Consiglio dell'Unione europea

Bruxelles, 12 gennaio 2017
(OR. en)

5034/17

Fascicolo interistituzionale: 2017/0002 (COD)

DATAPROTECT 2
JAI 2
DAPIX 2
FREMP 1
DIGIT 2
CODEC 4

PROPOSTA

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	12 gennaio 2017
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2017) 8 final
Oggetto:	Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché la libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE

Si trasmette in allegato, per le delegazioni, il documento COM(2017) 8 final.

All.: COM(2017) 8 final

COMMISSIONE
EUROPEA

Bruxelles, 10.1.2017
COM(2017) 8 final

2017/0002 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

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

RELAZIONE

1. CONTESTO DELLA PROPOSTA

• Motivi e obiettivi della proposta

L'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE), introdotto dal trattato di Lisbona, stabilisce il principio secondo il quale ogni persona ha diritto alla protezione dei dati personali che la riguardano. Inoltre al paragrafo 2 dello stesso articolo il trattato di Lisbona ha introdotto una base giuridica specifica per l'adozione di norme in materia di protezione dei dati personali. L'articolo 8 della Carta dei diritti fondamentali dell'Unione europea (Carta) annovera la protezione dei dati personali tra i diritti fondamentali.

Il diritto alla protezione dei dati personali si applica anche al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione. Il regolamento (CE) n. 45/2001[1] – pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali – è stato adottato nel 2001 con due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali in tutta l'Unione. Il regolamento è stato integrato dalla decisione n. 1247/2002/CE[2].

Il 27 aprile 2016 il Parlamento europeo e il Consiglio hanno adottato il regolamento generale sulla protezione dei dati (regolamento (UE) 2016/679) che sarà applicabile dal 25 maggio 2018. Il presente regolamento richiede che il regolamento (CE) n. 45/2001 sia adeguato ai principi e alle norme stabiliti nel regolamento (UE) 2016/679 al fine di fornire un quadro di protezione dei dati solido e coerente nell'Unione e consentire di applicare contemporaneamente entrambi gli strumenti[3].

L'allineamento, per quanto possibile, delle norme sulla protezione dei dati per le istituzioni, gli organi, gli uffici e le agenzie dell'Unione a quelle adottate per il settore pubblico degli Stati membri è in linea con l'approccio coerente in materia di protezione dei dati personali in tutta l'Unione. Quando le disposizioni della proposta si basano sullo stesso concetto su cui si basano le disposizioni del regolamento (UE) 2016/679, le disposizioni dei due regolamenti dovrebbero essere interpretate in modo omogeneo, in particolare in considerazione del fatto che il regime della proposta dovrebbe essere inteso come equivalente a quello del regolamento (UE) 2016/679[4].

Il riesame del regolamento (CE) n. 45/2001 tiene conto anche dei risultati delle indagini, delle consultazioni con i portatori di interesse e dello studio di valutazione dell'applicazione del medesimo negli ultimi 15 anni.

La presente iniziativa non rientra nel programma di controllo dell'adeguatezza e dell'efficienza normativa (REFIT).

---

1 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).

2 Decisione n. 1247/2002/CE, del 1° 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).

3 Cfr. regolamento (UE) 2016/679, articolo 98 e considerando 17.

4 Cfr. sentenza della Corte di giustizia del 9 marzo 2010, *Commissione/Germania*, causa C-518/07, ECLI:EU:C:2010:125, punti 26 e 28.

- **Coerenza con le disposizioni vigenti nel settore normativo interessato**

La proposta si prefigge di allineare le disposizioni del regolamento (CE) n. 45/2001 ai principi e alle norme stabiliti dal regolamento (UE) 2016/679, al fine di fornire un quadro di protezione dei dati solido e coerente nell'Unione. La proposta integra anche le norme pertinenti stabilite dal regolamento (UE) XXXX/XX [regolamento relativo alla vita privata e alle comunicazioni elettroniche] per quanto riguarda la protezione delle apparecchiature terminali degli utenti finali.

- **Coerenza con le altre normative dell'Unione**

Non pertinente

2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- **Base giuridica**

La protezione delle persone fisiche in relazione al trattamento dei loro dati personali è un diritto fondamentale stabilito dall'articolo 8, paragrafo 1, della Carta.

La presente proposta si basa sull'articolo 16 del TFUE, la base giuridica per l'adozione delle norme in materia di protezione dei dati. Tale articolo consente di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli delle istituzioni, degli organi e degli organismi dell'Unione nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione. Tale disposizione consente inoltre l'adozione di norme relative alla libera circolazione dei dati personali, inclusi i dati personali trattati da dette istituzioni, organi e organismi.

- **Sussidiarietà (per la competenza non esclusiva)**

L'oggetto del presente regolamento ricade nell'ambito della competenza esclusiva dell'Unione, in quanto soltanto l'Unione può adottare norme che disciplinano il trattamento dei dati personali da parte delle proprie istituzioni.

- **Proporzionalità**

In conformità al principio di proporzionalità, per il conseguimento degli obiettivi fondamentali di garantire un livello equivalente di protezione delle persone fisiche per quanto riguarda il trattamento dei dati personali e la libera circolazione degli stessi in tutta l'Unione, è necessario e appropriato stabilire norme per il trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione. Il presente regolamento si limita a quanto necessario per il raggiungimento degli obiettivi perseguiti, in conformità dell'articolo 5, paragrafo 4, del trattato sull'Unione europea.

- **Scelta dell'atto giuridico**

Un regolamento è considerato lo strumento giuridico appropriato per definire il quadro di protezione delle persone fisiche per quanto riguarda il trattamento di dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione e la libera circolazione di tali dati. Esso conferisce alle persone fisiche diritti azionabili e precisa gli obblighi in materia di trattamento di dati dei titolari del trattamento nelle istituzioni, negli organi, negli uffici e nelle agenzie dell'Unione. Esso prevede inoltre che un'autorità di controllo indipendente, il garante europeo della protezione dei dati, sia responsabile di sorvegliare il trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione.

3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

La Commissione ha condotto consultazioni con i portatori di interessi nel 2010 e nel 2011 e una valutazione d'impatto nell'ambito della preparazione del pacchetto di riforme della protezione dei dati, in cui sono fornite informazioni sulle modifiche che si propone di apportare al regolamento (CE) n. 45/2001. In tale contesto la Commissione ha svolto anche un'indagine sui coordinatori per la protezione dei dati (CPD) della Commissione stessa[5].

Con riguardo all'applicazione pratica del regolamento (CE) n. 45/2001 da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, sono state raccolte informazioni dal garante europeo della protezione dei dati (GEPD), dalle altre istituzioni, organi, uffici e agenzie dell'Unione, dalle altre DG della Commissione e da un contraente esterno. Un questionario è stato inviato alla rete dei responsabili della protezione dei dati[6].

I responsabili della protezione dei dati di varie istituzioni, organi, uffici e agenzie dell'Unione hanno tenuto workshop sulla riforma del regolamento (CE) n. 45/2001 il 9 luglio 2015, il 22 ottobre 2015, il 19 gennaio 2016 e il 15 marzo 2016.

Nel 2013 la Commissione ha deciso di condurre uno studio di valutazione sull'applicazione, fino a quel momento, del regolamento (CE) n. 45/2001, che ha affidato a un contraente esterno. I risultati finali dello studio di valutazione (relazione finale, cinque studi di casi e un'analisi dei singoli articoli) sono stati presentati alla Commissione l'8 giugno 2015[7].

La valutazione ha dimostrato l'efficacia del sistema di governance che si basa sui responsabili della protezione dei dati (RPD) e sul GEPD. Essa ha stabilito che la suddivisione dei poteri tra gli RPD e il GEPD è chiara ed equilibrata e che entrambi hanno una gamma adeguata di poteri. Potrebbero tuttavia sorgere difficoltà a causa della mancanza di autorità, in quanto gli RPD non ricevono un sostegno sufficiente da parte della loro gestione.

Lo studio di valutazione indica che si potrebbe migliorare l'attuazione del regolamento (CE) n. 45/2001 conferendo al GEPD il potere di imporre sanzioni. L'aumento dell'uso dei suoi poteri di autorità di controllo potrebbe portare a una migliore attuazione delle norme in materia di protezione dei dati. Lo studio conclude poi che i titolari del trattamento dovrebbero adottare un approccio di gestione dei rischi e svolgere valutazioni dei rischi prima di effettuare i trattamenti al fine di migliorare l'attuazione dei requisiti di conservazione e sicurezza dei dati.

Lo studio ha dimostrato anche che le attuali norme del capo IV del regolamento (CE) n. 45/2001 concernenti il settore delle telecomunicazioni sono superate ed è necessario allineare detto capo con la direttiva relativa alla vita privata e alle comunicazioni elettroniche. Secondo lo studio di valutazione è inoltre necessario chiarire ulteriormente alcune definizioni

---

5 Si veda http://ec.europa.eu/justice/data-protection/reform/index_en.htm

6 Si veda la relazione generale del garante europeo della protezione dei dati "Measuring compliance with Regulation (EC) 45/2001 in EU institutions ("Survey 2013")" ("Misura del rispetto del regolamento (CE) n. 45/2001 nelle istituzioni dell'UE ("indagine 2013") e il documento "Opinion 3/2015 "Europe's big opportunity: EDPS recommendations on the EU's options for data protection reform" (Opinione 3/2015 "Una grande opportunità per l'Europa: le raccomandazioni del GEPD sulle opzioni dell'UE per la riforma della protezione dei dati)".

7 JUST/2013/FRAC/FW/0157/A4 nel contesto del contratto quadro multiplo JUST/2011/EVAL/01JUST/2011/EVAL/01 (RS 2013/05) - "Evaluation Study on Regulation (EC) 45/2001" (Studio di valutazione sul regolamento (CE) n. 45/2001), realizzato da Ernst and Young, disponibile all'indirizzo http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087

fondamentali del regolamento (CE) n. 45/2001. Esse includono l'individuazione dei titolari del trattamento dei dati all'interno delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, la definizione dei destinatari e l'estensione dell'obbligo di riservatezza ai responsabili del trattamento esterni.

Lo studio di valutazione ha inoltre indicato la necessità di semplificare il regime delle notifiche e dei controlli preventivi al fine di aumentare l'efficienza e ridurre gli oneri amministrativi.

Il valutatore ha condotto un'indagine online su 64 istituzioni, organi e uffici e agenzie dell'Unione. Hanno risposto alle domande dell'indagine 422 funzionari responsabili dei titolari del trattamento, 73 RPD, 118 CPD e 109 membri del personale informatico. Il valutatore ha anche condotto una serie di interviste con i portatori di interesse. Il 26 marzo 2015 il valutatore e la Commissione hanno organizzato un workshop finale a cui hanno partecipato vari titolari del trattamento, RPD, CPD, membri del personale informatico e rappresentanti del GEDP.

- **Assunzione e uso di perizie**

Si veda il riferimento allo studio di valutazione nel punto precedente.

- **Valutazione d'impatto**

L'impatto della presente proposta riguarda principalmente le istituzioni, gli organi, gli uffici e le agenzie dell'Unione. Ciò è stato confermato dalle informazioni che sono state raccolte dal garante europeo della protezione dei dati, dalle altre istituzioni, organi, uffici e agenzie dell'Unione, dalle altre DG della Commissione e da un contraente esterno. Inoltre l'impatto dei nuovi obblighi derivanti dal regolamento (UE) 2016/679, a cui il presente regolamento deve essere allineato, è stato valutato nell'ambito dei lavori preparatori per quest'ultimo. Non è pertanto necessaria una valutazione d'impatto specifica per il presente regolamento.

