda un'esperienza e delle competenze notorie per l'esercizio delle funzioni di Garante europeo della protezione dei dati, come, ad esempio, l'aver fatto parte di una delle autorità di controllo di cui all'articolo 51 del regolamento (UE) 2016/679.

(73) Al fine di garantire un monitoraggio e un'applicazione coerenti delle norme in materia di protezione dei dati in tutta l'Unione, il Garante europeo della protezione dei dati dovrebbe avere gli stessi compiti e poteri effettivi delle autorità di controllo nazionali, fra cui poteri di indagine, poteri correttivi e sanzionatori, e poteri autorizzativi e consultivi, segnatamente in caso di reclamo proposto da persone fisiche, e il potere di intentare un'azione dinanzi alla Corte di giustizia e di agire in sede giudiziale conformemente alle disposizioni del diritto primario 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. Onde evitare costi superflui ed eccessivi disagi alle persone interessate che potrebbero subire pregiudizio, ogni misura del Garante europeo della protezione dei dati dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità al presente regolamento, dovrebbe tenere conto delle circostanze di ciascun singolo caso e rispettare il diritto di ogni persona di essere ascoltata prima che nei suoi confronti sia adottato un provvedimento individuale. Ogni misura giuridicamente vincolante del Garante europeo della protezione dei dati dovrebbe avere forma scritta, essere chiara e univoca, riportare la data di adozione della misura, recare la firma del Garante europeo della protezione dei dati, precisare i motivi della misura e fare riferimento al diritto a un ricorso effettivo.

(74) Non è opportuno che rientri nella competenza di controllo del Garante europeo della protezione dei dati il trattamento di dati personali effettuato dalla Corte di giustizia nell'esercizio delle sue funzioni giurisdizionali, al fine di salvaguardare l'indipendenza della Corte nell'adempimento dei suoi compiti giurisdizionali, compreso il processo decisionale. Per tali trattamenti, la Corte dovrebbe istituire un controllo indipendente conformemente all'articolo 8, paragrafo 3, della Carta, ad esempio attraverso un meccanismo interno.

(75) È opportuno che le decisioni del Garante europeo della protezione dei dati riguardanti le deroghe, le garanzie, le autorizzazioni e le condizioni relative ai trattamenti di dati, quali definiti dal presente regolamento, siano pubblicate nel rapporto sulle attività svolte. A prescindere dalla pubblicazione annuale del rapporto sulle attività svolte, il Garante europeo della protezione dei dati può pubblicare relazioni su temi specifici.

(76) Il Garante europeo della protezione dei dati dovrebbe rispettare il regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([1]).

(77) Le autorità di controllo nazionali sorvegliano l'applicazione del regolamento (UE) 2016/679 e contribuiscono 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. Al fine di aumentare la coerenza dell'applicazione delle norme in materia di protezione dei dati applicabili negli Stati membri e di quelle applicabili alle istituzioni e agli organi dell'Unione, il Garante europeo della protezione dei dati dovrebbe cooperare efficacemente con le autorità di controllo nazionali.

(78) In taluni casi, il diritto dell'Unione prevede un modello di controllo coordinato, condiviso tra il Garante europeo della protezione dei dati e le autorità di controllo nazionali. Il Garante europeo della protezione dei dati è altresì l'autorità di controllo di Europol e a tali fini è stato istituito un modello specifico di cooperazione con le autorità di controllo nazionali mediante un consiglio di cooperazione con funzione consultiva. Per migliorare l'efficacia del controllo e dell'applicazione delle norme sostanziali in materia di protezione dei dati, è opportuno introdurre nell'Unione un singolo modello coerente di controllo coordinato. Pertanto la Commissione dovrebbe, se del caso, presentare proposte legislative volte a modificare gli atti giuridici dell'Unione che prevedono un modello di controllo coordinato, onde allinearli al modello di controllo coordinato del presente regolamento. Il comitato europeo per la protezione dei dati dovrebbe costituire un forum unico per garantire un controllo coordinato efficace in tutti i settori.

(79) Ciascun interessato dovrebbe avere il diritto di proporre reclamo al Garante europeo della protezione dei dati e il diritto a un ricorso giurisdizionale effettivo dinanzi alla Corte di giustizia, in conformità dei trattati, qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento o se il Garante europeo della protezione dei dati non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato. Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico. È opportuno che il Garante europeo della protezione dei dati informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole. Se il caso richiede un ulteriore coordinamento con un'autorità di controllo nazionale, l'interessato dovrebbe ricevere informazioni interlocutorie. Per agevolare la proposizione di reclami, il Garante europeo della protezione dei dati 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.

(80) Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento dovrebbe avere il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento, alle condizioni stabilite nei trattati.

(81) Al fine di rafforzare la funzione di controllo del Garante europeo della protezione dei dati e l'applicazione efficace del presente regolamento, il Garante europeo della protezione dei dati dovrebbe, come sanzione di ultima istanza, poter imporre sanzioni amministrative pecuniarie. Tali sanzioni dovrebbero mirare a sanzionare l'istituzione o l'organo dell'Unione — piuttosto che la persona fisica — per la mancata conformità al presente regolamento, scoraggiarne future violazioni e promuovere una cultura di protezione dei dati personali all'interno delle istituzioni e degli organi dell'Unione. Il presente regolamento dovrebbe specificare le violazioni soggette a sanzione amministrativa pecuniaria, indicare i limiti massimi e i criteri per prevedere le sanzioni associate. Il Garante europeo della protezione dei dati dovrebbe stabilire l'ammontare della sanzione pecuniaria in ogni singolo caso, tenuto conto di tutte le circostanze pertinenti della situazione specifica, della natura, gravità e durata dell'infrazione, delle relative conseguenze e delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione. Quando impone una sanzione amministrativa pecuniaria a un'istituzione o un organo dell'Unione, il Garante europeo della protezione dei dati dovrebbe tenere conto della proporzionalità dell'importo della sanzione. La procedura amministrativa per l'imposizione di sanzioni pecuniarie a istituzioni e organi dell'Unione dovrebbe rispettare i principi generali del diritto dell'Unione, come interpretato dalla Corte di giustizia.

(82) Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento, dovrebbe avere il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto dell'Unione o di uno Stato membro, con obiettivi statutari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto al

([1]) Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

Garante europeo della protezione dei dati. Tale organismo, organizzazione o associazione dovrebbe essere in grado di esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o di esercitare il diritto a ottenere il risarcimento del danno per conto degli interessati.

(83) Il funzionario o altro agente dell'Unione che non assolva agli obblighi previsti dal presente regolamento dovrebbe essere passibile di provvedimenti disciplinari o di altro genere, secondo le norme e le procedure previste dallo statuto dei funzionari dell'Unione europea e dal regime applicabile agli altri agenti dell'Unione, stabilite nel regolamento (CEE, Euratom, CECA) n. 259/68 del Consiglio ([1]) («statuto»).

(84) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([2]). È opportuno applicare la procedura d'esame per l'adozione di clausole contrattuali tipo tra i titolari del trattamento e i responsabili del trattamento e tra responsabili del trattamento, per l'adozione di un elenco di trattamenti che richiede la consultazione preventiva del Garante europeo della protezione dei dati personali da parte dei titolari del trattamento che effettuano un trattamento di dati personali necessario all'esecuzione di un compito di interesse pubblico e per l'adozione di clausole contrattuali tipo che prevedano garanzie adeguate per i trasferimenti internazionali.

(85) È opportuno proteggere le informazioni riservate raccolte dalle autorità statistiche dell'Unione e nazionali per la produzione di statistiche ufficiali europee e nazionali. Le statistiche europee dovrebbero essere sviluppate, prodotte e diffuse conformemente ai principi statistici di cui all'articolo 338, paragrafo 2, TFUE. Il regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio ([3]) fornisce ulteriori specificazioni in merito al segreto statistico per quanto riguarda le statistiche europee.

(86) Il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE del Parlamento europeo, del Consiglio e della Commissione ([4]) dovrebbero essere abrogati. I riferimenti al regolamento e alla direttiva abrogati dovrebbero intendersi fatti al presente regolamento.

(87) Al fine di garantire la piena indipendenza dei membri dell'autorità di controllo indipendente, il presente regolamento non dovrebbe incidere sui mandati dell'attuale Garante europeo della protezione dei dati e dell'attuale Garante aggiunto. L'attuale Garante aggiunto dovrebbe rimanere in carica fino alla fine del mandato, a meno che non si verifichi una delle condizioni per la cessazione anticipata del mandato del Garante europeo della protezione dei dati stabilite dal presente regolamento. Le disposizioni pertinenti del presente regolamento dovrebbero applicarsi al Garante aggiunto fino alla fine del suo mandato.

(88) Conformemente al principio di proporzionalità, è necessario e appropriato, al fine del conseguimento dell'obiettivo fondamentale di garantire un livello equivalente di tutela delle persone fisiche in relazione al trattamento dei dati personali e la libera circolazione dei dati personali nell'Unione, stabilire norme relative al trattamento dei dati personali nelle istituzioni e negli organi dell'Unione. Il presente regolamento si limita a quanto è necessario per conseguire gli obiettivi perseguiti, in ottemperanza all'articolo 5, paragrafo 4, TUE.

(89) Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e ha espresso il proprio parere in data 15 marzo 2017 ([5]),

---

([1]) GU L 56 del 4.3.1968, pag. 1.

([2]) 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).

([3]) Regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio, dell'11 marzo 2009, relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del Parlamento europeo e del Consiglio, relativo alla trasmissione all'Istituto statistico delle Comunità europee di dati statistici protetti dal segreto, il regolamento (CE) n. 322/97 del Consiglio, relativo alle statistiche comunitarie, e la decisione 89/382/CEE, Euratom del Consiglio, che istituisce un comitato del programma statistico delle Comunità europee (GU L 87 del 31.3.2009, pag. 164).

([4]) Decisione n. 1247/2002/CE del Parlamento europeo, del Consiglio e della Commissione, del 1º luglio 2002, relativa allo statuto e alle condizioni generali d'esercizio delle funzioni di Garante europeo della protezione dei dati (GU L 183 del 12.7.2002, pag. 1).

([5]) GU C 164 del 24.5.2017, pag. 2.

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organi dell'Unione, nonché norme relative alla libera circolazione dei dati personali tra tali istituzioni e organi o verso altri destinatari stabiliti nell'Unione.

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

3. Il Garante europeo della protezione dei dati sorveglia l'applicazione delle disposizioni del presente regolamento a tutti i trattamenti effettuati da un'istituzione o un organo dell'Unione.

Articolo 2

Ambito di applicazione

1. Il presente regolamento si applica al trattamento di dati personali da parte di tutte le istituzioni e di tutti gli organi dell'Unione.

2. Solo l'articolo 3 e il capo IX del presente regolamento si applicano al trattamento dei dati personali operativi da parte degli organi e degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE.

3. Il presente regolamento non si applica al trattamento dei dati personali operativi da parte di Europol e della Procura europea, finché il regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio ([1]) e il regolamento (UE) 2017/1939 del Consiglio ([2]) non saranno sono adattati conformemente all'articolo 98 del presente regolamento.

4. Il presente regolamento non si applica al trattamento dei dati personali da parte delle missioni di cui all'articolo 42, paragrafo 1, e agli articoli 43 e 44 TUE.

5. 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.