- **Efficienza normativa e semplificazione**

Non pertinente

- **Diritti fondamentali**

Il diritto alla protezione dei dati personali è sancito dall'articolo 8 della Carta, dall'articolo 16 del TFUE e dall'articolo 8 della Convenzione europea dei diritti dell'uomo. Come sottolinea la Corte di giustizia dell'Unione europea[8], il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale[9]. La protezione dei dati è strettamente legata anche al rispetto della vita privata e familiare tutelato dall'articolo 7 della Carta.

La presente proposta stabilisce le norme di protezione delle persone fisiche per quanto riguarda il trattamento di dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione e la libera circolazione di tali dati.

---

[8] Cfr. sentenza della Corte di giustizia del 9 novembre 2010, *Volker und Markus Schecke e Eifer*, cause riunite C-92/09 e C-93/09, ECLI:EU:C:2009:284, punto 48.

[9] Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni all'esercizio del diritto alla protezione dei dati devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

Altri diritti fondamentali sanciti dalla Carta che potrebbero essere potenzialmente interessati sono: la libertà di espressione (articolo 11); il diritto di proprietà e, in particolare, la tutela della proprietà intellettuale (articolo 17, paragrafo 2); il divieto di qualsiasi forma di discriminazione fondata, tra l'altro, sulla razza, l'origine etnica, le caratteristiche genetiche, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, la disabilità, o l'orientamento sessuale (articolo 21); i diritti del minore (articolo 24); il diritto a un elevato livello di protezione sanitaria (articolo 35); il diritto d'accesso ai documenti (articolo 42) e il diritto a un ricorso effettivo e a un giudice imparziale (articolo 47*)*.

4. INCIDENZA SUL BILANCIO

Si veda la scheda finanziaria nell'allegato.

5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

Non pertinente

- **Documenti esplicativi (per le direttive)**

Non pertinente

CAPO I - DISPOSIZIONI GENERALI

L'articolo 1 definisce l'oggetto del regolamento e, alla stregua dell'articolo 1 del regolamento (CE) n. 45/2001, stabilisce i due obiettivi del regolamento: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali in tutta l'Unione. Esso prevede inoltre i compiti principali del garante europeo della protezione dei dati.

L'articolo 2 delimita l'ambito di applicazione del regolamento. Quest'ultimo si applica al trattamento dei dati personali, con l'ausilio di strumenti automatizzati o in altro modo, da parte di tutte le istituzioni e di tutti gli organi dell'Unione, nella misura in cui detto trattamento è effettuato nell'esercizio di attività che rientrano in tutto o in parte nell'ambito di applicazione del diritto dell'Unione. L'ambito di applicazione materiale del regolamento proposto è tecnologicamente neutro. La protezione dei dati personali si applica sia al trattamento dei dati personali con l'ausilio di strumenti automatizzati sia al trattamento manuale, se i dati personali sono contenuti o destinati a essere contenuti in un archivio.

L'articolo 3 contiene le definizioni dei termini utilizzati nel regolamento. Eccettuate le definizioni di "istituzioni e organi dell'Unione", "titolare del trattamento", "utente" ed "elenco", che sono specifiche del regolamento proposto, i termini in esso utilizzati sono definiti nel regolamento (UE) 2016/679, nel regolamento (UE) 0000/00 [nuovo regolamento relativo alla vita privata e alle comunicazioni elettroniche], nella direttiva 00/0000/UE [direttiva che istituisce il codice europeo delle comunicazioni elettroniche] e la direttiva 2008/63/CE della Commissione.

CAPO II - PRINCIPI

L'articolo 4 stabilisce i principi in materia di trattamento dei dati personali, che corrispondono a quelli di cui all'articolo 5 del regolamento (UE) 2016/679. Rispetto al regolamento (CE) n. 45/2001 esso aggiunge i nuovi principi di trasparenza, integrità e riservatezza.

L'articolo 5 si basa sull'articolo 6 del regolamento (UE) 2016/679 e stabilisce i criteri per il trattamento lecito, con la sola eccezione del criterio del legittimo interesse del titolare del trattamento che non è applicabile al settore pubblico e pertanto non si dovrebbe applicare alle

istituzioni e agli organi dell'Unione. L'articolo 5 mantiene i criteri già stabiliti dall'articolo 5 del regolamento (CE) n. 45/2001.

L'articolo 6 chiarisce le condizioni del trattamento per un'altra finalità compatibile in linea con l'articolo 6, paragrafo 4, del regolamento (UE) 2016/679. Rispetto all'articolo 6 del regolamento (CE) n. 45/2001 la nuova disposizione prevede una flessibilità e una certezza del diritto maggiori per quanto riguarda l'ulteriore trattamento per finalità compatibili.

L'articolo 7 chiarisce, conformemente all'articolo 7 del regolamento (UE) 2016/679, le condizioni alle quali il consenso è valido come base giuridica ai fini di un trattamento lecito.

L'articolo 8 stabilisce, in linea con l'articolo 8 del regolamento (UE) 2016/679, ulteriori condizioni per la liceità del trattamento dei dati personali di un minore in relazione ai servizi della società dell'informazione diretti ai minori. Esso fissa a 13 anni l'età minima per il consenso valido del minore.

L'articolo 9 stabilisce, in conformità all'articolo 8 del regolamento (CE) n. 45/2001, norme che prevedono un livello specifico di protezione per la trasmissione di dati personali a destinatari diversi dalle istituzioni e dagli organi dell'Unione, stabiliti nell'Unione e soggetti al regolamento (UE) 2016/679 o alla direttiva (UE) 2016/680. Esso chiarisce che, quando dà origine alla trasmissione, il titolare del trattamento dovrebbe dimostrare la necessità e la proporzionalità della trasmissione.

Sulla base dell'articolo 9 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 10 del regolamento (CE) n. 45/2001, l'articolo 10 stabilisce il divieto generale di trattamento di categorie particolari di dati personali e le eccezioni a questa regola generale.

In conformità all'articolo 10 del regolamento (UE) 2016/679 e in linea con l'articolo 10, paragrafo 5, del regolamento (CE) n. 45/2001, l'articolo 11 stabilisce le condizioni per il trattamento dei dati personali relativi alle condanne penali e ai reati.

In conformità all'articolo 11 del regolamento (UE) 2016/679, l'articolo 12 chiarisce gli obblighi di informazione del titolare del trattamento nei confronti dell'interessato e stabilisce che se i dati personali che tratta non gli consentono di identificare una persona fisica, il titolare del trattamento non dovrebbe avere l'obbligo di 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.

Sulla base dell'articolo 89, paragrafo 1, del regolamento (UE) 2016/679, l'articolo 13 stabilisce le norme sulle garanzie relative al trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

CAPO III - DIRITTI DELL'INTERESSATO

Sezione 1 – Trasparenza e modalità

Sulla base dell'articolo 12 del regolamento (UE) 2016/679, l'articolo 14 introduce l'obbligo in capo ai titolari del trattamento di fornire informazioni trasparenti, facilmente accessibili e comprensibili, e prevedere le procedure e i meccanismi che permettano all'interessato di esercitare i propri diritti, compresi, se del caso, i mezzi per introdurre le richieste per via elettronica, l'obbligo di rispondere entro un termine determinato e di motivare un eventuale rifiuto. Poiché le istituzioni e gli organi dell'Unione non dovrebbero applicare in nessun caso contributi spese relativi ai costi amministrativi per fornire informazioni, tale possibilità non è stata ripresa dal regolamento (UE) 2016/679.

Sezione 2 – Informazioni e accesso ai dati

L'articolo 15 precisa gli obblighi di informazione del responsabile del trattamento nei confronti dell'interessato qualora i dati siano raccolti presso l'interessato, sulla base dell'articolo 13 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 11 del regolamento (CE) n. 45/2001, ossia le informazioni da fornire all'interessato, compreso il periodo di conservazione, il diritto di proporre reclamo e i trasferimenti internazionali.

Sulla base dell'articolo 14 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 12 del regolamento (CE) n. 45/2001, l'articolo 16 precisa che il titolare del trattamento ha l'obbligo di informare l'interessato, qualora i dati personali non siano stati ottenuti presso l'interessato, della fonte da cui hanno origine i dati personali. Tale articolo mantiene le deroghe previste dal regolamento (UE) 2016/679, ad esempio l'obbligo viene meno se l'interessato dispone già delle informazioni; se comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato da parte del titolare del trattamento; se i dati personali devono rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o se la registrazione o la comunicazione sono espressamente previsti per legge. Ciò potrebbe avvenire, ad esempio, nei procedimenti avviati dai servizi competenti in materia di sicurezza sociale o sanità pubblica.

L'articolo 17 stabilisce, conformemente all'articolo 15 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 13 del regolamento (CE) n. 45/2001, norme sul diritto di accesso dell'interessato ai propri dati personali e aggiunge nuovi elementi, quali l'obbligo di informare gli interessati del periodo di conservazione, dei diritti di rettifica e cancellazione e di proporre reclamo.

Sezione 3 – Rettifica e cancellazione

Sulla base dell'articolo 16 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 14 del regolamento (CE) n. 45/2001, l'articolo 18 stabilisce il diritto di rettifica dell'interessato.

In linea con l'articolo 17 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 16 del regolamento (CE) n. 45/2001, l'articolo 19 stabilisce il diritto dell'interessato all'oblio e alla cancellazione. Esso prevede le condizioni del diritto all'oblio, compreso l'obbligo del responsabile del trattamento che abbia pubblicato dati personali di informare i terzi della richiesta dell'interessato di cancellare qualsiasi link verso tali dati, copia o riproduzione.

L'articolo 20 introduce il diritto alla limitazione di trattamento in determinati casi, evitando il termine ambiguo "blocco", utilizzato nel regolamento (CE) n. 45/2001, e garantendo la coerenza con la nuova terminologia dell'articolo 18 del regolamento (UE) 2016/679.

In linea con l'articolo 19 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 17 del regolamento (CE) n. 45/2001, l'articolo 21 stabilisce l'obbligo del titolare del trattamento di comunicare ai destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni dei dati personali o le eventuali limitazioni salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento deve inoltre comunicare all'interessato tali destinatari qualora l'interessato lo richieda.

In linea con l'articolo 20 del regolamento (UE) 2016/679, l'articolo 22 introduce il diritto alla portabilità dei dati dell'interessato, ossia il diritto di ricevere i dati personali che lo riguardano che ha fornito a un titolare del trattamento o di ottenere la trasmissione diretta di tali dati personali a un altro titolare del trattamento, se tecnicamente fattibile. Come presupposto e al fine di migliorare l'accesso dell'interessato ai dati personali che lo riguardano, detto articolo prevede il diritto di ottenere tali dati dal titolare del trattamento in un formato strutturato, di

uso comune e leggibile da dispositivo automatico. Tale diritto si applica soltanto quando il trattamento si fonda sul consenso dell'interessato o su un contratto concluso da questi.

Sezione 4 – Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

Sulla base dell'articolo 21 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 18 del regolamento (CE) n. 45/2001, l'articolo 23 stabilisce il diritto di opposizione dell'interessato.

L'articolo 24 riguarda il diritto dell'interessato di non essere sottoposto a una misura basata unicamente sul trattamento automatizzato, compresa la profilazione, in linea con l'articolo 22 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 19 del regolamento (CE) n. 45/2001.

Sezione 5 – Limitazioni

L'articolo 25 consente limitazioni ai diritti dell'interessato stabiliti dagli articoli da 14 a 22 e dagli articoli da 34 a 38 e ai principi stabiliti dall'articolo 4 (nella misura in cui le disposizioni corrispondono ai diritti e agli obblighi previsti dagli articoli da 14 a 22). Tali limitazioni dovrebbero essere disposte da atti giuridici adottati sulla base dei trattati o dalle norme interne delle istituzioni e degli organi dell'Unione. Nel caso in cui la possibilità di tale limitazione non sia disposta negli atti giuridici adottati sulla base dei trattati o nelle norme interne delle istituzioni e degli organi dell'Unione, questi ultimi possono imporre una limitazione ad hoc se essa rispetta l'essenza dei diritti e delle libertà fondamentali e, in relazione a uno specifico trattamento, è una misura necessaria e proporzionata in una società democratica per salvaguardare uno o più degli obiettivi che consentono le limitazioni dei diritti dell'interessato. Tale approccio è conforme all'articolo 23 del regolamento (UE) 2016/679. Tuttavia, a differenza dell'articolo 23 del regolamento (UE) 2016/679 e in linea con l'articolo 20 del regolamento (CE) n. 45/2001, questa disposizione non prevede la possibilità di limitare il diritto di opposizione e il diritto di non essere sottoposto a decisioni che siano basate unicamente su un trattamento automatizzato. I requisiti per le limitazioni sono in linea con la Carta e la Convenzione europea dei diritti dell'uomo, come interpretate rispettivamente dalla Corte di giustizia dell'Unione europea e dalla Corte europea dei diritti dell'uomo.

CAPO IV - TITOLARE DEL TRATTAMENTO E RESPONSABILE DEL TRATTAMENTO

Sezione 1 – Obblighi generali

L'articolo 26 si basa sull'articolo 24 del regolamento (UE) 2016/679 e introduce il "principio di responsabilizzazione", descrivendo l'obbligo di responsabilità del titolare del trattamento di conformarsi al regolamento proposto e di dimostrare la conformità, anche adottando misure tecniche e organizzative adeguate e, se del caso, politiche interne e meccanismi atti ad assicurare tale conformità. L'articolo 24, paragrafo 3, del regolamento (UE) 2016/679 non è stato mantenuto in questa disposizione in quanto le istituzioni e gli organi dell'Unione non dovrebbero aderire a codici di condotta o meccanismi di certificazione.

In conformità all'articolo 25 del regolamento (UE) 2016/679, l'articolo 27 enuncia gli obblighi del titolare del trattamento derivanti dai principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita.

L'articolo 28 sui contitolari del trattamento si basa sull'articolo 26 del regolamento (UE) 2016/679 e chiarisce le responsabilità dei contitolari del trattamento – siano essi istituzioni o organi dell'Unione o meno – per quanto riguarda il loro rapporto interno e nei confronti

dell'interessato. Questa disposizione disciplina la situazione in cui tutti i contitolari del trattamento sono soggetti allo stesso regime giuridico (il regolamento proposto) e quella in cui alcuni sono soggetti al regolamento proposto e altri a un diverso strumento giuridico (regolamento (UE) 2016/679, direttiva (UE) 2016/680, direttiva (UE) 2016/681 e altri regimi specifici di protezione dei dati concernenti le istituzioni e gli organi dell'Unione).

L'articolo 29 si basa sull'articolo 28 del regolamento (UE) 2016/679 e sviluppa ulteriormente l'articolo 23 del regolamento (CE) n. 45/2001 per chiarire la posizione e gli obblighi del responsabile del trattamento, disponendo altresì che il responsabile del trattamento che violi il regolamento determinando le finalità e i mezzi del trattamento è considerato titolare del trattamento per il trattamento in questione.

L'articolo 30 sul trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento si basa sull'articolo 29 del regolamento (UE) 2016/679 e stabilisce il divieto per il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento e abbia accesso a dati personali, di 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.

L'articolo 31 si basa sull'articolo 30 del regolamento (UE) 2016/679 e introduce l'obbligo per i titolari e i responsabili del trattamento di conservare la documentazione delle operazioni effettuate sotto la propria responsabilità, invece della notificazione preventiva al GEPD richiesta dall'articolo 25 del regolamento (CE) n. 45/2001 e dell'iscrizione nel registro del responsabile della protezione dei dati. A differenza del regolamento (UE) 2016/679, questa disposizione non fa riferimento ai rappresentanti, in quanto le istituzioni dell'Unione non hanno rappresentanti e avranno sempre RPD. I riferimenti ai trasferimenti sulla base di deroghe per situazioni specifiche previste nel regolamento (UE) 2016/679 non sono state mantenute in quanto tali tipi di trasferimenti non sono contemplati dal regolamento proposto. L'obbligo di tenere un registro delle attività di trattamento può essere centralizzato a livello di un'istituzione o di un organo dell'Unione. In tali casi le istituzioni e gli organi dell'Unione hanno la possibilità di tenere i registri delle attività di trattamento sotto forma di registri accessibili al pubblico.

Sulla base dell'articolo 31 del regolamento (UE) 2016/679, l'articolo 32 chiarisce gli obblighi delle istituzioni e degli organi dell'Unione di cooperare con il GEPD.

Sezione 2 – Sicurezza dei dati personali e riservatezza delle comunicazioni elettroniche

In linea con l'articolo 32 del regolamento (UE) 2016/679 e sviluppando ulteriormente l'articolo 22 del regolamento (CE) n. 45/2001, l'articolo 33 pone l'obbligo in capo al titolare del trattamento di mettere in atto misure appropriate al fine di garantire la sicurezza del trattamento ed estende tale obbligo anche al responsabile del trattamento, indipendentemente dal contratto con il titolare del trattamento.

L'articolo 34 si basa sull'articolo 36 del regolamento (CE) n. 45/2001 e assicura la riservatezza delle comunicazioni elettroniche all'interno delle istituzioni e degli organi dell'Unione.

L'articolo 35 si basa sulle pratiche esistenti delle istituzioni e degli organi dell'Unione e protegge le informazioni relative alle apparecchiature terminali degli utenti finali che accedono ai siti web e alle applicazioni per dispositivi mobili a disposizione del pubblico delle istituzioni e degli organi dell'Unione in conformità al regolamento (UE) XXXX/XX [nuovo regolamento relativo alla vita privata e alle comunicazioni elettroniche], in particolare all'articolo 8.

L'articolo 36 si basa sull'articolo 38 del regolamento (CE) n. 45/2001 e protegge i dati conservati in elenchi pubblici e privati delle istituzioni e degli organi dell'Unione.

Gli articoli 37 e 38 introducono l'obbligo di notificare le violazioni dei dati personali in conformità agli articoli 33 e 34 del regolamento (UE) 2016/679.

Sezione 3 – Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

L'articolo 39 si basa sull'articolo 35 del regolamento (UE) 2016/679 e introduce l'obbligo per i titolari del trattamento e i responsabili del trattamento di eseguire una valutazione d'impatto sulla protezione dei dati prima di effettuare i trattamenti che potrebbero presentare un elevato rischio per i diritti e le libertà delle persone fisiche. Tale obbligo si applica in particolare alla valutazione sistematica e globale di aspetti personali relativi a persone fisiche, che si basa su un trattamento automatizzato, tra cui la profilazione, il trattamento su larga scala di categorie particolari di dati o la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

L'articolo 40 si basa sull'articolo 36 del regolamento (UE) 2016/679 e riguarda i casi in cui è obbligatorio ottenere l'autorizzazione del GEPD e consultarlo prima del trattamento. Tuttavia il primo paragrafo dell'articolo 40 riprende il considerando 94 del regolamento (UE) 2016/679 e si prefigge di chiarire la portata dell'obbligo di consultazione.

Sezione 4 – Informazioni e consultazione legislativa

L'articolo 41 stabilisce che le istituzioni e gli organi dell'Unione hanno l'obbligo di informare il GEPD quando elaborano misure amministrative e norme interne relative al trattamento di dati personali.

L'articolo 42 stabilisce che la Commissione ha l'obbligo di consultare il GEPD a seguito dell'adozione di proposte di atti legislativi e di raccomandazioni o proposte al Consiglio a norma dell'articolo 218 del TFUE e quando elabora atti delegati o di esecuzione che incidano sulla tutela dei diritti e delle libertà delle persone per quanto riguarda il trattamento dei dati personali. Qualora tali atti abbiano una particolare rilevanza ai fini della 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 le due autorità dovrebbero coordinare le proprie attività al fine di emettere un parere congiunto. Nei suddetti casi si applica un termine di 8 settimane per fornire una consulenza, con la possibilità di derogare in casi di urgenza o di opportunità, ad esempio quando la Commissione elabora atti delegati o di esecuzione.

Sezione 5 – Obbligo di rispondere ai rilievi

L'articolo 43 definisce l'obbligo dei titolari del trattamento e del responsabile del trattamento di rispondere ai rilievi quando il GEPD decide di sottoporre una questione alla loro attenzione.

Sezione 6 – Responsabile della protezione dei dati

L'articolo 44 si basa sull'articolo 37, paragrafo 1, lettera a), del regolamento (UE) 2016/679 e sull'articolo 24 del regolamento (CE) n. 45/2001 e prevede la designazione di un RPD obbligatorio per le istituzioni e gli organi dell'Unione.

L'articolo 45 si basa sull'articolo 38 del regolamento (UE) 2016/679 e sull'articolo 24 del regolamento (CE) n. 45/2001 per definire la funzione dell'RPD.

L'articolo 46 si basa sull'articolo 39 del regolamento (UE) 2016/679 e sull'articolo 24 del regolamento (CE) n. 45/2001 e sui punti 2 e 3 dell'allegato al regolamento (CE) n. 45/2001 per stabilire i compiti principali dell'RPD.

CAPO V - TRASFERIMENTI DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI

L'articolo 47 si basa sull'articolo 9 del regolamento (CE) n. 45/2001 e stabilisce, in conformità all'articolo 44 del regolamento (UE) 2016/679, il principio generale secondo cui la conformità alle altre disposizioni del regolamento proposto e alle condizioni stabilite nel capo V è obbligatoria per i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali, compresi i trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale.

L'articolo 48 stabilisce che un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale può avere luogo quando la Commissione ha deciso, a norma dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato e che i dati personali sono trasferiti unicamente per consentire l'espletamento dei compiti che rientrano nelle competenze del titolare del trattamento. I paragrafi 2 e 3 di questo articolo sono ripresi dall'articolo 9 del regolamento (CE) n. 45/2001 in quanto rappresentano elementi utili per monitorare il livello di protezione in paesi terzi e organizzazioni internazionali.

L'articolo 49 si basa sull'articolo 46 del regolamento (UE) 2016/679 e prevede che, in mancanza di una decisione di adeguatezza della Commissione, i trasferimenti a paesi terzi siano subordinati ad adeguate garanzie, in particolare clausole tipo di protezione dei dati e clausole contrattuali. Conformemente al regolamento (UE) 2016/679, i responsabili del trattamento diversi dalle istituzioni e dagli organi dell'Unione possono ricorrere a norme vincolanti d'impresa, codici di condotta e meccanismi di certificazione. Il paragrafo 4 di questo articolo, relativo l'obbligo delle istituzioni e degli organi dell'Unione di informare il GEPD delle categorie di casi in cui hanno applicato questo articolo, corrisponde all'articolo 9, paragrafo 8, del regolamento (CE) n. 45/2001 ed è mantenuto in considerazione della sua specificità. Il paragrafo 5 si basa sulla validità delle autorizzazioni esistenti stabilite dall'articolo 46, paragrafo 5, del regolamento (UE) 2016/679.

L'articolo 50 chiarisce, in conformità all'articolo 48 del regolamento (UE) 2016/679, che 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 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 capo V.

L'articolo 51 si basa sull'articolo 49 del regolamento (UE) 2016/679 e precisa e chiarisce le deroghe al trasferimento di dati. Ciò vale in particolare per i trasferimenti di dati richiesti e necessari per motivi di interesse pubblico rilevante, per esempio in caso di trasferimenti di dati internazionali che coinvolgono autorità garanti della concorrenza, amministrazioni fiscali o doganali oppure tra servizi competenti per la sicurezza sociale o per la gestione delle risorse alieutiche. Il paragrafo 5, sull'obbligo di informare il GEPD delle categorie di casi in cui le deroghe sono state utilizzate per un trasferimento, corrisponde all'articolo 9, paragrafo 8, del regolamento (CE) n. 45/2001.