Articolo 3

Definizioni

Ai fini del presente regolamento si applicano le seguenti definizioni:

1) «dati personali»: qualsiasi informazione concernente una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «dati personali operativi»: tutti i dati personali trattati da organi o organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE per conseguire gli obiettivi ed eseguire i compiti stabiliti negli atti giuridici che li istituiscono;

([1]) Regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI (GU L 135 del 24.5.2016, pag. 53).

([2]) Regolamento (UE) 2017/1939 del Consiglio, del 12 ottobre 2017, relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea («EPPO») (GU L 283 del 31.10.2017, pag. 1).

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 conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

4) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

5) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

6) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

7) «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;

8) «titolare del trattamento»: l'istituzione o l'organo dell'Unione, la direzione generale o qualunque altra entità organizzativa che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati da un atto specifico dell'Unione, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione;

9) «titolari del trattamento diversi dalle istituzioni e dagli organi dell'Unione»: i titolari del trattamento ai sensi dell'articolo 4, punto 7), del regolamento (UE) 2016/679 e i titolari del trattamento ai sensi dell'articolo 3, punto 8), della direttiva (UE) 2016/680;

10) «istituzioni e organi dell'Unione»: le istituzioni, gli organi e gli organismi dell'Unione istituiti dal TUE, dal TFUE o dal trattato Euratom oppure sulla base di tali trattati;

11) «autorità competente»: qualsiasi autorità pubblica di uno Stato membro competente in materia di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

12) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

13) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

14) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

15) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

16) «violazione dei dati personali»: violazione di sicurezza che comporta in modo accidentale o illecito la distruzione, la perdita, la modifica, la comunicazione non autorizzata dei dati personali trasmessi, memorizzati o comunque trattati, o l'accesso agli stessi;

17) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano, in particolare, dati dall'analisi di un campione biologico della persona fisica in questione;

18) «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;

19) «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;

20) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([1]);

21) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più paesi;

22) «autorità di controllo nazionale»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del regolamento (UE) 2016/679 o ai sensi dell'articolo 41 della direttiva (UE) 2016/680;

23) «utente»: qualsiasi persona fisica che si serve di una rete o di un'apparecchiatura terminale che funziona sotto il controllo di un'istituzione o di un organo dell'Unione;

24) «elenco»: elenco di utenti accessibile al pubblico o elenco interno di utenti disponibile in un'istituzione od organo dell'Unione o condiviso tra istituzioni e organi dell'Unione, in formato cartaceo o elettronico.

25) «rete di comunicazione elettronica»: un sistema di trasmissione basato o meno su un'infrastruttura permanente o una capacità di amministrazione centralizzata e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri fisse (a commutazione di circuito e a commutazione di pacchetto, compreso Internet) e mobili, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti utilizzate per le trasmissioni radio e televisive nonché le reti televisive via cavo, indipendentemente dal tipo di informazione trasmesso;

26) «apparecchiature terminali»: le apparecchiature terminali quali definite all'articolo 1, punto 1), della direttiva 2008/63/CE della Commissione ([2]).

CAPO II

PRINCIPI GENERALI

Articolo 4

Principi applicabili al trattamento di dati personali

1. I dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 13, 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 adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati personali inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

([1]) Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

([2]) Direttiva 2008/63/CE della Commissione, del 20 giugno 2008, relativa alla concorrenza sui mercati delle apparecchiature terminali di telecomunicazioni (GU L 162 del 21.6.2008, pag. 20).

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 13, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

Articolo 5

Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:

a) il trattamento è necessario per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri di cui sono investiti l'istituzione o l'organo dell'Unione;

b) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

c) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

d) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

e) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica.

2. La base su cui si fonda il trattamento di cui al paragrafo 1, lettere a) e b), è stabilita dal diritto dell'Unione.

Articolo 6

Trattamento per un'altra finalità compatibile

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su disposizioni del diritto dell'Unione che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 25, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 10, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 11;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Articolo 7

Condizioni per il consenso

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

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Articolo 8

Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

1. Qualora si applichi l'articolo 5, paragrafo 1, lettera d), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 13 anni. Ove il minore abbia un'età inferiore ai 13 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

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

3. Il paragrafo 1 non pregiudica le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore.

Articolo 9

Trasmissione di dati personali a destinatari stabiliti nell'Unione diversi dalle istituzioni e dagli organi dell'Unione

1. Fatti salvi gli articoli da 4 a 6 e l'articolo 10, i dati personali possono essere trasmessi a destinatari stabiliti nell'Unione diversi dalle istituzioni e dagli organi dell'Unione solo se:

a) il destinatario dimostra che i dati sono necessari per l'esecuzione di un compito svolto nell'interesse pubblico o nell'esercizio di pubblici poteri di cui è investito; oppure

b) il destinatario dimostra che la trasmissione dei dati è necessaria al fine specifico di servire l'interesse pubblico e il responsabile del trattamento, qualora sussistano motivi per presumere che gli interessi legittimi dell'interessato possano subire pregiudizio, dimostra che è proporzionato trasmettere i dati personali per detto fine specifico dopo aver chiaramente soppesato i vari interessi in conflitto.

2. Ove dia origine alla trasmissione a norma del presente articolo il titolare del trattamento dimostra che la trasmissione dei dati personali è necessaria e proporzionata alle finalità cui è destinata, applicando i criteri di cui al paragrafo 1, lettera a) o b).

3. Le istituzioni e gli organi dell'Unione conciliano il diritto alla protezione dei dati personali con il diritto di accesso ai documenti in conformità del diritto dell'Unione.

Articolo 10

Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

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

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1;

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

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

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da un organismo senza scopo di lucro che costituisca un'entità integrata in un'istituzione o in un organo dell'Unione e 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 l'organismo a motivo delle sue finalità e che i dati non siano comunicati a terzi senza il consenso dell'interessato;

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

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta la Corte di giustizia eserciti la sua funzione giurisdizionale;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; o

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici sulla base del diritto dell'Unione, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

Articolo 11

Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento di dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 5, paragrafo 1, avviene solo sotto il controllo dell'autorità ufficiale o se il trattamento è autorizzato da disposizioni del diritto dell'Unione che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

Articolo 12

Trattamento che non richiede l'identificazione

1. Se le finalità per cui un titolare del trattamento tratta i dati personali non richiedono o non richiedono più l'identificazione dell'interessato, il titolare del trattamento non è obbligato a conservare, acquisire o trattare ulteriori informazioni per identificare l'interessato al solo fine di rispettare il presente regolamento.

2. Qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 17 a 22 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.

Articolo 13

Garanzie relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici

Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

CAPO III

DIRITTI DELL'INTERESSATO

SEZIONE 1

Trasparenza e modalità

Articolo 14

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

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 15 e 16 e le comunicazioni di cui agli articoli da 17 a 24 e all'articolo 35 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 17 a 24. Nei casi di cui all'articolo 12, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato di esercitare i suoi diritti ai sensi degli articoli da 17 a 24, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 17 a 24 senza indebito ritardo e, comunque, entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo al Garante europeo della protezione dei dati e di proporre ricorso giurisdizionale.

5. Le informazioni fornite ai sensi degli articoli 15 e 16 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 17 a 24 e dell'articolo 35 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può rifiutare di soddisfare la richiesta. Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6. Fatto salvo l'articolo 12, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 17 a 23, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

7. Le informazioni da fornire agli interessati a norma degli articoli 15 e 16 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

8. Se la Commissione adotta atti delegati conformemente all'articolo 12, paragrafo 8, del regolamento (UE) 2016/679 che stabiliscono le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate, le istituzioni e gli organi dell'Unione forniscono, se del caso, le informazioni di cui agli articoli 15 e 16 del presente regolamento in combinazione con le icone standardizzate.

SEZIONE 2

Informazioni e accesso ai dati personali

Articolo 15

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

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

a) l'identità e i dati di contatto del titolare del trattamento;

b) i dati di contatto del responsabile della protezione dei dati;

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

d) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

e) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 48, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:

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

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o, ove applicabile, del diritto di opporsi al trattamento o del diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'articolo 5, paragrafo 1, lettera d), oppure sull'articolo 10, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo al Garante europeo della protezione dei dati;

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

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 24, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

4. I paragrafi 1, 2 e 3 non si applicano se e nella misura in cui l'interessato dispone già delle informazioni.

Articolo 16

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

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

a) l'identità e i dati di contatto del titolare del trattamento;

b) i dati di contatto del responsabile della protezione dei dati;

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

d) le categorie di dati personali in questione;

e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 48, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato:

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

b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o, ove applicabile, del diritto di opporsi al trattamento o del diritto alla portabilità dei dati;

c) qualora il trattamento sia basato sull'articolo 5, paragrafo 1, lettera d), oppure sull'articolo 10, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo al Garante europeo della protezione dei dati;

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

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 24, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2:

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

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

c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2.

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

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento;

c) l'ottenimento o la comunicazione sono espressamente previsti da disposizioni del diritto dell'Unione che prevedono misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure

d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione, compreso un obbligo di segretezza previsto per legge.

6. Nei casi di cui al paragrafo 5, lettera b), il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e gli interessi legittimi dell'interessato, anche rendendo pubbliche le informazioni.

Articolo 17

Diritto di accesso dell'interessato

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;

f) il diritto di proporre reclamo al Garante europeo della protezione dei dati;

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 24, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 48 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui.

SEZIONE 3

Rettifica e cancellazione

Articolo 18

Diritto di rettifica

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza indebito ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 19

Diritto alla cancellazione («diritto all'oblio»)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza indebito ritardo e il titolare del trattamento ha l'obbligo di cancellare senza indebito ritardo i dati personali, se sussiste uno dei motivi seguenti:

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

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 5, paragrafo 1, lettera d), o all'articolo 10, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 23, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo legale cui è soggetto il titolare del trattamento;

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

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento, o i titolari del trattamento diversi dalle istituzioni e dagli organi dell'Unione, che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 10, paragrafo 2, lettere h) e i), e dell'articolo 10, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; oppure

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

Articolo 20

Diritto di limitazione di trattamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza, inclusa la completezza, di tali dati personali;

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

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 23, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal titolare del trattamento prima che detta limitazione sia revocata.

4. Negli archivi automatizzati la limitazione del trattamento è assicurata, in linea di massima, mediante dispositivi tecnici. Il sistema deve indicare che i dati personali sono stati limitati in modo da rendere evidente che non possono essere utilizzati.

Articolo 21

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 18, dell'articolo 19, paragrafo 1, e dell'articolo 20, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Articolo 22

Diritto alla portabilità dei dati

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 5, paragrafo 1, lettera d), o dell'articolo 10, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 5, paragrafo 1, lettera c); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento a un altro o a titolari del trattamento diversi dalle istituzioni e dagli organi dell'Unione, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 19. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

SEZIONE 4

Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

Articolo 23

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 5, paragrafo 1, lettera a), compresa la profilazione sulla base di tale disposizione. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Il diritto di cui al paragrafo 1 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.

3. Fatti salvi gli articoli 36 e 37, nel contesto dell'utilizzo di servizi della società dell'informazione l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

4. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Articolo 24

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

2. Il paragrafo 1 non si applica nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento;

b) sia autorizzata dal diritto dell'Unione, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e degli interessi legittimi dell'interessato; oppure

c) si basi sul consenso esplicito dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e gli interessi legittimi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.

4. Le decisioni di cui al paragrafo 2 del presente articolo non si basano sulle categorie particolari di dati personali di cui all'articolo 10, paragrafo 1, a meno che non sia d'applicazione l'articolo 10, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e degli interessi legittimi dell'interessato.

SEZIONE 5

Limitazioni

Articolo 25

Limitazioni

1. Gli atti giuridici adottati sulla base dei trattati oppure, per le questioni relative al funzionamento delle istituzioni e degli organi dell'Unione, le norme interne stabilite da questi ultimi possono limitare l'applicazione degli articoli da 14 a 22 e degli articoli 35 e 36, nonché dell'articolo 4 nella misura in cui le sue disposizioni corrispondano ai diritti e agli obblighi di cui agli articoli da 14 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale, la sicurezza pubblica o la difesa degli Stati membri;

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 gli obiettivi della politica estera e di sicurezza comune dell'Unione o 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;

d) la sicurezza interna delle istituzioni e degli organi dell'Unione, inclusa quella delle loro reti di comunicazione elettronica;

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

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

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

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

i) l'esecuzione delle azioni civili.

2. In particolare, gli atti giuridici o le norme interne di cui al paragrafo 1 contengono disposizioni specifiche riguardanti, se del caso:

a) le finalità del trattamento o delle categorie di trattamento;

b) le categorie di dati personali;

c) la portata delle limitazioni introdotte;

d) le garanzie per prevenire abusi o l'accesso o il trasferimento illeciti;

e) l'indicazione precisa del titolare del trattamento o delle categorie di titolari;

f) i periodi di conservazione e le garanzie applicabili tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento o delle categorie di trattamento; e

g) i rischi per i diritti e le libertà degli interessati.

3. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione, che può comprendere norme interne adottate dalle istituzioni e dagli organi dell'Unione relative a questioni connesse al loro funzionamento, può prevedere deroghe ai diritti di cui agli articoli 17, 18, 20 e 23, fatte salve le condizioni e le garanzie di cui all'articolo 13, 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. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione, che può comprendere norme interne adottate dalle istituzioni e dagli organi dell'Unione relative a questioni connesse al loro funzionamento, può prevedere deroghe ai diritti di cui agli articoli 17, 18, 20, 21, 22 e 23, fatte salve le condizioni e le garanzie di cui all'articolo 13, 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.

5. Le norme interne di cui ai paragrafi 1, 3 e 4 sono atti di applicazione generale chiari e precisi intesi a produrre effetti giuridici nei confronti degli interessati, adottati al più alto livello di gestione delle istituzioni e degli organi dell'Unione e destinati a essere pubblicati nella *Gazzetta ufficiale dell'Unione europea*.

6. Qualora si applichi una delle limitazioni di cui al paragrafo 1, l'interessato è informato, conformemente al diritto dell'Unione, dei principali motivi della limitazione e del suo diritto di proporre reclamo al Garante europeo della protezione dei dati.

7. Qualora si applichino le limitazioni previste al paragrafo 1 per negare all'interessato l'accesso ai dati che lo riguardano, il Garante europeo della protezione dei dati, nell'esaminare il reclamo, gli comunica solo se i dati sono stati trattati correttamente ovvero, in caso contrario, se sono state apportate tutte le rettifiche necessarie.

8. La comunicazione delle informazioni di cui ai paragrafi 6 e 7 del presente articolo e all'articolo 45, paragrafo 2, può essere rinviata, omessa o negata qualora annulli l'effetto della limitazione imposta in forza del paragrafo 1 del presente articolo.

CAPO IV

TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO

SEZIONE 1

Obblighi generali

Articolo 26

Responsabilità del titolare del trattamento

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

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3. L'adesione a meccanismi di certificazione approvati di cui all'articolo 42 del regolamento (UE) 2016/679 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Articolo 27

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 del regolamento (UE) 2016/679 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

Articolo 28

Contitolari del trattamento

1. Allorché due o più titolari del trattamento o uno o più titolari del trattamento insieme a uno o più titolari del trattamento diversi dalle istituzioni e dagli organi dell'Unione determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi di protezione dei dati, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 15 e 16, a meno che e nella misura in cui le rispettive responsabilità dei contitolari siano determinate dal diritto dell'Unione o dello Stato membro cui i contitolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Articolo 29

Responsabile del trattamento

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

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo 33;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

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

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 33 a 41, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

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

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

5. Quando un responsabile del trattamento non è un'istituzione o un organo dell'Unione, la sua adesione a un codice di condotta approvato di cui all'articolo 40, paragrafo 5, del regolamento (UE) 2016/679 o a un meccanismo di certificazione approvato di cui all'articolo 42 dello stesso regolamento può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo l'eventuale contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al responsabile del trattamento diverso da un'istituzione o un organo dell'Unione ai sensi dell'articolo 42 del regolamento (UE) 2016/679.

7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 96, paragrafo 2.

8. Il Garante europeo della protezione dei dati può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4.

9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico.

10. Fatti salvi gli articoli 65 e 66, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

Articolo 30

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

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

Articolo 31

Registri delle attività di trattamento

1. Ogni titolare del trattamento tiene un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento, del responsabile della protezione dei dati e, ove applicabile, del responsabile del trattamento e del contitolare del trattamento;

b) le finalità del trattamento;

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

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Stati membri, paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;

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

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 33.

2. Ogni responsabile del trattamento tiene un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento e del responsabile della protezione dei dati;

b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 33.

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

4. Su richiesta, le istituzioni e gli organi dell'Unione mettono il registro a disposizione del Garante europeo della protezione dei dati.

5. A meno che non sia opportuno tener conto delle dimensioni dell'istituzione o dell'organo dell'Unione, le istituzioni e gli organi dell'Unione conservano i loro registri delle attività di trattamento in un registro centrale che rendono accessibile al pubblico.

Articolo 32

Cooperazione con il Garante europeo della protezione dei dati;

Le istituzioni e gli organi dell'Unione collaborano, su richiesta, con il Garante europeo della protezione dei dati nello svolgimento dei suoi compiti.

SEZIONE 2

Sicurezza dei dati personali

Articolo 33

Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

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

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

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare, in modo accidentale o illegale, dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata di dati personali trasmessi, conservati o comunque trattati o dall'accesso agli stessi.

3. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione.

4. L'adesione a un meccanismo di certificazione approvato ai sensi dell'articolo 42 del regolamento (UE) 2016/679 può essere utilizzata come elemento per dimostrare il rispetto dei requisiti di cui al paragrafo 1 del presente articolo.

Articolo 34

Notifica di una violazione dei dati personali al Garante europeo della protezione dei dati

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante europeo della protezione dei dati, senza indebito ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica al Garante europeo della protezione dei dati non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. Il responsabile del trattamento informa il titolare del trattamento senza indebito ritardo dopo essere venuto a conoscenza della violazione.

3. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati;

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

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

4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5. Il titolare del trattamento comunica al responsabile della protezione dei dati la violazione dei dati personali.

6. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente al Garante europeo della protezione dei dati di verificare il rispetto del presente articolo.

Articolo 35

Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza indebito ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 34, paragrafo 3, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

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

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante europeo della protezione dei dati può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

SEZIONE 3

Riservatezza delle comunicazioni elettroniche

Articolo 36

Riservatezza delle comunicazioni elettroniche

Le istituzioni e gli organi dell'Unione garantiscono la riservatezza delle comunicazioni elettroniche, in particolare proteggendo le proprie reti di comunicazione elettronica.

Articolo 37

Tutela delle informazioni trasmesse relative all'apparecchiatura terminale degli utenti, nonché conservate, elaborate e raccolte dalla stessa

Le istituzioni e gli organi dell'Unione tutelano le informazioni trasmesse all'apparecchiatura terminale degli utenti, conservate nell'apparecchiatura terminale degli utenti, relative all'apparecchiatura terminale degli utenti, elaborate dall'apparecchiatura terminale degli utenti e raccolte dall'apparecchiatura terminale degli utenti che accede ai loro siti web e alle applicazioni per dispositivi mobili a disposizione del pubblico, in ottemperanza all'articolo 5, paragrafo 3, della direttiva 2002/58/CE.

Articolo 38

Elenchi di utenti

1. I dati personali contenuti in elenchi di utenti e l'accesso a detti elenchi sono limitati allo stretto necessario ai fini specifici degli elenchi.

2. Le istituzioni e gli organi dell'Unione prendono le misure necessarie per impedire che i dati personali contenuti in tali elenchi siano utilizzati a fini di diffusione commerciale diretta, indipendentemente dal fatto che gli elenchi siano o meno accessibili al pubblico.

SEZIONE 4

Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Articolo 39

Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati.

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

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 10, o di dati relativi a condanne penali e a reati di cui all'articolo 11; oppure

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

4. Il Garante europeo della protezione dei dati 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.

5. Il Garante europeo della protezione dei dati 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.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5 del presente articolo, il Garante europeo della protezione dei dati chiede che il comitato europeo per la protezione dei dati istituito dall'articolo 68 del regolamento (UE) 2016/679 esamini detti elenchi conformemente all'articolo 70, paragrafo 1, lettera e), dello stesso regolamento ove tali elenchi si riferiscano a trattamenti da parte di un titolare del trattamento che agisce congiuntamente a uno o più titolari del trattamento diversi dalle istituzioni e dagli organi dell'Unione.

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità 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; e

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.

8. Nel valutare l'impatto del trattamento effettuato dai relativi responsabili diversi dalle istituzioni e dagli organi dell'Unione è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40 del regolamento (UE) 2016/679, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 5, paragrafo 1, lettera a) o b), trovi una base giuridica in un atto giuridico adottato sulla base dei trattati, 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 precedente all'adozione di tale atto giuridico, i paragrafi da 1 a 6 del presente articolo non si applicano, salvo se tale atto giuridico stabilisce altrimenti.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Articolo 40

Consultazione preventiva

1. Prima di procedere al trattamento, il titolare del trattamento consulta il Garante europeo della protezione dei dati se dalla valutazione d'impatto sulla protezione dei dati a norma dell'articolo 39 risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il titolare del trattamento è del parere che il rischio non possa essere ragionevolmente attenuato in considerazione delle tecnologie disponibili e dei costi di attuazione. Il titolare del trattamento chiede il parere del responsabile della protezione dei dati sulla necessità di una consultazione preventiva.

2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, il Garante europeo della protezione dei dati fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. Il Garante europeo della protezione dei dati informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte del Garante europeo della protezione dei dati delle informazioni richieste ai fini della consultazione.

3. Al momento di consultare il Garante europeo della protezione dei dati ai sensi del paragrafo 1, il titolare del trattamento comunica al Garante europeo della protezione dei dati:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;

b) le finalità e i mezzi del trattamento previsto;

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

d) i dati di contatto del responsabile della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 39; e

f) ogni altra informazione richiesta dal Garante europeo della protezione dei dati.

4. La Commissione può definire, mediante un atto di esecuzione, un elenco dei casi in cui i titolari del trattamento consultano il Garante europeo della protezione dei dati, e ne ottengono l'autorizzazione preliminare, in relazione al trattamento necessario all'esecuzione, da parte del titolare del trattamento di dati personali, di un compito di interesse pubblico, tra cui il trattamento di tali dati in relazione alla protezione sociale e alla sanità pubblica.

SEZIONE 5

Informazioni e consultazione legislativa

Articolo 41

Informazione e consultazione

1. Le istituzioni e gli organi dell'Unione informano il Garante europeo della protezione dei dati al momento di elaborare provvedimenti amministrativi e norme interne in tema di trattamento di dati personali da parte di un'istituzione o un organo dell'Unione, singolarmente o congiuntamente con altri.