L'articolo 52 si basa sull'articolo 50 del regolamento (UE) 2016/679 e stabilisce esplicitamente meccanismi di cooperazione internazionale per la protezione dei dati personali tra il GEDP, in cooperazione con la Commissione e il comitato europeo per la protezione dei dati, e le autorità di controllo dei paesi terzi.

CAPO VI - IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

L'articolo 53 si basa sull'articolo 41 del regolamento (CE) n. 45/2001 e concerne l'istituzione del GEDP.

L'articolo 54 si basa sull'articolo 42 del regolamento (CE) n. 45/2001 e sull'articolo 3 della decisione 1247/2002/CE e stabilisce le norme per la nomina del GEPD da parte del Parlamento europeo e del Consiglio. Esso fissa inoltre a cinque anni la durata del suo mandato.

L'articolo 55 si basa sull'articolo 43 del regolamento (CE) n. 45/2001 e sull'articolo 1 della decisione 1247/2002/CE e disciplina lo statuto e le condizioni generali di esercizio delle funzioni del GEPD e le sue risorse umane e finanziarie.

L'articolo 56 si basa sull'articolo 52 del regolamento (UE) 2016/679 e sull'articolo 44 del regolamento (CE) 45/2001 e precisa le condizioni per l'indipendenza del GEPD, tenendo conto della giurisprudenza della Corte di giustizia dell'Unione europea.

L'articolo 57 stabilisce, sulla base dell'articolo 45 del regolamento (CE) n. 45/2001, i doveri di segretezza del GEPD durante e dopo il mandato in merito alle informazioni riservate cui ha avuto accesso durante l'esercizio delle proprie funzioni.

L'articolo 58 si basa sull'articolo 57 del regolamento (UE) 2016/679 e sull'articolo 46 del regolamento (CE) n. 45/2001 e stabilisce i compiti del GEPD, compresi il trattamento dei reclami e il compimento dei relativi accertamenti, e la promozione della consapevolezza del pubblico rispetto a rischi, norme, garanzie e diritti.

L'articolo 59 si basa sull'articolo 58 del regolamento (UE) 2016/679 e sull'articolo 47 del regolamento (CE) n. 45/2001 e stabilisce le competenze del GEPD.

L'articolo 60 si basa sull'articolo 59 del regolamento (UE) 2016/679 e sull'articolo 48 del regolamento (CE) n. 45/2001 e fissa gli obblighi del GEDP di redigere un rapporto annuale sulle attività svolte.

CAPO VII - COOPERAZIONE E COERENZA

L'articolo 61 si basa sull'articolo 61 del regolamento (UE) 2016/679 e sull'articolo 46, lettera f), del regolamento (CE) n. 45/2001 e introduce norme esplicite sulla cooperazione del GEPD con le autorità nazionali di controllo.

L'articolo 62 stabilisce gli obblighi del GEPD quando altri atti dell'Unione si riferiscono a questo articolo nell'ambito del controllo coordinato con le autorità di controllo nazionali. Esso mira ad attuare un unico modello di controllo coordinato. Tale modello potrebbe essere utilizzato per il controllo coordinato di grandi sistemi informatici, quali Eurodac, il sistema di informazione Schengen II, il sistema di informazione visti, il sistema di informazione doganale o il sistema di informazione del mercato interno, ma anche per il controllo di alcune agenzie dell'Unione, quali Europol, quando si stabilisce un modello specifico di cooperazione tra il GEPD e le autorità nazionali. Il comitato europeo per la protezione dei dati dovrebbe costituire un forum unico per garantire un controllo coordinato efficace sistematico.

CAPO VIII - RICORSI GIURISDIZIONALI, RESPONSABILITÀ E SANZIONI

L'articolo 63 si basa sull'articolo 77 del regolamento (UE) 2016/679 e sull'articolo 32 del regolamento (CE) n. 45/2001 e stabilisce il diritto di qualunque interessato di proporre reclamo al GEPD. Esso prevede inoltre l'obbligo del GEPD di trattare i reclami e comunicarne all'interessato il progresso e l'esito del reclamo entro un termine di tre mesi dopodiché il reclamo si considererà rigettato.

L'articolo 64 mantiene l'articolo 32, paragrafo 1, del regolamento (CE) n. 45/2001 e stabilisce la competenza della Corte di giustizia dell'Unione europea a conoscere delle controversie

relative alle disposizioni del regolamento proposto, incluse le azioni per risarcimento del danno.

L'articolo 65 disciplina il diritto al risarcimento dei danni materiali e immateriali, fatte salve le condizioni stabilite dai trattati, comprese quelle in materia di responsabilità.

L'articolo 66 si basa sull'articolo 83 del regolamento (UE) 2016/679 e attribuisce al GEPD il potere di imporre sanzioni amministrative pecuniarie alle istituzioni e agli organi dell'Unione, come sanzione di ultima istanza e soltanto qualora le istituzioni e gli organi dell'Unione non rispettino un ordine del GEPD di cui all'articolo 59, paragrafo 2, lettere da a) ad h) e j). L'articolo precisa inoltre i criteri per fissare l'ammontare della sanzione pecuniaria in ogni singolo caso, mentre i massimali annui si ispirano all'ammontare delle sanzioni pecuniarie applicate in alcuni Stati membri.

In linea con l'articolo 80, paragrafo 1, del regolamento (UE) 2016/679, l'articolo 67 autorizza alcuni organismi, organizzazioni o associazioni a proporre reclamo per conto dell'interessato.

In linea con l'articolo 33 del regolamento (CE) n. 45/2001, l'articolo 68 stabilisce norme specifiche intese a proteggere il personale dell'Unione che, senza seguire la via gerarchica, propone reclamo al GEPD per un'asserita violazione delle disposizioni del regolamento proposto.

L'articolo 69 si basa sull'articolo 49 del regolamento (CE) n. 45/2001 e disciplina le sanzioni applicabili ai funzionari o altri agenti dell'Unione europea che non assolvano agli obblighi previsti dal presente regolamento.

CAPO IX - ATTI DI ESECUZIONE

L'articolo 70 dispone la procedura di comitato necessaria per il conferimento delle competenze di esecuzione alla Commissione, nei casi in cui, conformemente all'articolo 291 del TFUE, sono necessarie condizioni uniformi di esecuzione degli atti giuridicamente vincolanti dell'Unione. Si applica la procedura d'esame.

CAPO X - DISPOSIZIONI FINALI

L'articolo 71 abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE e dispone che i riferimenti ai due strumenti abrogati sono intesi come riferimenti al futuro regolamento.

L'articolo 72 specifica che il futuro regolamento non inciderà sugli attuali mandati del garante europeo della protezione dei dati e del garante aggiunto e che l'articolo 54, paragrafi 4, 5 e 7, e gli articoli 56 e 57 del regolamento si applicano all'attuale garante aggiunto fino al termine del suo mandato, ossia fino al 5 dicembre 2019.

L'articolo 73 fissa il 25 maggio 2018 come data di entrata in vigore del futuro regolamento al fine di assicurare la coerenza con la data di applicazione del regolamento (UE) 2016/679.

2017/0002 (COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché la

libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE

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[10],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea ("Carta") e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea ("TFUE") stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

(2) Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio[11] 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. Tuttavia esso non si applica 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[12] e la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio[13]. 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.

---

10 GU C [...] del [...], pag. [...].

11 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).

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

13 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).

(4) Il regolamento (UE) 2016/679 sottolinea la necessità di procedere agli opportuni adeguamenti del regolamento (CE) n. 45/2001 per offrire un quadro di protezione dei dati solido e coerente nell'Unione e per consentire l'applicazione di quest'ultimo contemporaneamente al regolamento (UE) 2016/679.

(5) È nell'interesse di un approccio coerente alla protezione dei dati in tutta l'Unione e alla libera circolazione dei dati personali all'interno dell'Unione allineare per quanto possibile le norme sulla protezione dei dati per le istituzioni e gli organi dell'Unione a quelle adottate per il settore pubblico degli Stati membri. Quando le disposizioni del presente regolamento si basano sullo stesso concetto su cui si basano le disposizioni del regolamento (UE) 2016/679, 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. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.

(8) 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 del TFUE. Il presente regolamento dovrebbe pertanto applicarsi alle agenzie dell'Unione che svolgono attività nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia soltanto nella misura in cui il diritto dell'Unione applicabile a tali agenzie non preveda norme specifiche sul trattamento dei dati personali.

(9) 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 promuovere 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 le agenzie dell'Unione che svolgono attività nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia e le autorità competenti degli Stati membri, è opportuno che le norme per la protezione e la libera circolazione dei dati

personali operativi trattati da tali agenzie dell'Unione si basino sui principi su cui si fonda il presente regolamento e siano coerenti con la direttiva (UE) 2016/680.

(10) Laddove l'atto istitutivo di un'agenzia dell'Unione che svolge attività rientranti nell'ambito di applicazione del titolo V, capi 4 e 5, del trattato stabilisca un regime di protezione dei dati indipendente per quanto riguarda il trattamento dei dati personali operativi, tale regime non dovrebbe essere interessato dal presente regolamento. Tuttavia, in conformità all'articolo 62 della direttiva (UE) 2016/680, la Commissione, entro il 6 maggio 2019, dovrebbe riesaminare gli atti dell'Unione che disciplinano il trattamento da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica e formulare, ove opportuno, le proposte necessarie per modificarli in modo da garantire un approccio coerente alla protezione dei dati personali nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia.

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

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

(13) 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.

(14) Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra

dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

(15) 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 con riguardo 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 o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

(16) Conformemente al principio di responsabilizzazione, quando le istituzioni e gli organi dell'Unione trasmettono dati personali al loro interno o ad altre istituzioni e altri organi dell'Unione, dovrebbero verificare se tali dati personali sono necessari per il legittimo esercizio dei compiti che rientrano nelle competenze del destinatario quando il destinatario non è il titolare del trattamento. 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 il trattamento e la competenza del destinatario, e dovrebbe 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.

(17) 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 all'obbligo

legale al quale è soggetto il titolare del trattamento o su qualsiasi altra base legittima di cui al 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.

(18) Il diritto dell'Unione, comprese le norme interne di cui al presente regolamento, dovrebbe essere chiaro e preciso, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei diritti dell'uomo.

(19) 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 dovrebbe, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

(20) 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[14] 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.

(21) 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 vengono utilizzati servizi forniti 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 quando il trattamento dei dati personali si basa sul consenso.

(22) I destinatari stabiliti nell'Unione e soggetti al regolamento (UE) 2016/679 e alla direttiva (UE) 2016/680 che desiderano che le istituzioni e gli organi dell'Unione trasmettano loro dati personali dovrebbero dimostrare che la trasmissione è necessaria per conseguire il loro obiettivo, è proporzionata e si limita a quanto necessario per il conseguimento di quell'obiettivo. Nel rispetto del principio della trasparenza, le istituzioni e gli organi dell'Unione dovrebbero dimostrare tale necessità quando danno origine alla trasmissione.

(23) Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini «origine razziale» nel presente regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte. Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando saranno trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. 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 se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.

(24) Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso

[14] 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).

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[15]: tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi.

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

(26) Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici dovrebbe essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie dovrebbero assicurare che siano state predisposte misure tecniche e organizzative al fine di garantire, in particolare, il principio della minimizzazione dei dati. L'ulteriore trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è da effettuarsi quando il titolare del trattamento ha valutato la fattibilità di conseguire tali finalità trattando dati personali che non consentono o non consentono più di identificare l'interessato, purché esistano garanzie adeguate (come ad esempio la pseudonimizzazione dei dati personali). Le istituzioni e gli organi dell'Unione dovrebbero prevedere garanzie adeguate nel diritto dell'Unione, ed eventualmente nelle norme interne, per il trattamento di dati personali a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici.

(27) È opportuno prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici. Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

---

15 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).

(28) 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 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone dovrebbero essere leggibili da dispositivo automatico.