2. Le istituzioni e gli organi dell'Unione consultano il Garante europeo della protezione dei dati al momento di elaborare le norme interne di cui all'articolo 25.

Articolo 42

Consultazione legislativa

1. Dopo l'adozione di proposte di atti legislativi e di raccomandazioni o proposte al Consiglio a norma dell'articolo 218 TFUE o durante la stesura di atti delegati o di esecuzione, qualora essi incidano sulla tutela dei diritti e delle libertà delle persone in relazione al trattamento dei dati personali, la Commissione consulta il Garante europeo della protezione dei dati.

2. Se un atto di cui al paragrafo 1 è di particolare rilevanza per la tutela dei diritti e delle libertà fondamentali delle persone in relazione al trattamento di dati personali, la Commissione può consultare anche il comitato europeo per la protezione dei dati. In tali casi, il Garante europeo per la protezione dei dati e il comitato europeo per la protezione dei dati coordinano le proprie attività al fine di emettere un parere congiunto.

3. La consulenza di cui ai paragrafi 1 e 2 è fornita per iscritto entro un termine di otto settimane dal ricevimento della richiesta di consultazione di cui ai paragrafi 1 e 2. In caso di urgenza, o se altrimenti opportuno, la Commissione può abbreviare il termine.

4. Il presente articolo non si applica quando il regolamento (UE) 2016/679 fa obbligo alla Commissione di consultare il comitato europeo per la protezione dei dati.

SEZIONE 6

Responsabile della protezione dei dati

Articolo 43

Designazione del responsabile della protezione dei dati

1. Ogni istituzione od organo dell'Unione designa un responsabile della protezione dei dati.

2. Un unico responsabile della protezione dei dati può essere designato per più istituzioni e organi dell'Unione, tenuto conto della loro struttura organizzativa e dimensione.

3. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 45.

4. Il responsabile della protezione dei dati è un membro del personale dell'istituzione o dell'organo dell'Unione. Tenuto conto della loro dimensione e se l'opzione di cui al paragrafo 2 non è esercitata, le istituzioni e gli organi dell'Unione possono designare un responsabile della protezione dei dati che assolve i suoi compiti in base a un contratto di servizi.

5. Le istituzioni e gli organi dell'Unione pubblicano i dati di contatto del responsabile della protezione dei dati e li comunicano al Garante europeo della protezione dei dati.

Articolo 44

Posizione del responsabile della protezione dei dati

1. Le istituzioni e gli organi dell'Unione si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Le istituzioni e gli organi dell'Unione sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 45 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

3. Le istituzioni e gli organi dell'Unione si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

4. Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

5. Il responsabile della protezione dei dati e il suo personale sono tenuti al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

7. Il responsabile della protezione dei dati può essere consultato dal titolare del trattamento e dal responsabile del trattamento, dal comitato del personale interessato e da qualsiasi persona su qualsiasi aspetto riguardante l'interpretazione o l'applicazione del presente regolamento, senza seguire la via gerarchica. Nessuno deve subire pregiudizio per una questione portata all'attenzione del responsabile della protezione dei dati competente e riguardante un'asserita violazione delle disposizioni del presente regolamento.

8. Il responsabile della protezione dei dati è designato per un periodo da tre a cinque anni e il suo mandato è rinnovabile. Il responsabile della protezione dei dati può essere destituito dalle sue funzioni dall'istituzione o dall'organo dell'Unione che lo ha designato, se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni, solo con il consenso del Garante europeo della protezione dei dati.

9. La designazione del responsabile della protezione dei dati è comunicata al Garante europeo della protezione dei dati dall'istituzione o dall'organo dell'Unione che lo ha designato.

Articolo 45

Compiti del responsabile della protezione dei dati

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

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione relative alla protezione dei dati;

b) assicurare in modo indipendente l'applicazione interna del presente regolamento; sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione applicabili relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) garantire che gli interessati siano informati dei propri diritti e obblighi ai sensi del presente regolamento;

d) fornire, se richiesto, un parere in merito alla necessità di notificare o comunicare una violazione dei dati personali a norma degli articoli 34 e 35;

e) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento a norma dell'articolo 39 e consultare il Garante europeo della protezione dei dati in caso di dubbi sulla necessità di una valutazione d'impatto sulla protezione dei dati;

f) fornire, se richiesto, un parere in merito alla necessità di una consultazione preventiva del Garante europeo della protezione dei dati a norma dell'articolo 40; consultare il Garante europeo della protezione dei dati in caso di dubbi sulla necessità di una consultazione preventiva;

g) rispondere alle richieste del Garante europeo della protezione dei dati; nell'ambito delle sue competenze, cooperare e consultarsi con il Garante europeo della protezione dei dati su richiesta di quest'ultimo o di propria iniziativa;

h) garantire che i trattamenti non arrechino pregiudizio ai diritti e alle libertà degli interessati.

2. Il responsabile della protezione dei dati può formulare raccomandazioni al titolare del trattamento e al responsabile del trattamento per il miglioramento concreto della protezione dei dati e consigliare questi ultimi in merito all'applicazione delle disposizioni sulla protezione dei dati. Può inoltre, di propria iniziativa o a richiesta del titolare del trattamento o del responsabile del trattamento, del comitato del personale interessato o di qualsiasi persona, indagare sulle questioni e sui fatti direttamente collegati con l'esercizio delle sue funzioni di cui viene a conoscenza e riferire in merito alla persona che lo ha incaricato dell'indagine o al titolare o al responsabile del trattamento.

3. Altre norme di attuazione relative al responsabile della protezione dei dati sono adottate da ogni istituzione od organo dell'Unione. Tali norme di attuazione riguardano in particolare le funzioni, gli obblighi e le competenze del responsabile della protezione dei dati.

CAPO V

TRASFERIMENTI DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

Articolo 46

Principio generale per il trasferimento

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Articolo 47

Trasferimento sulla base di una decisione di adeguatezza

1. Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso, ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 o dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680, che il paese terzo, un territorio o uno o più settori specifici all'interno di tale paese terzo o l'organizzazione internazionale in questione assicurano un livello di protezione adeguato, e qualora i dati personali siano trasferiti esclusivamente per consentire lo svolgimento dei compiti che rientrano nelle competenze del titolare del trattamento.

2. Le istituzioni e gli organi dell'Unione informano la Commissione e il Garante europeo della protezione dei dati circa i casi in cui a loro parere un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo o un'organizzazione internazionale in questione non assicurano un livello di protezione adeguato ai sensi del paragrafo 1.

3. Le istituzioni e gli organi dell'Unione adottano le misure necessarie per conformarsi alle decisioni della Commissione che constatano, in applicazione dell'articolo 45, paragrafo 3 o 5, del regolamento (UE) 2016/679 o dell'articolo 36, paragrafo 3 o 5, della direttiva (UE) 2016/680, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo o un'organizzazione internazionale assicurano o non assicurano più un livello di protezione adeguato.

Articolo 48

Trasferimento soggetto a garanzie adeguate

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 o dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte del Garante europeo della protezione dei dati:

a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;

b) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 96, paragrafo 2;

c) le clausole tipo di protezione dei dati adottate dal Garante europeo della protezione dei dati e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 96, paragrafo 2;

d) qualora il responsabile del trattamento non sia un'istituzione o un organo dell'Unione, le norme vincolanti d'impresa, i codici di condotta o i meccanismi di certificazione ai sensi dell'articolo 46, paragrafo 2, lettere b), e) ed f), del regolamento (UE) 2016/679.

3. Fatta salva l'autorizzazione del Garante europeo della protezione dei dati, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1:

a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; oppure

b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

4. Le autorizzazioni rilasciate dal Garante europeo della protezione dei dati in base all'articolo 9, paragrafo 7, del regolamento (CE) 45/2001 restano valide fino a quando non sono modificate, sostituite o abrogate, se necessario, dal Garante europeo della protezione dei dati.

5. Le istituzioni e gli organi dell'Unione informano il Garante europeo della protezione dei dati in merito alle categorie di casi in cui è stato applicato il presente articolo.

Articolo 49

Trasferimento o comunicazione non autorizzati dal diritto dell'Unione

Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.

Articolo 50

Deroghe in specifiche situazioni

1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 o dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680, o di garanzie adeguate ai sensi dell'articolo 48 del presente regolamento, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

a) l'interessato ha esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;

b) il trasferimento è necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;

c) il trasferimento è necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;

d) il trasferimento è necessario per importanti motivi di interesse pubblico;

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

f) il trasferimento è necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; oppure

g) il trasferimento è effettuato a partire da un registro che, a norma del diritto dell'Unione, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un interesse legittimo, ma solo purché sussistano i requisiti per la consultazione previsti dal diritto dell'Unione.

2. Il paragrafo 1, lettere a), b) e c), non si applica alle attività svolte dalle istituzioni e dagli organi dell'Unione nell'esercizio dei pubblici poteri.

3. L'interesse pubblico di cui al paragrafo 1, lettera d), deve essere riconosciuto dal diritto dell'Unione.

4. 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, salvo se autorizzato dal diritto dell'Unione. Se il registro è destinato a essere consultato da persone aventi un interesse legittimo, il trasferimento è ammesso soltanto su richiesta di tali persone o qualora tali persone ne siano i destinatari.

5. In mancanza di una decisione di adeguatezza, il diritto dell'Unione 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.

6. Le istituzioni e gli organi dell'Unione informano il Garante europeo della protezione dei dati in merito alle categorie di casi in cui è stato applicato il presente articolo.

Articolo 51

Cooperazione internazionale per la protezione dei dati personali

In relazione ai paesi terzi e alle organizzazioni internazionali, il Garante europeo della protezione dei dati, in cooperazione con la Commissione e il comitato europeo per la protezione dei dati, adotta misure appropriate per:

a) sviluppare meccanismi di cooperazione internazionale per facilitare l'applicazione efficace della legislazione sulla protezione dei dati personali;

b) prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, in particolare mediante notificazione, deferimento dei reclami, assistenza alle indagini e scambio di informazioni, fatte salve garanzie adeguate per la protezione dei dati personali e gli altri diritti e libertà fondamentali;

c) coinvolgere le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali;

d) promuovere lo scambio e la documentazione delle legislazioni e prassi in materia di protezione dei dati personali, compresi i conflitti di giurisdizione con paesi terzi.

CAPO VI

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Articolo 52

Garante europeo della protezione dei dati

1. È istituito il Garante europeo della protezione dei dati.

2. Il Garante europeo della protezione dei dati ha il compito di garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, segnatamente del diritto alla protezione dei dati, in relazione al trattamento dei dati personali da parte delle istituzioni e degli organi dell'Unione.

3. Il Garante europeo della protezione dei dati ha il compito di sorvegliare e assicurare l'applicazione del presente regolamento e di qualunque altro atto dell'Unione relativo alla tutela dei diritti e delle libertà fondamentali delle persone fisiche in relazione al trattamento dei dati personali da parte di un'istituzione o di un organo dell'Unione, e di fornire alle istituzioni e agli organi dell'Unione nonché agli interessati pareri su tutte le questioni relative al trattamento dei dati personali. A tal fine esso assolve ai compiti previsti all'articolo 57 ed esercita i poteri attribuitigli dall'articolo 58.

4. Il regolamento (CE) n. 1049/2001 si applica ai documenti detenuti dal Garante europeo della protezione dei dati. Il Garante europeo della protezione dei dati adotta le modalità di applicazione del regolamento (CE) n. 1049/2001 per quanto riguarda tali documenti.

Articolo 53

Nomina del Garante europeo della protezione dei dati

1. Il Parlamento europeo e il Consiglio nominano di comune accordo il Garante europeo della protezione dei dati, per un periodo di cinque anni, in base a un elenco predisposto dalla Commissione dopo un invito pubblico a presentare candidature. Tale invito consente a tutte le parti interessate nell'insieme dell'Unione di presentare la propria candidatura. L'elenco di candidati elaborato dalla Commissione è pubblico e include almeno tre candidati. Sulla base dell'elenco elaborato dalla Commissione, la commissione competente del Parlamento europeo può decidere di organizzare un'audizione per poter esprimere una preferenza.

2. L'elenco di candidati di cui al paragrafo 1 deve essere composto da personalità che offrano ogni garanzia di indipendenza e che possiedano una conoscenza specialistica in materia di protezione dei dati nonché esperienza e competenze per l'esercizio delle funzioni di Garante europeo della protezione dei dati.

3. Il mandato del Garante europeo della protezione dei dati è rinnovabile una volta.

4. Le funzioni del Garante europeo della protezione dei dati cessano nei seguenti casi:

a) se il Garante europeo della protezione dei dati è sostituito;

b) se il Garante europeo della protezione dei dati si dimette;

c) se il Garante europeo della protezione dei dati è rimosso o collocato a riposo d'ufficio.

5. Il Garante europeo della protezione dei dati può essere rimosso o privato del diritto a pensione o di altri vantaggi sostitutivi dalla Corte di giustizia su richiesta del Parlamento europeo, del Consiglio o della Commissione qualora non sia più in possesso dei requisiti necessari all'esercizio delle sue funzioni o abbia commesso una colpa grave.

6. In caso di normale avvicendamento o di dimissioni volontarie, il Garante europeo della protezione dei dati resta comunque in carica fino all'atto della sua sostituzione.

7. Gli articoli da 11 a 14 e l'articolo 17 del protocollo sui privilegi e sulle immunità dell'Unione europea si applicano al Garante europeo della protezione dei dati.

Articolo 54

Statuto e condizioni generali di esercizio delle funzioni di Garante europeo della protezione dei dati, risorse umane e finanziarie

1. Il Garante europeo della protezione dei dati è equiparato a un giudice della Corte di giustizia per quanto riguarda la retribuzione, le indennità, il trattamento di quiescenza e ogni altro compenso sostitutivo.

2. L'autorità di bilancio provvede a che il Garante europeo della protezione dei dati disponga delle risorse umane e finanziarie necessarie per l'esercizio delle sue funzioni.

3. Il bilancio assegnato al Garante europeo della protezione dei dati figura su una linea specifica della sezione del bilancio generale dell'Unione relativa alle spese amministrative.

4. Il Garante europeo della protezione dei dati è assistito da un segretariato. I funzionari e gli altri agenti del segretariato sono nominati dal Garante europeo della protezione dei dati, che è il loro superiore gerarchico. Essi sono tenuti a conformarsi esclusivamente alle sue istruzioni. Il loro numero è stabilito ogni anno nell'ambito della procedura di bilancio. L'articolo 75, paragrafo 2, del regolamento (UE) 2016/679 si applica al personale del Garante europeo della protezione dei dati incaricato di svolgere i compiti attribuiti al comitato europeo per la protezione dei dati in virtù del diritto dell'Unione.

5. I funzionari e gli altri agenti del segretariato del Garante europeo della protezione dei dati sono soggetti alla normativa relativa ai funzionari e agli altri agenti dell'Unione.

6. La sede del Garante europeo della protezione dei dati è a Bruxelles.

Articolo 55

Indipendenza

1. Il Garante europeo della protezione dei dati agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente regolamento.

2. Nell'adempimento dei propri compiti e nell'esercizio dei propri poteri previsti dal presente regolamento, il Garante europeo della protezione dei dati non subisce pressioni esterne, né dirette né indirette, e non sollecita né accetta istruzioni da alcuno.

3. Per tutta la durata del mandato, il Garante europeo della protezione dei dati si astiene da qualunque azione incompatibile con i suoi doveri e non può esercitare alcuna altra attività professionale, remunerata o meno.

4. Al termine del mandato, il Garante europeo della protezione dei dati agisce con integrità e discrezione nell'accettazione di nomine e altri benefici.

Articolo 56

Segreto professionale

Durante e dopo il mandato, il Garante europeo della protezione dei dati ed il personale alle sue dipendenze sono tenuti al segreto professionale in merito alle informazioni riservate cui hanno avuto accesso durante l'esercizio delle loro funzioni.

Articolo 57

Compiti

1. Fatti salvi gli altri compiti indicati nel presente regolamento, il Garante europeo della protezione dei dati:

a) sorveglia e garantisce l'applicazione del presente regolamento da parte delle istituzioni e degli organi dell'Unione, fatta eccezione per il trattamento di dati personali da parte della Corte di giustizia nell'esercizio delle sue funzioni giurisdizionali;

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

c) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;

d) 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 nazionali;

e) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 67, 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;

f) 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;

g) fornisce, di propria iniziativa o su richiesta, consulenza alle istituzioni e agli organi dell'Unione in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche in relazione al trattamento dei dati personali;

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

i) adotta le clausole contrattuali tipo di cui all'articolo 29, paragrafo 8, e all'articolo 48, paragrafo 2, lettera c);

j) redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 39, paragrafo 4;

k) partecipa alle attività del comitato europeo per la protezione dei dati;

l) espleta i compiti di segreteria per il comitato europeo per la protezione dei dati, a norma dell'articolo 75 del regolamento (UE) 2016/679;

m) fornisce consulenza in merito al trattamento di cui all'articolo 40, paragrafo 2;

n) autorizza le clausole contrattuali e le altre disposizioni di cui all'articolo 48, paragrafo 3;

o) tiene registri interni delle violazioni del presente regolamento e delle misure adottate in conformità dell'articolo 58, paragrafo 2;

p) svolge qualsiasi altro compito legato alla protezione dei dati personali; e

q) adotta il proprio regolamento interno.

2. Il Garante europeo della protezione dei dati agevola la proposizione di reclami di cui al paragrafo 1, lettera e), tramite un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.

3. Il Garante europeo della protezione dei dati svolge i propri compiti senza spese per l'interessato.

4. Qualora le richieste siano manifestamente infondate o eccessive, in particolare per il carattere ripetitivo, il Garante europeo della protezione dei dati può rifiutarsi di soddisfare la richiesta. Incombe al Garante europeo della protezione dei dati dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Articolo 58

Poteri

1. Il Garante europeo della protezione dei dati dispone dei seguenti poteri di indagine:

a) ingiungere al titolare del trattamento e al responsabile del trattamento di fornirgli ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;

b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati;

c) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;

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

e) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione.

2. Il Garante europeo della protezione dei dati dispone dei seguenti poteri correttivi:

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

b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;

c) interpellare il titolare del trattamento o il responsabile del trattamento in questione e, se necessario, il Parlamento europeo, il Consiglio e la Commissione;

d) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti che gli derivano dal presente regolamento;

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

f) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;

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

h) ordinare la rettifica o la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 18, 19 e 20 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 19, paragrafo 2, e dell'articolo 21;

i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 66, in caso di inosservanza da parte di un'istituzione o un organo dell'Unione di una delle misure di cui al presente paragrafo, lettere da d) ad h) e lettera j), in funzione delle circostanze di ogni singolo caso;

j) ordinare la sospensione dei flussi di dati verso un destinatario in uno Stato membro, in un paese terzo o verso un'organizzazione internazionale.

3. Il Garante europeo della protezione dei dati dispone dei seguenti poteri autorizzativi e consultivi:

a) fornire consulenza agli interessati in merito all'esercizio dei loro diritti;

b) fornire consulenza al titolare del trattamento secondo la procedura di consultazione preventiva di cui all'articolo 40 e in conformità dell'articolo 41, paragrafo 2;

c) rilasciare, di propria iniziativa o su richiesta, pareri alle istituzioni e agli organi dell'Unione e al pubblico su questioni riguardanti la protezione dei dati personali;

d) adottare le clausole tipo di protezione dei dati di cui all'articolo 29, paragrafo 8, e all'articolo 48, paragrafo 2, lettera c);

e) autorizzare le clausole contrattuali di cui all'articolo 48, paragrafo 3, lettera a);

f) autorizzare gli accordi amministrativi di cui all'articolo 48, paragrafo 3, lettera b);

g) autorizzare trattamenti ai sensi degli atti di esecuzione adottati a norma dell'articolo 40, paragrafo 4.

4. Il Garante europeo della protezione dei dati ha il potere di adire la Corte di giustizia alle condizioni previste dai trattati e di intervenire nelle cause dinanzi alla Corte di giustizia.

5. L'esercizio da parte del Garante europeo della protezione dei dati dei poteri attribuitigli dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione.

Articolo 59

Obbligo dei titolari del trattamento e dei responsabili del trattamento di rispondere ai rilievi

Qualora il Garante europeo della protezione dei dati eserciti i poteri di cui all'articolo 58, paragrafo 2, lettere a), b) e c), il titolare del trattamento o il responsabile del trattamento gli comunica il proprio punto di vista entro un termine ragionevole fissato dal Garante europeo della protezione dei dati, tenendo conto delle circostanze di ciascun caso. Il parere comprende anche una descrizione degli eventuali provvedimenti presi a seguito delle osservazioni del Garante europeo della protezione dei dati.

Articolo 60

Rapporto sulle attività

1. Il Garante europeo della protezione dei dati presenta al Parlamento europeo, al Consiglio e alla Commissione un rapporto annuale sulla propria attività, rendendolo pubblico allo stesso tempo.

2. Il Garante europeo della protezione dei dati trasmette il rapporto sulle attività di cui al paragrafo 1 alle altre istituzioni e agli altri organi dell'Unione, che possono formulare osservazioni in vista dell'eventuale discussione dello stesso da parte del Parlamento europeo.

CAPO VII

COOPERAZIONE E COERENZA

Articolo 61

Cooperazione tra il Garante europeo della protezione dei dati e le autorità di controllo nazionali

Il Garante europeo per la protezione dei dati le autorità di controllo nazionali e l'autorità comune di controllo istituita dall'articolo 25 della decisione 2009/917/GAI del Consiglio ([1]) cooperano nella misura necessaria all'esecuzione delle rispettive funzioni, in particolare fornendosi reciprocamente informazioni pertinenti, chiedendosi reciprocamente di esercitare i rispettivi poteri e rispondendo alle reciproche richieste.

Articolo 62

Controllo coordinato del Garante europeo della protezione dei dati e delle autorità di controllo nazionali

1. Quando un atto dell'Unione rinvia al presente articolo, il Garante europeo della protezione dei dati e le autorità di controllo nazionali, agendo ciascuno nei limiti delle proprie competenze, cooperano attivamente nell'ambito delle proprie responsabilità per garantire un controllo efficace dei sistemi IT su larga scala e degli organi e degli organismi dell'Unione.