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

(30) 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.

(31) 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 dati 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 indipendentemente dal fatto che non sia più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

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

(33) 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.

(34) 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.

(35) 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.

(36) L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali 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 che comportano misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni.

(37) Gli atti giuridici adottati sulla base dei trattati o le norme interne delle istituzioni e degli organi dell'Unione 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 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, delle attività di prevenzione, indagine e perseguimento di reati o dell'esecuzione di sanzioni penali, tra cui la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, ivi comprese 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 un interesse economico o finanziario rilevante dell'Unione o di uno Stato membro, 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.

Qualora gli atti giuridici adottati sulla base dei trattati o le norme interne non prevedano una limitazione, le istituzioni e gli organi dell'Unione possono, in casi specifici, imporre una limitazione ad hoc concernente specifici principi e i diritti dell'interessato se tale limitazione rispetta l'essenza dei diritti e delle libertà fondamentali e, in relazione a un trattamento specifico, è necessaria e proporzionata in una società democratica per salvaguardare uno o più degli obiettivi di cui al paragrafo 1. La limitazione dovrebbe essere comunicata al responsabile della protezione dei dati. Tutte le limitazioni dovrebbero essere conformi alla Carta e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

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

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

(40) 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 ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.

(41) Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. L'applicazione da parte 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 dovrebbe essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato. Il titolare del trattamento e il responsabile del trattamento 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.

(42) 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. Sarebbe necessario obbligare le istituzioni e gli organi dell'Unione 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. È opportuno che le istituzioni e gli organi dell'Unione siano in grado di istituire un registro centrale in cui registrare le proprie attività di trattamento. Per motivi di trasparenza, dovrebbero poter rendere tale registro pubblico.

(43) Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere. Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale.

(44) 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, proteggere le informazioni relative alle apparecchiature terminali degli utenti finali che accedono ai loro siti web e alle applicazioni per dispositivi mobili a disposizione del pubblico in ottemperanza al regolamento (UE) XXXX/XX [nuovo regolamento relativo alla vita privata e alle comunicazioni elettroniche] e proteggere i dati personali in elenchi di utenti.

(45) Una violazione dei dati personali potrebbe, se non affrontata in modo adeguato e tempestivo, 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 notificare la violazione dei dati personali al garante europeo della protezione dei dati, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni 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.

(46) Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con il garante europeo della

protezione dei dati e nel rispetto degli orientamenti impartiti da questo o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge.

(47) 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, che a sua volta terrà un registro dei trattamenti notificati. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includerebbero, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale. In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento.

(48) 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 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.

(49) Il garante europeo della protezione dei dati dovrebbe essere informato circa le misure amministrative e le norme interne delle istituzioni e degli organi dell'Unione che prevedono il trattamento di dati personali, stabiliscono le condizioni per le limitazioni dei diritti dell'interessato o fissano garanzie adeguate per i diritti dell'interessato, al fine di garantire la conformità del trattamento previsto al presente regolamento e, in particolare, attenuare i rischi per l'interessato.

(50) Il regolamento (UE) 2016/679 istituisce 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 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 del TFUE e a seguito dell'adozione di raccomandazioni e proposte relative ad accordi con paesi terzi e organizzazioni internazionali di cui all'articolo 218 del 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 nei casi in cui il regolamento (UE) 2016/679 stabilisce 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 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.

(51) Un responsabile della protezione dei dati dovrebbe provvedere, all'interno di ciascuna istituzione o organo dell'Unione, all'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 e dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati dovrebbero poter adempiere le funzioni e i compiti loro incombenti in maniera indipendente.

(52) 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, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali potrebbero essere effettuati soltanto nel pieno rispetto del presente regolamento. Il trasferimento potrebbe aver luogo soltanto se, fatte salve le altre disposizioni del presente regolamento, il titolare del trattamento o il responsabile del trattamento rispetta le condizioni stabilite dalle disposizioni del presente regolamento in relazione al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

(53) A norma dell'articolo 45 del regolamento (UE) 2016/679 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.

(54) 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 rispetto ai principi generali in materia di trattamento dei dati personali e ai principi di protezione dei dati fin dalla progettazione e di protezione dei dati di default. I trasferimenti possono essere effettuati anche da 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.

(55) 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.

(56) 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.

(57) 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 legittimo interesse. 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 legittimo interesse, i dati possono essere trasferiti soltanto se tali persone lo richiedono o ne sono destinatarie, tenendo pienamente conto degli interessi e dei diritti fondamentali dell'interessato.

(58) 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.

(59) 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.

(60) 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 dell'Unione, incluso 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 altre autorità di controllo della protezione dei dati affinché possano scambiare informazioni con le loro controparti internazionali.

(61) L'istituzione, con 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 con riguardo al trattamento dei loro dati personali. Il presente regolamento dovrebbe rafforzarne e chiarirne ulteriormente il ruolo e l'indipendenza.

(62) 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 degli Stati membri, 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 dell'Unione europea 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, e 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.

(63) 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.

(64) 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.

(65) 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. Inoltre, il garante europeo della protezione dei dati è l'autorità di controllo di Europol e un modello specifico di cooperazione con le autorità di controllo nazionali è istituito 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 sistematico.

(66) 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 dell'Unione europea, in conformità ai 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.

(67) 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 nel trattato.

(68) 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 pecuniarie dovrebbero mirare a sanzionare l'istituzione o l'organo – 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, indicare i limiti massimi e i criteri per prevedere la relativa sanzione amministrativa pecuniaria. 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 e delle relative conseguenze, nonché delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione. Quando impone una sanzione amministrativa pecuniaria a 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 dell'Unione europea.

(69) 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 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.

(70) Il funzionario o altro agente dell'Unione che non assolva agli obblighi previsti dal presente regolamento è passibile di provvedimenti disciplinari o di altro genere, secondo le norme e le procedure previste dallo statuto dei funzionari dell'Unione europea o dal regime applicabile agli altri agenti dell'Unione.

(71) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione ove previsto dal presente regolamento. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio[16]. 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 in cui è richiesta la consultazione preventiva del garante europeo della protezione dei dati da parte dei titolari del trattamento che effettuano un trattamento 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.

(72) È opportuno proteggere le informazioni riservate raccolte dalle autorità statistiche nazionali e dell'Unione per la produzione di statistiche ufficiali europee e nazionali. Le statistiche europee dovrebbero essere sviluppate, prodotte e diffuse conformemente ai principi statistici di cui all'articolo 338, paragrafo 2, del TFUE. Il regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio[17] fornisce ulteriori specificazioni in merito al segreto statistico per quanto riguarda le statistiche europee.

(73) Il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE dovrebbero essere abrogati. I riferimenti al regolamento e alla direttiva abrogati dovrebbero intendersi fatti al presente regolamento.

(74) 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

---

16 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).

17 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).

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.

(75) In conformità 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 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 tale obiettivo, in ottemperanza all'articolo 5, paragrafo 4, del trattato sull'Unione europea.

(76) 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 XX.XX.XX,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1
Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché norme relative alla libera circolazione dei dati personali tra tali istituzioni, organi, uffici e agenzie o verso destinatari stabiliti nell'Unione e soggetti al regolamento (UE) 2016/679[18] o alle disposizioni della legislazione nazionale adottata a norma della direttiva (UE) 2016/680[19].

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 (GEPD) sorveglia l'applicazione delle disposizioni del presente regolamento a tutti i trattamenti effettuati da un'istituzione o un organo dell'Unione.

---

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

[19] 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).

Articolo 2
Ambito d'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, nella misura in cui detto trattamento è effettuato nell'esercizio di attività che rientrano in tutto o in parte nell'ambito di applicazione del diritto dell'Unione.

2. Il presente regolamento si applica al trattamento di dati personali, interamente o parzialmente automatizzato, nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi.

Articolo 3
Definizioni

1. Ai fini del presente regolamento si applicano le seguenti definizioni:

   (a) le definizioni di cui al regolamento (UE) 2016/679, ad eccezione della definizione di "titolare del trattamento" di cui all'articolo 4, punto 7, di tale regolamento;

   (b) la definizione di "comunicazione elettronica" di cui all'articolo 4, punto 2, lettera a), del regolamento (UE) XX/XXXX [regolamento relativo alla vita privata e alle comunicazioni elettroniche];

   (c) le definizioni di "rete di comunicazione elettronica" e di "utente finale" di cui all'articolo 2, punti 1 e 14, della direttiva 00/0000/UE [direttiva che istituisce il codice europeo delle comunicazioni elettroniche] rispettivamente;

   (d) la definizione di "apparecchiature terminali" di cui all'articolo 1, punto 1, della direttiva 2008/63/CE[20] della Commissione.

2. Ai fini del presente regolamento si applicano inoltre le seguenti definizioni:

   (a) "istituzioni e organi dell'Unione": le istituzioni, gli organi, gli uffici e le agenzie dell'Unione istituiti dal trattato sull'Unione europea, dal trattato sul funzionamento dell'Unione europea o dal trattato Euratom oppure sulla base di tali trattati;

   (b) "titolare del trattamento": l'istituzione, l'organo, l'ufficio o l'agenzia 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 del 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;

   (c) "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;

[20] 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).

(d) “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.

CAPO II

PRINCIPI

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 inesatti o incompleti rispetto alle finalità per le quali sono raccolti o successivamente trattati (“esattezza”);

e) conservati in una forma che consenta l’identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente 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 di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita 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. I compiti di cui al paragrafo 1, lettera a), sono stabiliti 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 un atto legislativo 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, diversi dalle istituzioni e dagli organi dell'Unione, stabiliti nell'Unione e soggetti al regolamento (UE) 2016/679 o alla direttiva (UE) 2016/680.

1. Fatti salvi gli articoli 4, 5, 6 e 10, i dati personali possono essere trasmessi a destinatari stabiliti nell'Unione e soggetti al regolamento (UE) 2016/679 o alla legislazione nazionale adottata a norma della direttiva (UE) 2016/680 solo se il destinatario dimostra che:

   a) i dati sono necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; oppure

   b) la trasmissione dei dati è necessaria e proporzionata alle finalità cui è destinata e non sussistono motivi per presumere che i diritti, le libertà e i legittimi interessi dell'interessato possano subire pregiudizio.

2. Ove la trasmissione a norma del presente articolo avvenga su iniziativa del titolare del trattamento, quest'ultimo 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).

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 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 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 dell'Unione europea 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;

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.

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, può avvenire solo se autorizzato dal diritto dell'Unione, che può comprendere norme interne 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 38 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 al fine 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 ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

4. Se non ottempera alla richiesta dell'interessato, il titolare del trattamento informa l'interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo 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 38 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 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 49, 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 49, 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 dal diritto dell'Unione; oppure

d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione.

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 49 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 ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Articolo 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 ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

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

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 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 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 all'altro, 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 34 e 35, 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 dei legittimi interessi 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 i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 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 dei legittimi interessi 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 34 e 38, 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 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. Se non è prevista alcuna limitazione da un atto giuridico adottato sulla base dei trattati o da una norma interna conformemente al paragrafo 1, le istituzioni e gli organi dell'Unione possono limitare l'applicazione degli articoli da 14 a 22 e degli articoli 34 e 38, 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, in relazione a un trattamento specifico, e sia una misura necessaria e proporzionata in una società democratica per salvaguardare uno o più degli obiettivi di cui al paragrafo 1. La limitazione è comunicata al responsabile della protezione dei dati competente.

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, 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, 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 sufficientemente chiare, precise e oggetto di una pubblicazione adeguata.

6. Qualora si applichi una delle limitazioni di cui ai paragrafi 1 o 2, 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 ai paragrafi 1 e 2 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 e all'articolo 46, paragrafo 2, può essere rinviata, omessa o negata qualora annulli l'effetto della limitazione imposta in forza dei paragrafi 1 o 2.

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 è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

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

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.