2. Essi, agendo ciascuno nei limiti delle proprie competenze e nell'ambito delle proprie responsabilità, si scambiano in funzione delle necessità informazioni pertinenti, si forniscono assistenza reciproca nello svolgimento di revisioni e ispezioni, esaminano difficoltà di interpretazione o applicazione del presente regolamento e di altri atti dell'Unione applicabili, studiano problemi inerenti all'esercizio di un controllo indipendente o all'esercizio dei diritti degli interessati, elaborano proposte armonizzate per soluzioni di eventuali problemi e promuovono la sensibilizzazione del pubblico in materia di diritto alla protezione dei dati.

3. Ai fini di cui al paragrafo 2, il Garante europeo della protezione dei dati e le autorità di controllo nazionali si incontrano almeno due volte all'anno nell'ambito del comitato europeo per la protezione dei dati. A tali fini, il comitato europeo per la protezione dei dati può elaborare ulteriori metodi di lavoro, se necessario.

4. Ogni due anni il comitato europeo per la protezione dei dati trasmette al Parlamento europeo, al Consiglio e alla Commissione una relazione congiunta sulle attività svolte in materia di controllo coordinato.

([1]) Decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale (GU L 323 del 10.12.2009, pag. 20).

CAPO VIII

MEZZI DI RICORSO, RESPONSABILITÀ E SANZIONI

Articolo 63

Diritto di proporre reclamo al Garante europeo della protezione dei dati

1. Fatto salvo ogni ricorso giurisdizionale, amministrativo o extragiudiziale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo al Garante europeo della protezione dei dati.

2. Il Garante europeo della protezione dei dati informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 64.

3. Se il Garante europeo della protezione dei dati non tratta il reclamo o non informa l'interessato entro tre mesi dello stato o dell'esito del reclamo, si considera che abbia adottato una decisione negativa.

Articolo 64

Diritto a un ricorso giurisdizionale effettivo

1. La Corte di giustizia è competente a conoscere delle controversie relative alle disposizioni del presente regolamento, incluse le azioni per risarcimento del danno.

2. Avverso le decisioni del Garante europeo della protezione dei dati, comprese le decisioni a norma dell'articolo 63, paragrafo 3, può essere proposto ricorso dinanzi alla Corte di giustizia.

3. La Corte di giustizia ha competenza giurisdizionale anche di merito per le sanzioni amministrative pecuniarie di cui all'articolo 66. Essa può annullare, ridurre o aumentare dette sanzioni entro i limiti dell'articolo 66.

Articolo 65

Diritto al risarcimento

Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dall'istituzione o dall'organo dell'Unione, fatte salve le condizioni previste dai trattati.

Articolo 66

Sanzioni amministrative pecuniarie

1. Il Garante europeo della protezione dei dati può imporre sanzioni amministrative pecuniarie alle istituzioni e agli organi dell'Unione, a seconda delle circostanze di ciascun caso, qualora un'istituzione o un organo dell'Unione non rispetti un ordine del Garante europeo della protezione dei dati emesso ai sensi dell'articolo 58, paragrafo 2, lettere da d) a h) e j). Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso, si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi e il livello del danno da essi subito;

b) le misure adottate dall'istituzione o dall'organo dell'Unione per attenuare il danno subito dagli interessati;

c) il grado di responsabilità dell'istituzione o dell'organo dell'Unione tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 27 e 33;

d) eventuali precedenti violazioni analoghe commesse dall'istituzione o dall'organo dell'Unione;

e) il grado di cooperazione con il Garante europeo della protezione dei dati al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

f) le categorie di dati personali interessate dalla violazione;

g) la maniera in cui il Garante europeo della protezione dei dati ha preso conoscenza della violazione, in particolare se e in che misura l'istituzione o l'organo dell'Unione ha notificato la violazione;

h) il rispetto di qualsiasi provvedimento di cui all'articolo 58 precedentemente disposto nei confronti dell'istituzione o dell'organo dell'Unione in questione relativamente allo stesso oggetto. Il procedimento che porta all'imposizione di tali sanzioni pecuniarie si svolge in tempi ragionevoli in funzione delle circostanze del caso e tenendo conto delle pertinenti azioni e procedimenti di cui all'articolo 69.

2. Le violazioni degli obblighi che incombono alle istituzioni o agli organi dell'Unione a norma degli articoli 8, 12, da 27 a 35, 39, 40, 43, 44 e 45 sono soggette, conformemente al paragrafo 1 del presente articolo, a sanzioni amministrative pecuniarie fino a 25 000 EUR per violazione e fino a un massimo di 250 000 EUR all'anno.

3. Le violazioni delle seguenti disposizioni da parte delle istituzioni o degli organi dell'Unione sono soggette, conformemente al paragrafo 1, a sanzioni amministrative pecuniarie fino a 50 000 EUR per violazione e fino a un massimo di 500 000 EUR all'anno:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 4, 5, 7 e 10;

b) i diritti degli interessati a norma degli articoli da 14 a 24;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale a norma degli articoli da 46 a 50.

4. Se, in relazione allo stesso trattamento o a trattamenti collegati o continui, un'istituzione o un organo dell'Unione viola varie disposizioni del presente regolamento o ripetutamente la stessa disposizione del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

5. Prima di adottare qualsiasi decisione prevista dal presente articolo, il Garante europeo della protezione dei dati dà modo all'istituzione o all'organo dell'Unione oggetto del procedimento avviato dal Garante europeo della protezione dei dati di essere sentiti relativamente agli addebiti che muove loro. Il Garante europeo della protezione dei dati basa le sue decisioni solo sugli addebiti in merito ai quali le parti interessate sono state poste in condizione di esprimersi. I reclamanti sono strettamente associati al procedimento.

6. Nel corso del procedimento sono pienamente garantiti i diritti di difesa delle parti interessate. Esse hanno diritto d'accesso al fascicolo del Garante europeo della protezione dei dati, fermo restando l'interesse legittimo delle persone fisiche o delle imprese alla tutela dei propri dati personali o segreti aziendali.

7. I fondi raccolti mediante l'imposizione di sanzioni pecuniarie in forza del presente articolo entrano nel bilancio generale dell'Unione.

Articolo 67

Rappresentanza degli interessati

L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro che siano debitamente costituiti secondo il diritto dell'Unione o di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati in relazione alla protezione dei dati personali di proporre il reclamo al Garante europeo della protezione dei dati per suo conto e di esercitare per suo conto i diritti di cui agli articoli 63 e 64 nonché il diritto di ottenere il risarcimento di cui all'articolo 65.

Articolo 68

Reclami del personale dell'Unione

Qualsiasi persona alle dipendenze di un'istituzione o di un organo dell'Unione può proporre un reclamo al Garante europeo della protezione dei dati anche senza seguire la via gerarchica per un'asserita violazione delle norme del presente regolamento. Nessun pregiudizio può derivare ad alcuno per il fatto di aver presentato al Garante europeo della protezione dei dati un reclamo relativo a un'asserita violazione.

Articolo 69

Sanzioni

Il funzionario o altro agente dell'Unione che, volontariamente o per negligenza, non assolva agli obblighi previsti dal presente regolamento è passibile di provvedimenti disciplinari o di altro tipo, secondo le norme e le procedure previste dallo statuto.

CAPO IX

TRATTAMENTO DEI DATI PERSONALI OPERATIVI DA PARTE DEGLI ORGANI E DEGLI ORGANISMI DELL'UNIONE NELL'ESERCIZIO DI ATTIVITÀ RIENTRANTI NELL'AMBITO DI APPLICAZIONE DELLA PARTE TERZA, TITOLO V, CAPO 4 O CAPO 5, TFUE

Articolo 70

Ambito di applicazione del presente capo

Il presente capo si applica solo al trattamento dei dati personali operativi da parte di organi e organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE, fatte salve le norme specifiche in materia di protezione dei dati applicabili a tali organi o organismi dell'Unione.

Articolo 71

Principi applicabili al trattamento dei dati personali operativi

1. I dati personali operativi sono:

a) trattati in modo lecito e corretto («liceità e correttezza»);

b) raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità («limitazione della finalità»);

c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati personali operativi 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 a quello necessario al conseguimento delle finalità per le quali sono trattati («limitazione della conservazione»);

f) trattati in modo da garantire un'adeguata sicurezza dei dati personali operativi, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il trattamento da parte dello stesso o di un altro titolare del trattamento per una qualsiasi delle finalità stabilite nell'atto giuridico istitutivo dell'istituzione, dell'organo o dell'organismo dell'Unione diversa da quella per cui sono raccolti i dati personali operativi è consentito nella misura in cui:

a) il titolare del trattamento è autorizzato a trattare tali dati personali operativi per detta finalità conformemente al diritto dell'Unione; e

b) il trattamento è necessario e proporzionato a tale altra finalità conformemente al diritto dell'Unione.

3. Il trattamento da parte dello stesso o di un altro titolare del trattamento può comprendere l'archiviazione nel pubblico interesse, l'utilizzo scientifico, storico o statistico per le finalità stabilite nell'atto giuridico istitutivo dell'organo o dell'organismo dell'Unione, fatte salve le garanzie adeguate per i diritti e le libertà degli interessati.

4. Il titolare del trattamento è competente per il rispetto dei paragrafi 1, 2 e 3 e in grado di comprovarlo.

Articolo 72

Liceità del trattamento dei dati personali operativi

1. Il trattamento dei dati personali operativi è lecito solo se e nella misura in cui è necessario per l'esecuzione di un compito da parte degli organi e degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE ed è basato sul diritto dell'Unione.

2. Specifici atti giuridici dell'Unione che disciplinano il trattamento rientrante nell'ambito di applicazione del presente capo definiscono quantomeno gli obiettivi del trattamento, i dati personali operativi da trattare, le finalità del trattamento e il termine per la conservazione dei dati personali operativi o per un esame periodico della necessità dell'ulteriore conservazione dei dati personali operativi.

Articolo 73

Distinzione tra diverse categorie di interessati

Il titolare del trattamento, se del caso e nella misura del possibile, opera una chiara distinzione tra i dati personali operativi delle diverse categorie di interessati, quali le categorie elencate negli atti giuridici istitutivi degli organi e degli organismi dell'Unione.

Articolo 74

Distinzione tra i dati personali operativi e verifica della qualità dei dati personali operativi

1. Il titolare del trattamento differenzia, nella misura del possibile, i dati personali operativi fondati su fatti da quelli fondati su valutazioni personali.

2. Il titolare del trattamento prende tutte le misure ragionevoli per garantire che i dati personali operativi inesatti, incompleti o non più aggiornati non siano trasmessi o resi disponibili. A tal fine, il titolare del trattamento verifica, per quanto possibile e ove pertinente, la qualità dei dati personali operativi prima che questi siano trasmessi o resi disponibili, ad esempio consultando l'autorità competente da cui provengono i dati. Per quanto possibile, il titolare del trattamento correda tutte le trasmissioni di dati personali operativi delle informazioni necessarie che consentono al destinatario di valutare il grado di esattezza, completezza e affidabilità dei dati personali operativi, e la misura in cui essi sono aggiornati.

3. Qualora risulti che sono stati trasmessi dati personali operativi inesatti o che sono stati trasmessi dati personali operativi illecitamente, il destinatario ne è informato quanto prima. In tal caso, i dati personali operativi interessati sono rettificati o cancellati o ne è limitato il trattamento a norma dell'articolo 82.