Articolo 28
Contitolari del trattamento

1. Allorché un'istituzione o un organo dell'Unione e uno o più titolari del trattamento, che possono essere istituzioni od organi dell'Unione o meno, 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 siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

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

3. L'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun contitolare del trattamento, tenendo conto dei loro ruoli stabiliti nelle disposizioni dell'accordo di cui al paragrafo 1.

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 nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

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

   c) 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 40, 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 70, 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 e 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. Le istituzioni e gli organi dell'Unione possono decidere di conservare i loro registri delle attività di trattamento in un registro centrale. In tal caso, possono decidere anche di rendere il registro 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 E RISERVATEZZA DELLE COMUNICAZIONI ELETTRONICHE

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 del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
   (a) la pseudonimizzazione e la cifratura dei dati personali;
   (b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   (c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   (d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
3. 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.

Articolo 34
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 35
Protezione delle informazioni relative alle apparecchiature terminali degli utenti finali

Le istituzioni e gli organi dell'Unione proteggono le informazioni relative alle apparecchiature terminali degli utenti finali che accedono ai loro siti internet e applicazioni mobili disponibili al pubblico conformemente al regolamento (UE) XX/XXXX [nuovo regolamento relativo alla vita privata e alle comunicazioni elettroniche], in particolare l'articolo 8.

Articolo 36
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.

Articolo 37
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 ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica 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 ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

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

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

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

   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 38
Comunicazione di una violazione dei dati personali all'interessato

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

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 37, 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

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. 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.

7. 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.

8. 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.

9. 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 non si applicano, salvo se il diritto dell'Unione stabilisca altrimenti.

10. 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 termini di tecnologie disponibili e 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 59. 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;

   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 un compito di interesse pubblico, tra cui il trattamento di tali dati con riguardo alla protezione sociale e alla sanità pubblica.

SEZIONE 4

INFORMAZIONI E CONSULTAZIONE LEGISLATIVA

Articolo 41
Informazioni

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 che interessino un'istituzione o un organo dell'Unione singolarmente o congiuntamente.

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 del TFUE e durante la stesura di atti delegati o di esecuzione, che incidono 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. Il parere di cui ai paragrafi 1 e 2 è fornito 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 5

OBBLIGO DI RISPONDERE AI RILIEVI

Articolo 43
Obbligo di rispondere ai rilievi

Qualora il garante europeo della protezione dei dati eserciti i poteri di cui all'articolo 59, 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.

SEZIONE 6

RESPONSABILE DELLA PROTEZIONE DEI DATI

Articolo 44
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 46.
4. Il responsabile della protezione dei dati può essere un membro del personale dell'istituzione o dell'organo dell'Unione oppure assolvere 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 45
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 46 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 dei suoi 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 e da qualsiasi persona, senza seguire la via gerarchica, su qualsiasi aspetto riguardante l'interpretazione o l'applicazione del presente regolamento. Nessuno deve subire pregiudizio per una questione portata all'attenzione del responsabile della protezione dei dati competente e riguardante una 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 solo con il consenso del garante europeo della protezione dei dati, se non soddisfa più le condizioni richieste per l'esercizio delle sue funzioni.

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 46
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 e 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, compresi 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 37 e 38;

   (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 e 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 e, 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.

2. Il responsabile della protezione dei dati può formulare raccomandazioni per il miglioramento concreto della protezione dei dati al titolare del trattamento e al responsabile del trattamento 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 o di qualsiasi persona, indagare sulle questioni e sui fatti direttamente collegati con l'esercizio delle sue funzioni e 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 potranno in particolare riguardare 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 47
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 48
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, che è garantito un livello di protezione adeguato nel paese terzo, in un territorio o in uno o più settori specifici all'interno del paese terzo o all'interno dell'organizzazione internazionale, e che i dati personali sono 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 il paese terzo o l'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, paragrafi 3 e 5, del regolamento (UE) 2016/679, che un paese terzo o

un'organizzazione internazionale assicura o non assicura più un livello di protezione adeguato.

Articolo 49
Trasferimento soggetto a garanzie adeguate

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679, 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 70, 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 70, paragrafo 2;

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

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 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.

5. 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 vengono modificate, sostituite o abrogate, se necessario, dal garante europeo della protezione dei dati.

Articolo 50
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 51
Deroghe in specifiche situazioni

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 o di garanzie adeguate ai sensi dell'articolo 49, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

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

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

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

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

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

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

   (g) il trasferimento sia 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 legittimo interesse, ma solo purché sussistano i requisiti per la consultazione previsti dalla normativa dell'Unione.

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

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

4. 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.

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 52
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

IL GARANTE EUROPEO DELLA PROTEZIONE DEI DATI

Articolo 53
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, riguardo 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 riguardo 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 58 ed esercita i poteri attribuitigli dall'articolo 59.

Articolo 54
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. 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 elaborato dalla Commissione da cui viene scelto il garante europeo della protezione dei dati è composto da personalità che offrono ogni garanzia di indipendenza e che possiedono un'esperienza e delle competenze notorie per l'esercizio delle funzioni di garante europeo della protezione dei dati, come ad esempio il far parte o l'aver fatto parte delle autorità di controllo di cui all'articolo 41 del regolamento (UE) 2016/679.

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 dell'Unione europea 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 55

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 dell'Unione europea 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 IX del bilancio generale dell'Unione europea.

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 alle sue istruzioni. Il numero di detti funzionari e agenti è stabilito ogni anno nell'ambito della procedura di bilancio.

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 europea.

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

Articolo 56
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 57
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 58
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 e degli altri atti dell'Unione relativi alla tutela delle persone fisiche riguardo al trattamento dei dati personali da parte di un'istituzione o di un organo dell'Unione, fatta eccezione per il trattamento di dati personali da parte della Corte di giustizia dell'Unione europea 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 degli Stati membri;
   (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 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 con riguardo 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 49, 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 istituito dall'articolo 68 del regolamento (UE) 2016/679;

(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 49, paragrafo 3;

(o) tiene registri interni delle violazioni del presente regolamento e delle misure adottate in conformità dell'articolo 59, 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 59
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 o il diritto processuale degli Stati membri.

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) rivolgersi al titolare del trattamento o al responsabile del trattamento in questione e, se necessario, al Parlamento europeo, al Consiglio e alla Commissione;

(d) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;

(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, 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 dell'istituzione o dell'organo dell'Unione di una delle misure di cui al presente paragrafo e 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 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;

(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 49, paragrafo 2, lettera c);

(e) autorizzare le clausole contrattuali di cui all'articolo 49, paragrafo 3, lettera a);

(f) autorizzare gli accordi amministrativi di cui all'articolo 49, paragrafo 3, lettera b).

4. 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.

5. Il garante europeo della protezione dei dati ha il potere di adire la Corte di giustizia dell'Unione europea alle condizioni previste dal trattato e di intervenire nelle cause dinanzi alla Corte di giustizia dell'Unione europea.

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 alle altre istituzioni e agli altri organi dell'Unione, che possono formulare osservazioni in vista dell'eventuale discussione dello stesso presso il Parlamento europeo.

CAPO VII

COOPERAZIONE E COERENZA

Articolo 61
Cooperazione con le autorità di controllo nazionali

Il garante europeo per la protezione dei dati coopera con le autorità di controllo istituite ai sensi dell'articolo 41 del regolamento (UE) 2016/679 e dall'articolo 51 della direttiva (UE) 2016/680 (in seguito "autorità di controllo nazionali") e con l'autorità comune di controllo istituita dall'articolo 25 della decisione 2009/917/GAI del Consiglio[21] nella misura necessaria all'esecuzione delle rispettive funzioni, in particolare fornendosi reciprocamente informazioni pertinenti, chiedendo alle autorità di controllo nazionali di esercitare i loro poteri o rispondendo alle richieste formulate da tali autorità.

[21] 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).

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 coopera attivamente con le autorità di controllo nazionali al fine di garantire un controllo efficace dei sistemi IT su larga scala o delle agenzie dell'Unione.

2. Il garante europeo della protezione dei dati, agendo nei limiti delle proprie competenze e nell'ambito delle proprie responsabilità, scambia informazioni pertinenti, fornisce assistenza nello svolgimento di revisioni e ispezioni, esamina difficoltà di interpretazione o applicazione del presente regolamento e di altri atti dell'Unione applicabili, studia problemi inerenti all'esercizio di un controllo indipendente o all'esercizio dei diritti degli interessati, elabora proposte armonizzate per soluzioni di eventuali problemi e promuove la sensibilizzazione del pubblico in materia di diritto alla protezione dei dati, in funzione delle necessità, insieme alle autorità di controllo nazionali.

3. Ai fini di cui al paragrafo 2, il garante europeo della protezione dei dati si incontra con le autorità di controllo nazionali almeno due volte all'anno nell'ambito del comitato europeo per la protezione dei dati. I costi e la gestione di tali riunioni sono a carico del comitato europeo per la protezione dei dati. Nella prima riunione è adottato un regolamento interno. Ulteriori metodi di lavoro sono elaborati congiuntamente, 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.

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 l'interessato 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, il reclamo è da ritenersi rigettato.

Articolo 64
Diritto a un ricorso giurisdizionale effettivo

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

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 dal titolare del trattamento o dal responsabile del trattamento, 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 59, 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 a finalità del trattamento in questione nonché il numero di interessati lesi dal danno 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) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 59 nei confronti dell'istituzione o dell'organo in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti.

Il procedimento che porta all'imposizione di tali sanzioni pecuniarie dovrebbe svolgersi 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, 27, 28, 29, 30, 31, 32, 33, 37, 38, 39, 40, 44, 45 e 46

sono soggette, conformemente al paragrafo 1, 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 un'organizzazione internazionale a norma degli articoli da 47 a 51.

4. Se, in relazione allo stesso trattamento o a trattamenti collegati o continui, un'istituzione o un organo dell'Unione viola, con dolo o colpa, 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 di essere sentiti relativamente agli addebiti su cui esso si basa. 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 essere sentite. 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 il legittimo interesse 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 europea.

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 con riguardo 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 all'articolo 63 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 senza seguire la via gerarchica per una asserita violazione delle norme del presente regolamento. Nessun pregiudizio può derivare ad alcuno dalla presentazione al garante europeo della protezione dei dati di un reclamo relativo a un'asserita violazione.

Articolo 69
Sanzioni

Il funzionario o altro agente dell'Unione europea 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 dei funzionari dell'Unione europea o dal regime applicabile agli altri agenti dell'Unione europea.

CAPO IX

ATTI DI ESECUZIONE

Articolo 70
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 X

DISPOSIZIONI FINALI

Articolo 71
Abrogazione del regolamento (CE) n. 45/2001 e della decisione n. 1247/2002/CE

Il regolamento (CE) n. 45/2001[22] e la decisione n. 1247/2002/CE[23] sono abrogati a decorrere dal 25 maggio 2018. I riferimenti al regolamento e alla decisione abrogati si intendono fatti al presente regolamento.

Articolo 72
Misure transitorie

1. Il presente regolamento non incide sulla decisione 2014/886/UE del Parlamento europeo e del Consiglio[24] e sugli attuali mandati del garante europeo della protezione dei dati e del garante aggiunto.

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

---

22 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).

23 Decisione n. 1247/2002/CE del Parlamento europeo, del Consiglio e della Commissione, del 1° 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).

24 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).

3. L’articolo 54, paragrafi 4, 5 e 7, e gli articoli 56 e 57 del presente regolamento si applicano all’attuale garante aggiunto fino al termine del suo mandato il 5 dicembre 2019.

4. Il garante aggiunto assiste il garante europeo della protezione dei dati in tutte le sue funzioni e lo sostituisce quando quest’ultimo è assente o impossibilitato a svolgere le sue funzioni fino alla fine del mandato del garante aggiunto il 5 dicembre 2019.

Articolo 73
Entrata in vigore e applicazione

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell’Unione europea*.

2. Esso si applica a decorrere dal 25 maggio 2018.

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

Fatto a Bruxelles, il

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

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

1.2. Settore/settori interessati nella struttura ABM/ABB

1.3. Natura della proposta/iniziativa

1.4. Obiettivi

1.5. Motivazione della proposta/iniziativa

1.6. Durata e incidenza finanziaria

1.7. Modalità di gestione previste

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

2.2. Sistema di gestione e di controllo

2.3. Misure di prevenzione delle frodi e delle irregolarità

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

3.2. Incidenza prevista sulle spese

3.2.1. Sintesi dell'incidenza prevista sulle spese

3.2.2. Incidenza prevista sugli stanziamenti operativi

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

3.2.5. Partecipazione di terzi al finanziamento

3.3. Incidenza prevista sulle entrate

SCHEDA FINANZIARIA LEGISLATIVA

1. CONTESTO DELLA PROPOSTA/INIZIATIVA

1.1. Titolo della proposta/iniziativa

Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi, degli uffici e delle agenzie dell'Unione, nonché la libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE.

1.2. Settore/settori interessati nella struttura ABM/ABB[25]

Giustizia – Protezione dei dati personali

1.3. Natura della proposta/iniziativa

☐ La proposta/iniziativa riguarda **una nuova azione**

☐ La proposta/iniziativa riguarda **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[26]

– La proposta/iniziativa riguarda **la proroga di un'azione esistente**

☐ La proposta/iniziativa riguarda **un'azione riorientata verso una nuova azione**

1.4. Obiettivi

1.4.1. Obiettivi strategici pluriennali della Commissione oggetto della proposta/iniziativa

L'entrata in vigore del trattato di Lisbona, in particolare l'introduzione di una nuova base giuridica (articolo 16 del TFUE), offre la possibilità di creare un quadro globale per la protezione dei dati che copra tutti i settori.

Il 27 aprile 2016 l'Unione ha adottato il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (Testo rilevante ai fini del SEE) (GU L 119 del 4.5.2016, pag. 1).

Lo stesso giorno l'Unione ha adottato la 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).

La presente proposta intende completare la creazione di un quadro globale per la protezione dei dati nell'Unione, allineando le norme in materia di protezione dei dati applicabili alle istituzioni e agli organi dell'Unione alle norme in materia di protezione dei dati del regolamento (UE) 2016/679. Per motivi di coerenza, le

[25] ABM: activity-based management (gestione per attività) ABB: activity-based budgeting (bilancio per attività).

[26] A norma dell'articolo 54, paragrafo 2, lettera a) o b), del regolamento finanziario.

istituzioni e gli organi dell'Unione dovrebbero applicare un insieme di norme in materia di protezione dei dati analogo a quello della pubblica amministrazione negli Stati membri.

1.4.2. Obiettivi specifici e attività ABM/ABB interessate

Obiettivo specifico 1:

garantire l'applicazione coerente delle norme in materia di protezione dei dati in tutta l'Unione.

Obiettivo specifico 2:

razionalizzare l'attuale modello di governance della protezione dei dati nelle istituzioni e negli organi dell'Unione.

Obiettivo specifico 3:

garantire una maggiore conformità alle norme in materia di protezione dei dati e l'attuazione di tali norme nelle istituzioni e negli organi dell'Unione.

1.4.3. Risultati e incidenza previsti

Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.

Nel loro ruolo di titolari del trattamento, le istituzioni e gli organi dell'Unione dovrebbero beneficiare del passaggio dalle attuali procedure amministrative (approccio ex ante) di protezione dei dati a un rispetto effettivo e a un'applicazione rafforzata delle norme sostanziali in materia di protezione dei dati e dei principi e delle nozioni nuovi introdotti dal regolamento (UE) 2016/679 (approccio ex post), che saranno applicabili in tutta l'Unione.

Le persone fisiche i cui dati saranno trattati dalle istituzioni e dagli organi dell'Unione avranno un miglior controllo dei propri dati personali e più fiducia nell'ambiente digitale. Constateranno inoltre un rafforzamento della responsabilità delle istituzioni e degli organi dell'Unione.

Il garante europeo della protezione dei dati potrà concentrarsi maggiormente sul proprio ruolo di vigilanza. La ripartizione tra il comitato europeo per la protezione dei dati, istituito dal regolamento (UE) 2016/679, e il garante europeo della protezione dei dati del compito di fornire consulenza alla Commissione sarà chiarita e le sovrapposizioni saranno evitate.

1.4.4. Indicatori di risultato e di incidenza

Precisare gli indicatori che permettono di seguire l'attuazione della proposta/iniziativa.

Gli indicatori includono gli elementi seguenti:

numero di pareri emessi dal comitato europeo per la protezione dei dati e dal garante europeo della protezione dei dati,

ripartizione delle attività dei responsabili della protezione dei dati,

ricorso alle valutazioni d'impatto sulla protezione dei dati,

numero di reclami presentati dagli interessati,

sanzioni irrogate ai titolari del trattamento per violazione della protezione dei dati.

1.5. Motivazione della proposta/iniziativa

1.5.1. Necessità nel breve e lungo termine

Nel regolamento (UE) 2016/679 (articolo 2, paragrafo 3, articolo 98, considerando 17) i colegislatori dell'Unione hanno chiesto un adeguamento del regolamento (CE) n. 45/2001 ai principi e alle norme stabiliti nel regolamento (UE) 2016/679, al fine di creare un quadro solido e coerente per la protezione dei dati nell'Unione e di consentire l'applicazione di entrambi gli strumenti a decorrere dalla stessa data, ossia il 25 maggio 2018.

1.5.2. Valore aggiunto dell'intervento dell'Unione europea

Le norme in materia di protezione dei dati applicabili alle istituzioni e agli organi dell'Unione possono essere introdotte solo mediante un atto dell'Unione.

1.5.3. Insegnamenti tratti da esperienze analoghe

La presente proposta si basa sull'esperienza maturata con il regolamento (CE) n. 45/2001 e sulla valutazione della sua applicazione effettuata nell'ambito di uno

studio di valutazione (condotto da un contraente esterno tra settembre 2014 e giugno 2015)[27].

1.5.4. Compatibilità ed eventuale sinergia con altri strumenti pertinenti

La presente proposta si basa sul regolamento (UE) 2016/679 e conclude la costruzione di un quadro per la protezione dei dati nell'Unione solido, coerente e moderno nonché neutrale sotto il profilo tecnologico e che possa dimostrarsi valido anche in futuro.

[27] JUST/2013/FRAC/FW/0157/A4 nell'ambito del contratto quadro multiplo JUST/2011/EVAL/01 (RS 2013/05) - Studio di valutazione sul regolamento (CE) 45/2001, di Ernst and Young

1.6. Durata e incidenza finanziaria

☐ Proposta/iniziativa di **durata limitata**

– ☐ Proposta/iniziativa in vigore a decorrere dal [GG/MM]AAAA fino al [GG/MM]AAAA

– ☐ Incidenza finanziaria dal AAAA al AAAA

- Proposta/iniziativa di **durata illimitata**
- Attuazione con un periodo di avviamento dal [2017] al 25 maggio 2018, seguito da un funzionamento a pieno ritmo.

1.7. Modalità di gestione previste[28]

- Gestione diretta a opera della Commissione

– ☐ a opera dei suoi servizi, compreso il personale delle delegazioni dell'Unione;

– ☐ a opera delle agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☐ **Gestione indiretta** con compiti di esecuzione del bilancio affidati:

– ☐ a paesi terzi o organismi da questi designati;

– ☐ a organizzazioni internazionali e rispettive agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– ☐ agli organismi di cui agli articoli 208 e 209 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui presentano sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che presentano sufficienti garanzie finanziarie;

– ☐ alle persone incaricate di attuare azioni specifiche nel settore della PESC a norma del titolo V del TUE, che devono essere indicate nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

Osservazioni

La presente proposta è limitata alle istituzioni e agli organi dell'Unione e riguarda l'insieme di essi.

[28] Le spiegazioni sulle modalità di gestione e i riferimenti al regolamento finanziario sono disponibili sul sito BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. MISURE DI GESTIONE

2.1. Disposizioni in materia di monitoraggio e di relazioni

Precisare frequenza e condizioni.

La presente proposta si limita all'applicazione delle norme in materia di protezione dei dati da parte delle istituzioni e degli organi dell'Unione. Il controllo e l'applicazione di dette norme è un compito del garante europeo della protezione dei dati, così come il monitoraggio e la comunicazione. In particolare, l'articolo 60 della presente proposta stabilisce che il garante europeo della protezione dei dati ha l'obbligo di presentare al Parlamento europeo, al Consiglio e alla Commissione una relazione annuale delle attività di sua competenza, rendendolo pubblico allo stesso tempo.

2.2. Sistema di gestione e di controllo

2.2.1. Rischi individuati

Tra settembre 2014 e giugno 2015 un contraente esterno ha effettuato uno studio di valutazione sull'applicazione del regolamento (CE) n. 45/2001. Lo studio ha esaminato anche le conseguenze dell'introduzione di nozioni e principi fondamentali del regolamento (UE) 2016/679 nelle istituzione e negli organi dell'Unione.

Il nuovo modello di protezione dei dati presterà attenzione all'effettivo rispetto delle norme in materia di protezione dei dati nonché all'applicazione e al controllo effettivi di tali norme. Esso richiederà un cambiamento della cultura della protezione dei dati nelle istituzioni e negli organi dell'Unione, che dovrà passare da un approccio ex ante a un approccio ex post.

2.2.2. Informazioni riguardanti il sistema di controllo interno istituito

I metodi di controllo esistenti applicati dalle istituzioni e dagli organi dell'Unione.

2.2.3. Stima dei costi e dei benefici dei controlli e valutazione del previsto livello di rischio di errore

I metodi di controllo esistenti applicati dalle istituzioni e dagli organi dell'Unione.

2.3. Misure di prevenzione delle frodi e delle irregolarità

Precisare le misure di prevenzione e tutela in vigore o previste.

I metodi esistenti di prevenzione delle frodi e delle irregolarità applicati dalle istituzioni e dagli organi dell'Unione.

3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Contributo			
	Numero [Rubrica……]	Diss./Non diss[29].	di paesi EFTA[30]	di paesi candidati[31]	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
	[XX.YY.YY.YY]	Diss./Non diss.	SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO

- Nuove linee di bilancio di cui è chiesta la creazione

Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio.

Rubrica del quadro finanziario pluriennale	Linea di bilancio	Natura della spesa	Contributo			
	Numero [Rubrica……]	Diss./Non diss.	di paesi EFTA	di paesi candidati	di paesi terzi	ai sensi dell'articolo 21, paragrafo 2, lettera b), del regolamento finanziario
	[XX.YY.YY.YY]		SÌ/NO	SÌ/NO	SÌ/NO	SÌ/NO

[29] Diss. = Stanziamenti dissociati / Non diss. = Stanziamenti non dissociati.
[30] EFTA: Associazione europea di libero scambio.
[31] Paesi candidati e, se del caso, paesi potenziali candidati dei Balcani occidentali.

3.2. Incidenza prevista sulle spese

L'incidenza sulla spesa della presente proposta è limitata alla spesa delle istituzioni e degli organi dell'Unione. Tuttavia la valutazione dei costi connessi alla presente proposta dimostra che essa non genera spese aggiuntive sostanziali per le istituzioni e gli organi dell'Unione.

Per quanto riguarda i titolari del trattamento dei dati nelle istituzioni e negli organi dell'Unione, lo studio di valutazione del regolamento (CE) n. 45/2001 indica che le loro attività di protezione dei dati corrispondono a circa 70 equivalenti a tempo pieno, ossia a circa 9,3 milioni di euro l'anno. Il 20% circa delle loro attività di protezione dei dati sono attualmente dedicate alla notificazione del trattamento dei dati. Il presente regolamento elimina tale attività, il che corrisponde a un risparmio annuo di 1 922 000 EUR per i titolari del trattamento dei dati nelle istituzioni e negli organi dell'Unione. Il risparmio dovrebbe essere controbilanciato da un maggiore coinvolgimento dei titolari del trattamento dei dati nell'applicazione dei nuovi principi e concetti introdotti dal presente regolamento.