Articolo 75

Condizioni di trattamento specifiche

1. Se il diritto dell'Unione applicabile al titolare del trattamento che trasmette i dati prevede condizioni di trattamento specifiche, il titolare del trattamento informa il destinatario dei dati personali operativi di tali condizioni e dell'obbligo di rispettarle.

2. Il titolare del trattamento rispetta le condizioni di trattamento specifiche previste dall'autorità competente che trasmette i dati, in conformità dell'articolo 9, paragrafi 3 e 4, della direttiva (UE) 2016/680.

Articolo 76

Trattamento di categorie particolari di dati personali operativi

1. Il trattamento di dati personali operativi che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati personali operativi relativi alla salute o alla vita sessuale o orientamento sessuale della persona fisica è autorizzato solo se strettamente necessario a fini operativi, nell'ambito del mandato dell'organo o dell'organismo dell'Unione interessato e se soggetto a garanzie adeguate per i diritti e le libertà dell'interessato. È vietata la discriminazione delle persone fisiche sulla base di tali dati personali.

2. Il responsabile della protezione dei dati è informato senza indebito ritardo del ricorso al presente articolo.

Articolo 77

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. Una decisione basata unicamente su un trattamento automatizzato, compresa la profilazione, che produca effetti giuridici negativi o incida significativamente sull'interessato è vietata salvo che sia autorizzata dal diritto dell'Unione cui è soggetto il titolare del trattamento e che preveda garanzie adeguate per i diritti e le libertà dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento.

2. Le decisioni di cui al paragrafo 1 del presente articolo non si basano sulle categorie particolari di dati personali di cui all'articolo 76, a meno che non siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e degli interessi legittimi dell'interessato.

3. La profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 76 è vietata, conformemente al diritto dell'Unione.

Articolo 78

Comunicazioni e modalità per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure ragionevoli per fornire all'interessato tutte le informazioni di cui all'articolo 79 ed effettua le comunicazioni con riferimento agli articoli da 80 a 84 e 92 relative al trattamento, in forma concisa, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite con qualsiasi mezzo adeguato, anche per via elettronica. Come regola generale il titolare del trattamento fornisce le informazioni nella stessa forma della richiesta.

2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 79 a 84.

3. Senza indebito ritardo e in ogni caso al più tardi entro tre mesi dal ricevimento della richiesta dell'interessato, il titolare del trattamento informa quest'ultimo per iscritto in merito al seguito dato alla sua richiesta.

4. Il titolare del trattamento dispone che le informazioni fornite ai sensi dell'articolo 79 ed eventuali comunicazioni effettuate o azioni intraprese ai sensi degli articoli da 80 a 84 e 92 siano gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può rifiutare di soddisfare la richiesta. Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

5. Qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta una richiesta di cui agli articoli 80 o 82, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

Articolo 79

Informazioni da rendere disponibili o da fornire all'interessato

1. Il titolare del trattamento mette a disposizione dell'interessato almeno le informazioni seguenti:

a) l'identità e i dati di contatto dell'organo o dell'organismo dell'Unione;

b) i dati di contatto del responsabile della protezione dei dati;

c) le finalità del trattamento cui sono destinati i dati personali operativi;

d) il diritto di proporre reclamo al Garante europeo della protezione dei dati e i suoi dati di contatto;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali operativi e la loro rettifica o cancellazione e la limitazione del trattamento dei dati personali operativi che lo riguardano.

2. In aggiunta alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato, in casi specifici previsti dal diritto dell'Unione, le seguenti ulteriori informazioni per consentire l'esercizio dei diritti dell'interessato:

a) la base giuridica per il trattamento;

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

c) se del caso, le categorie di destinatari dei dati personali operativi, anche in paesi terzi o in seno a organizzazioni internazionali;

d) se necessario, ulteriori informazioni, in particolare nel caso in cui i dati personali operativi siano raccolti all'insaputa dell'interessato.

3. Il titolare del trattamento può ritardare, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del paragrafo 2 nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e degli interessi legittimi della persona fisica interessata, al fine di:

a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;

c) proteggere la sicurezza pubblica degli Stati membri;

d) proteggere la sicurezza nazionale degli Stati membri;

e) proteggere i diritti e le libertà di altri, inclusi le vittime e i testimoni.

Articolo 80

Diritto di accesso dell'interessato

L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali operativi che lo riguardano e, in tal caso, ha il diritto di ottenere l'accesso ai dati personali operativi e alle informazioni seguenti:

a) le finalità e la base giuridica del trattamento;

b) le categorie di dati personali operativi in questione;

c) i destinatari o le categorie di destinatari a cui i dati personali operativi sono stati comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;

d) quando possibile, il periodo di conservazione dei dati personali operativi previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o cancellazione dei dati personali operativi o la limitazione del trattamento dei dati personali operativi che lo riguardano;

f) il diritto di proporre reclamo al Garante europeo della protezione dei dati e i suoi dati di contatto;

g) la comunicazione dei dati personali operativi oggetto del trattamento e di tutte le informazioni disponibili sulla loro origine.

Articolo 81

Limitazioni del diritto di accesso

1. Il titolare del trattamento può limitare, in tutto o in parte, il diritto di accesso dell'interessato nella misura e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e degli interessi legittimi della persona fisica interessata, al fine di:

a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

b) non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali;

c) proteggere la sicurezza pubblica degli Stati membri;

d) proteggere la sicurezza nazionale degli Stati membri;

e) proteggere i diritti e le libertà di altri, inclusi le vittime e i testimoni.

2. Nei casi di cui al paragrafo 1, il titolare del trattamento informa l'interessato, senza indebito ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei motivi del rifiuto o della limitazione. Detta comunicazione può essere omessa qualora il suo rilascio rischi di compromettere una delle finalità di cui al paragrafo 1. Il titolare del trattamento informa l'interessato della possibilità di proporre reclamo al Garante europeo della protezione dei dati o di proporre ricorso giurisdizionale dinanzi alla Corte di giustizia. Il titolare del trattamento documenta i motivi di fatto o di diritto su cui si basa la decisione. Tali informazioni sono messe a disposizione del Garante europeo della protezione dei dati su richiesta.

Articolo 82

Diritto di rettifica o cancellazione di dati personali operativi e limitazione di trattamento

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali operativi inesatti che lo riguardano senza indebito ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali operativi incompleti, anche fornendo una dichiarazione integrativa.

2. Il titolare del trattamento cancella senza indebito ritardo i dati personali operativi e l'interessato ha il diritto di ottenere dal titolare del trattamento, senza indebito ritardo, la cancellazione dei dati personali operativi che lo riguardano qualora il trattamento violi l'articolo 71, l'articolo 72, paragrafo 1, o l'articolo 76 oppure qualora i dati personali operativi debbano essere cancellati per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.

3. Anziché cancellare, il titolare del trattamento limita il trattamento quando:

a) l'esattezza dei dati personali è contestata dall'interessato e la loro esattezza o inesattezza non può essere accertata; oppure

b) i dati personali devono essere conservati a fini probatori.

Quando il trattamento è limitato a norma del primo comma, lettera a), il titolare del trattamento informa l'interessato prima di revocare la limitazione del trattamento.

I dati ai quali l'accesso è limitato sono trattati per la sola finalità che ne ha impedito la cancellazione.

4. Il titolare del trattamento informa per iscritto l'interessato dell'eventuale rifiuto di rettifica o cancellazione dei dati personali operativi o limitazione del trattamento e dei motivi del rifiuto. Il titolare del trattamento può limitare, in tutto o in parte, il rilascio di tali informazioni nella misura in cui tale limitazione costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e degli interessi legittimi della persona fisica interessata, al fine di:

a) non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

b) non compromettere la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali;

c) proteggere la sicurezza pubblica degli Stati membri;

d) proteggere la sicurezza nazionale degli Stati membri;

e) proteggere i diritti e le libertà di altri, inclusi le vittime e i testimoni.

Il titolare del trattamento informa l'interessato della possibilità di proporre reclamo al Garante europeo della protezione dei dati e di proporre ricorso giurisdizionale dinanzi alla Corte di giustizia.

5. Il titolare del trattamento comunica le rettifiche dei dati personali operativi inesatti all'autorità competente da cui i dati personali operativi inesatti provengono.

6. Il titolare del trattamento, qualora i dati personali operativi siano stati rettificati o cancellati o il trattamento sia stato limitato a norma dei paragrafi 1, 2 o 3, ne informa i destinatari, comunicando loro che devono rettificare o cancellare i dati personali operativi o limitare il trattamento dei dati personali operativi sotto la propria responsabilità.

Articolo 83

Diritto di accesso nel corso di indagini e procedimenti penali

Quando i dati personali operativi provengono da un'autorità competente, gli organi e gli organismi dell'Unione verificano con l'autorità competente interessata, prima di decidere sul diritto di accesso di un interessato, se tali dati personali figurano in una decisione giudiziaria, in un casellario o in un fascicolo giudiziario oggetto di trattamento nel corso di un'indagine e di un procedimento penale nello Stato membro dell'autorità competente in questione. In caso affermativo, la decisione sul diritto di accesso è adottata in consultazione e in stretta cooperazione con l'autorità competente in questione.

Articolo 84

Esercizio dei diritti da parte dell'interessato e verifica da parte del Garante europeo della protezione dei dati

1. Nei casi di cui all'articolo 79, paragrafo 3, all'articolo 81 e all'articolo 82, paragrafo 4, i diritti dell'interessato possono essere esercitati anche tramite il Garante europeo della protezione dei dati.

2. Il titolare del trattamento informa l'interessato della possibilità di esercitare i suoi diritti tramite il Garante europeo della protezione dei dati ai sensi del paragrafo 1.

3. Qualora sia esercitato il diritto di cui al paragrafo 1, il Garante europeo della protezione dei dati informa l'interessato, perlomeno, di aver eseguito tutte le verifiche necessarie o un riesame. Il Garante europeo della protezione dei dati informa inoltre l'interessato del diritto di quest'ultimo di proporre ricorso giurisdizionale dinanzi alla Corte di giustizia.

Articolo 85

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e del suo atto giuridico istitutivo e tutelare i diritti degli interessati.

2. Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali operativi adeguati, pertinenti e non eccedenti rispetto alle finalità per i quali sono trattati. Tale obbligo vale per la quantità dei dati personali operativi raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali operativi a un numero indefinito di persone fisiche senza l'intervento della persona fisica.

Articolo 86

Contitolari del trattamento

1. Allorché due o più titolari del trattamento o uno o più titolari del trattamento insieme a uno o più uno o più titolari del trattamento diversi dalle istituzioni e dagli organi dell'Unione determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi di protezione dei dati, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui all'articolo 79, a meno che e nella misura in cui le rispettive responsabilità dei contitolari siano determinate dal diritto dell'Unione o dello Stato membro cui i contitolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con l'interessato. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento.

Articolo 87

Responsabile del trattamento

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

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o del diritto degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali operativi e le categorie di interessati, nonché gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) agisca soltanto su istruzione del titolare del trattamento;

b) garantisca che le persone autorizzate al trattamento dei dati personali operativi si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) assista il titolare del trattamento con ogni mezzo adeguato per garantire la conformità con le disposizioni relative ai diritti dell'interessato;

d) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali operativi dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o il diritto degli Stati membri preveda la conservazione dei dati personali operativi;

e) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo;

f) soddisfi le condizioni di cui al paragrafo 2 e al presente paragrafo per ricorrere a un altro responsabile del trattamento.

4. Il contratto o altro atto giuridico di cui al paragrafo 3 è stipulato in forma scritta, anche in formato elettronico.

5. Se un responsabile del trattamento viola il presente regolamento o l'atto giuridico istitutivo del titolare del trattamento determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento relativamente al trattamento in questione.

Articolo 88

Registrazione

1. Il titolare del trattamento registra in sistemi di trattamento automatizzato qualsiasi delle seguenti operazioni di trattamento: raccolta, modifica, accesso, consultazione, comunicazione, inclusi i trasferimenti, interconnessione e cancellazione di dati personali operativi. Le registrazioni delle consultazioni e delle comunicazioni consentono di stabilire la motivazione, la data e l'ora di tali operazioni, di identificare la persona che ha consultato o comunicato i dati personali operativi, nonché, nella misura del possibile, di stabilire l'identità dei destinatari di tali dati personali operativi.

2. Le registrazioni sono usate ai soli fini della verifica della liceità del trattamento, dell'autocontrollo, per garantire l'integrità e la sicurezza dei dati personali operativi e nell'ambito di procedimenti penali. Le registrazioni sono cancellate dopo tre anni, salvo se sono necessarie per un controllo in corso.

3. Su richiesta, il titolare del trattamento mette le registrazioni a disposizione del suo responsabile della protezione dei dati e del Garante europeo della protezione dei dati.

Articolo 89

Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali operativi.

2. La valutazione di cui al paragrafo 1 contiene almeno una descrizione generale dei trattamenti previsti, una valutazione dei rischi per i diritti e le libertà degli interessati, le misure previste per affrontare tali rischi, le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali operativi e dimostrare la conformità alle norme in materia di protezione dei dati, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Articolo 90

Consultazione preventiva del Garante europeo della protezione dei dati

1. Il titolare del trattamento consulta il Garante europeo della protezione dei dati prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se:

a) una valutazione d'impatto sulla protezione dei dati a norma dell'articolo 89 indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure

b) il tipo di trattamento, in particolare se utilizza tecnologie, procedure o meccanismi nuovi, presenta un rischio elevato per i diritti e le libertà degli interessati.

2. Il Garante europeo della protezione dei dati può stabilire un elenco di trattamenti soggetti a consultazione preventiva ai sensi del paragrafo 1.

3. Il titolare del trattamento trasmette al Garante europeo della protezione dei dati la valutazione d'impatto sulla protezione dei dati di cui all'articolo 89 e, su richiesta, ogni altra informazione, al fine di consentire al Garante europeo della protezione dei dati di effettuare una valutazione della conformità del trattamento, in particolare dei rischi per la protezione dei dati personali operativi dell'interessato e delle relative garanzie.

4. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento o l'atto giuridico istitutivo dell'organo o dell'organsimo dell'Unione, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, il Garante europeo della protezione dei dati fornisce un parere scritto al titolare del trattamento entro un termine di sei settimane dal ricevimento della richiesta di consultazione. Tale periodo può essere prorogato di un mese, tenendo conto della complessità del trattamento previsto. Il Garante europeo della protezione dei dati informa il titolare del trattamento di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.

Articolo 91

Sicurezza del trattamento dei dati personali operativi

1. Il titolare del trattamento e il responsabile del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato ai rischi, in particolare riguardo al trattamento di categorie particolari di dati personali operativi.

2. In relazione al trattamento automatizzato, titolare del trattamento e il responsabile del trattamento, previa valutazione dei rischi, mettono in atto misure volte a:

a) vietare alle persone non autorizzate l'accesso alle attrezzature di trattamento dei dati utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);

b) impedire che i supporti di dati siano letti, copiati, modificati o rimossi senza autorizzazione («controllo dei supporti di dati»);

c) impedire che dati personali operativi conservati siano introdotti, consultati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);

e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali operativi cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

f) garantire la possibilità di verificare e accertare gli organi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali operativi utilizzando la trasmissione di dati («controllo della trasmissione»);

g) garantire la possibilità di verificare e accertare a posteriori quali dati personali operativi sono stati introdotti nei sistemi di trattamento automatizzato dei dati personali operativi, il momento dell'introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali operativi o il trasporto di supporti di dati («controllo del trasporto»);

i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);

j) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali operativi conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Articolo 92

Notifica di una violazione dei dati personali al Garante europeo della protezione dei dati

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante europeo della protezione dei dati senza indebito ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica al Garante europeo della protezione dei dati non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

2. La notifica di cui al paragrafo 1 deve almeno:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali operativi in questione;

b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati;

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

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

3. Qualora e nella misura in cui non sia possibile fornire le informazioni di cui al paragrafo 2 contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

4. Il titolare del trattamento documenta qualsiasi violazione dei dati personali di cui al paragrafo 1, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione deve consentire al Garante europeo della protezione dei dati di verificare il rispetto del presente articolo.

5. Se la violazione dei dati personali riguarda dati personali operativi che sono stati trasmessi dalle o alle autorità competenti, il titolare del trattamento comunica senza indebito ritardo le informazioni di cui al paragrafo 2 alle autorità competenti in questione.

Articolo 93

Comunicazione di una violazione dei dati personali all'interessato

1. Qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza indebito ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'articolo 92, paragrafo 2, lettere b), c) e d).

3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:

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

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante europeo della protezione dei dati, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, può richiedere che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

5. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo può essere ritardata, limitata od omessa alle condizioni e per i motivi di cui all'articolo 79, paragrafo 3.

Articolo 94

Trasferimento dei dati personali operativi a paesi terzi e a organizzazioni internazionali

1. Fatte salve le limitazioni e le condizioni stabilite negli atti giuridici istitutivi dell'organo o dell'organismo dell'Unione, il titolare del trattamento può trasferire i dati personali operativi a un'autorità di un paese terzo o a un'organizzazione internazionale nella misura in cui tale trasferimento è necessario per lo svolgimento delle attività del titolare del trattamento e soltanto se sono soddisfatte le condizioni di cui al presente articolo, vale a dire:

a) la Commissione ha adottato una decisione di adeguatezza ai sensi dell'articolo 36, paragrafo 3, della direttiva (UE) 2016/680, che sancisca che il paese terzo o un territorio o un settore di trattamento all'interno di tale paese terzo o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato;

b) in assenza di una decisione di adeguatezza della Commissione a norma della lettera a), è stato concluso un accordo internazionale tra l'Unione e tale paese terzo o organizzazione internazionale ai sensi dell'articolo 218 TFUE, che presti garanzie sufficienti con riguardo alla tutela della vita privata e dei diritti e delle libertà fondamentali delle persone;

c) in assenza di una decisione di adeguatezza della Commissione a norma della lettera a) o di un accordo internazionale di cui alla lettera b), tra l'organo o l'organismo dell'Unione e il paese terzo in questione è stato concluso, prima della data di applicazione dell'atto giuridico istitutivo dell'organo o dell'organismo dell'Unione interessato, un accordo di cooperazione che consenta lo scambio di dati personali operativi.

2. Gli atti giuridici istitutivi degli organi e degli organismi dell'Unione possono mantenere o introdurre disposizioni più specifiche riguardo alle condizioni per i trasferimenti internazionali di dati personali operativi, in particolare per quanto concerne il trasferimento in presenza di garanzie adeguate e le deroghe per situazioni specifiche.

3. Il titolare del trattamento pubblica sul proprio sito web e tiene aggiornato un elenco delle decisioni di adeguatezza di cui al paragrafo 1, lettera a), degli accordi, delle intese amministrative e degli altri strumenti riguardanti il trasferimento di dati personali operativi ai sensi del paragrafo 1.

4. Il titolare del trattamento provvede affinché siano registrati dettagliatamente tutti i trasferimenti effettuati a norma del presente articolo.

Articolo 95

Segretezza delle indagini e dei procedimenti penali

Gli atti giuridici istitutivi degli organi o degli organismi dell'Unione che svolgono attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE possono prescrivere che il Garante europeo della protezione dei dati tenga nella massima considerazione, nell'esercizio dei suoi poteri di vigilanza, la segretezza delle indagini e dei procedimenti penali, in conformità del diritto dell'Unione o degli Stati membri.

CAPO X

ATTI DI ESECUZIONE

Articolo 96

Procedura di comitato

1. La Commissione è assistita dal comitato istituito dall'articolo 93 del regolamento (UE) 2016/679. 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.

CAPO XI

RIESAME

Articolo 97

Clausola di riesame

Non oltre il 30 aprile 2022, e successivamente ogni cinque anni, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'applicazione del presente regolamento, corredata, se necessario, di proposte legislative adeguate.

Articolo 98

Riesame degli atti giuridici dell'Unione

1. Entro il 30 aprile 2022 la Commissione riesamina gli atti giuridici adottati a norma dei trattati che disciplinano il trattamento dei dati personali operativi da parte degli organi o degli organismi dell'Unione nell'esercizio di attività rientranti nell'ambito di applicazione della parte terza, titolo V, capo 4 o capo 5, TFUE al fine di:

a) valutarne la coerenza con la direttiva (UE) 2016/680 e con il capo IX del presente regolamento;

b) individuare disparità che possano ostacolare lo scambio di dati personali operativi tra gli organi o gli organismi dell'Unione nell'esercizio di attività in tali ambiti e le autorità competenti; e

c) individuare divergenze che possano dare luogo a una frammentazione giuridica della legislazione in materia di protezione dei dati nell'Unione.

2. Sulla base del riesame, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche in relazione al trattamento, la Commissione può presentare a Europol e alla Procura europea adeguate proposte legislative, in particolare ai fini dell'applicazione del capo IX del presente regolamento, inclusi, se del caso, adeguamenti del capo IX del presente regolamento.

CAPO XII

DISPOSIZIONI FINALI

Articolo 99

Abrogazione del regolamento (CE) n. 45/2001 e della decisione n. 1247/2002/CE

Il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE sono abrogati a decorrere dall'11 dicembre 2018. I riferimenti al regolamento e alla decisione abrogati si intendono fatti al presente regolamento.

Articolo 100

Misure transitorie

1. Il presente regolamento non incide sulla decisione 2014/886/UE del Parlamento europeo e del Consiglio [1] e sugli attuali mandati del Garante europeo della protezione dei dati e del garante aggiunto.

[1] Decisione 2014/886/UE del Parlamento europeo e del Consiglio, del 4 dicembre 2014, relativa alla nomina del garante europeo della protezione dei dati e del garante aggiunto (GU L 351 del 9.12.2014, pag. 9).

2. Il garante aggiunto è equiparato al cancelliere della Corte di giustizia per quanto riguarda la retribuzione, le indennità, il trattamento di quiescenza e ogni altro compenso sostitutivo.

3. L'articolo 53, paragrafi 4, 5 e 7, e gli articoli 55 e 56 del presente regolamento si applicano all'attuale garante aggiunto fino al termine del suo mandato.

4. Il garante aggiunto assiste il Garante europeo della protezione dei dati nell'espletamento di tutte le sue funzioni e lo sostituisce quando quest'ultimo è assente o impossibilitato a svolgere le sue funzioni fino alla fine dell'attuale mandato del garante aggiunto.

Articolo 101

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. Tuttavia il presente regolamento si applica al trattamento dei dati personali da parte di Eurojust a partire dal 12 dicembre 2019.

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

Fatto a Strasburgo, il 23 ottobre 2018.

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il president*
A. TAJANI	K. EDTSTADLER