Più precisamente, l'indagine svolta nell'ambito dello studio di valutazione ha rilevato che l'introduzione:

a) del principio di minimizzazione dei dati avrebbe conseguenze minime o inesistenti sulle istituzioni e gli organi dell'Unione;

b) del principio di trasparenza non avrebbe conseguenze significative sulle istituzioni e gli organi dell'Unione;

c) di maggiori obblighi di informazione aumenterebbe il carico di lavoro dei titolari del trattamento dei dati e dei responsabili della protezione dei dati;

d) del diritto all'oblio non avrebbe conseguenze significative sulle istituzioni e gli organi dell'Unione;

e) del diritto alla portabilità dei dati avrebbe conseguenze minime o inesistenti sulle istituzioni e gli organi dell'Unione;

f) delle valutazioni d'impatto sulla protezione dei dati avrebbe conseguenze moderatamente significative sul carico di lavoro dei titolari del trattamento dei dati e sui responsabili della protezione dei dati, dato che alcune istituzioni e alcuni organi dell'Unione effettuano già valutazioni d'impatto sulla protezione dei dati e le situazioni in cui tali valutazioni d'impatto sulla protezione dei dati saranno effettuate sono limitate;

g) delle notificazioni delle violazioni dei dati personali aumenterebbero il carico di lavoro dei titolari del trattamento dei dati, ma tali violazioni non sono frequenti;

h) della protezione dei dati fin dalla progettazione e della protezione dei dati di default sono già utilizzate in diverse istituzioni e in diversi organi dell'Unione.

Inoltre, la valutazione d'impatto realizzata prima dell'adozione della proposta del pacchetto di riforma della protezione dei dati ha concluso che le pubbliche amministrazioni o i titolari del trattamento non incontrerebbero ostacoli amministrativi in seguito all'introduzione del principio di protezione dei dati fin dalla progettazione.[32]

Per quanto riguarda i responsabili della protezione dei dati, lo studio di valutazione ha stimato il costo dell'attuale rete dei responsabili della protezione dei dati e dei coordinatori per la protezione dei dati nelle istituzioni e negli organi dell'Unione a 82,9 equivalenti a tempo pieno o a 10,9 milioni di EUR l'anno. Essi spendono il 26% del tempo correlato alla protezione dei dati in attività abolite dal presente regolamento, ad esempio la redazione di notificazioni (al posto dei titolari del trattamento), la valutazione delle notificazioni ricevute, la registrazione delle proprie attività nel registro e la realizzazione di controlli preventivi. L'abolizione di queste attività genera ulteriori risparmi pari a 2 834 000 EUR l'anno per le istituzioni e gli organi dell'Unione. Inoltre, il presente regolamento consente un potenziale di risparmi aggiuntivi, permettendo alle istituzioni e agli organi dell'Unione di esternalizzare le attività del responsabile della protezione dei dati, anziché assumere personale proprio.

I risparmi relativi alle attività dei responsabili della protezione dei dati saranno controbilanciati dal coinvolgimento di questi ultimi nei maggiori obblighi di informazione, nelle valutazioni d'impatto sulla protezione dei dati (in circostanze limitate in cui saranno richieste) e nella consultazione preventiva del garante europeo della protezione dei dati (la cui portata sarà molto più limitata rispetto all'attuale obbligo di controllo preventivo).

Il bilancio annuale del garante europeo della protezione dei dati è pressoché stabile dal 2011 e ammonta a circa 8 milioni di EUR. Attualmente le sue unità Controllo e applicazione e Politica e consulenza hanno un numero di dipendenti analogo, stabile dal 2008. La maggiore attenzione posta dal presente regolamento sul ruolo di controllo del garante europeo della protezione dei dati sarà compensata da un ruolo di consulenza più mirato e dall'eliminazione della duplicazione dei compiti svolti anche dal comitato europeo per la protezione dei dati. Il garante europeo della protezione dei dati può pertanto procedere alla ridistribuzione interna del personale.

La presente proposta prevede la possibilità per il garante europeo della protezione dei dati di imporre sanzioni amministrative alle istituzioni e agli organi dell'Unione. A ciascuna istituzione o a ciascun organo dell'Unione possono essere imposte sanzioni amministrative per un importo massimo di 250 000 EUR all'anno (25 000 EUR per violazione), o 500 000 EUR all'anno (50 000 EUR per violazione) per le violazioni più gravi del presente regolamento. Le sanzioni dovrebbero essere applicate solo nei casi più gravi e in seguito al mancato rispetto da parte dell'istituzione o dell'organo dell'Unione dell'esercizio di altre misure correttive adottate dal garante europeo della protezione dei dati. L'incidenza finanziaria di tali sanzioni dovrebbe pertanto essere limitata.

[32] Documento di lavoro dei servizi della Commissione, valutazione d'impatto, SEC (2012) 72 final, pagina 110.

3.2.1. Sintesi dell'incidenza prevista sulle spese

Mio EUR (al terzo decimale)

Rubrica del quadro finanziario pluriennale	Numero	[Rubrica……]

DG: <…….>			Anno **N**[33]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
•Stanziamenti operativi										
Numero della linea di bilancio	Impegni	(1)								
	Pagamenti	(2)								
Numero della linea di bilancio	Impegni	(1a)								
	Pagamenti	(2a)								
Stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici[34]										
Numero della linea di bilancio		(3)								
TOTALE degli stanziamenti per la DG <…….>	Impegni	=1+1a +3								
	Pagamenti	=2+2a +3								

•TOTALE degli stanziamenti operativi	Impegni	(4)								

[33] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa.

[34] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

	Pagamenti	(5)								
•TOTALE degli stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici		(6)								
TOTALE degli stanziamenti a titolo della RUBRICA <….> del quadro finanziario pluriennale	Impegni	=4+ 6								
	Pagamenti	=5+ 6								

Se la proposta/iniziativa incide su più rubriche:

•TOTALE degli stanziamenti operativi	Impegni	(4)								
	Pagamenti	(5)								
•TOTALE degli stanziamenti di natura amministrativa finanziati dalla dotazione di programmi specifici		(6)								
TOTALE degli stanziamenti per le RUBRICHE da 1 a 4 del quadro finanziario pluriennale (importo di riferimento)	Impegni	=4+ 6								
	Pagamenti	=5+ 6								

Rubrica del quadro finanziario pluriennale	**5**	"Spese amministrative"

Mio EUR (al terzo decimale)

		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
DG: <…….>									
• Risorse umane									
• Altre spese amministrative									
TOTALE DG <….>	Stanziamenti								

TOTALE degli stanziamenti per la RUBRICA 5 del quadro finanziario pluriennale	(Totale impegni = Totale pagamenti)								

Mio EUR (al terzo decimale)

		Anno **N**[35]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
TOTALE degli stanziamenti per le RUBRICHE da 1 a 5 del quadro finanziario pluriennale	Impegni								
	Pagamenti								

[35] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa.

3.2.2. Incidenza prevista sugli stanziamenti operativi

- La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

☐ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Stanziamenti di impegno in Mio EUR (al terzo decimale)

Specificare gli obiettivi e i risultati ⇩			Anno **N**		Anno **N+1**		Anno **N+2**		Anno **N+3**		Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)						**TOTALE**	
			RISULTATI															
	Tipo[36]	Costo medio	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N.	Costo	N. totale	Costo totale
OBIETTIVO SPECIFICO 1[37]…																		
- Risultato																		
- Risultato																		
- Risultato																		
Totale parziale dell'obiettivo specifico 1																		
OBIETTIVO SPECIFICO 2 ...																		
- Risultato																		
Totale parziale dell'obiettivo specifico 2																		
COSTO TOTALE																		

[36] I risultati sono i prodotti e servizi da fornire (ad esempio: numero di scambi di studenti finanziati, numero di km di strade costruiti ecc.).

[37] Come descritto nella sezione 1.4.2. "Obiettivi specifici… ".

3.2.3. Incidenza prevista sugli stanziamenti di natura amministrativa

3.2.3.1. Sintesi

- La proposta/iniziativa non comporta l'utilizzo di stanziamenti di natura amministrativa.

☐ La proposta/iniziativa comporta l'utilizzo di stanziamenti di natura amministrativa, come spiegato di seguito:

Mio EUR (al terzo decimale)

	Anno **N** [38]	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			**TOTALE**
RUBRICA 5 del quadro finanziario pluriennale								
Risorse umane								
Altre spese amministrative								
Totale parziale RUBRICA 5 del quadro finanziario pluriennale								

Esclusa la RUBRICA 5[39] **del quadro finanziario pluriennale**								
Risorse umane								
Altre spese di natura amministrativa								
Totale parziale esclusa la RUBRICA 5 del quadro finanziario pluriennale								

TOTALE								

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese di natura amministrativa è coperto dagli stanziamenti della DG già assegnati alla gestione dell'azione e/o riassegnati all'interno della stessa DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

[38] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa.

[39] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.3.2. Fabbisogno previsto di risorse umane

- La proposta/iniziativa non comporta l'utilizzo di risorse umane.

☐ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

Stima da esprimere in equivalenti a tempo pieno

	Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
• Posti della tabella dell'organico (funzionari e agenti temporanei)							
XX 01 01 01 (in sede e negli uffici di rappresentanza della Commissione)							
XX 01 01 02 (nelle delegazioni)							
XX 01 05 01 (ricerca indiretta)							
10 01 05 01 (ricerca diretta)							
•Personale esterno (in equivalenti a tempo pieno: ETP)[40]							
XX 01 02 01 (AC, END e INT della dotazione globale)							
XX 01 02 02 (AC, AL, END, INT e JED nelle delegazioni)							
XX 01 04 **aa** [41] - in sede							
XX 01 04 **aa** [41] - nelle delegazioni							
XX 01 05 02 (AC, END, INT - ricerca indiretta)							
10 01 05 02 (AC, END e INT – ricerca diretta)							
Altre linee di bilancio (specificare)							
TOTALE							

XX è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

Funzionari e agenti temporanei	
Personale esterno	

40 AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JED = giovane esperto in delegazione (jeune expert en délégation).

41 Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

3.2.4. Compatibilità con il quadro finanziario pluriennale attuale

- La proposta/iniziativa è compatibile con il quadro finanziario pluriennale attuale.

☐ La proposta/iniziativa richiede una riprogrammazione della pertinente rubrica del quadro finanziario pluriennale.

Spiegare la riprogrammazione richiesta, precisando le linee di bilancio interessate e gli importi corrispondenti.

☐ La proposta/iniziativa richiede l'applicazione dello strumento di flessibilità o la revisione del quadro finanziario pluriennale.

Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti.

3.2.5. Partecipazione di terzi al finanziamento

- La proposta/iniziativa non prevede cofinanziamenti da terzi.

La proposta/iniziativa prevede il cofinanziamento indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

	Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)			Totale
Specificare l'organismo di cofinanziamento								
TOTALE degli stanziamenti cofinanziati								

3.3. Incidenza prevista sulle entrate

- La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

– ☐ sulle risorse proprie

– ☐ sulle entrate varie

Mio EUR (al terzo decimale)

Linea di bilancio delle entrate:	Stanziamenti disponibili per l'esercizio in corso	Incidenza della proposta/iniziativa[42]						
		Anno **N**	Anno **N+1**	Anno **N+2**	Anno **N+3**	Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6)		
Articolo …….								

Per quanto riguarda le entrate varie con destinazione specifica, precisare la o le linee di spesa interessate.

Precisare il metodo di calcolo dell'incidenza sulle entrate.

[42] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 25% per spese di riscossione.