



**CONSIGLIO  
DELL'UNIONE EUROPEA**

**Bruxelles, 27 gennaio 2012 (13.02)  
(OR. en)**

**5833/12**

**Fascicolo interistituzionale:  
2012/0010 (COD)**

**DATA PROTECT 6  
JAI 41  
DAPIX 9  
FREMP 8  
COMIX 59  
CODEC 217**

**PROPOSTA**

---

Mittente: Commissione europea

Data: [27 gennaio 2012](#)

---

n. doc. Comm.: COM(2012) 10 final

---

Oggetto: Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati

---

Si trasmette in allegato, per le delegazioni, la proposta [della Commissione](#) inviata con lettera di [Jordi AYET PUIGARNAU, Direttore](#), a Uwe CORSEPIUS, Segretario generale del Consiglio dell'Unione europea.

---

All.: COM(2012) 10 final



COMMISSIONE EUROPEA

Bruxelles, 25.1.2012  
COM(2012) 10 final

2012/0010 (COD)

Proposta di

**DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

**concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati**

[...]

## RELAZIONE

### 1. CONTESTO DELLA PROPOSTA

La presente relazione illustra l'impostazione adottata ai fini dell'elaborazione del nuovo quadro giuridico per la protezione dei dati personali nell'Unione europea, delineata nella comunicazione COM (2012) 9 final. Il quadro giuridico consta di due proposte legislative:

- una proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati);
- una proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, e la libera circolazione di tali dati.

La presente relazione riguarda quest'ultima proposta legislativa.

La direttiva 95/46/CE<sup>1</sup> – pietra angolare nell'impianto della vigente normativa dell'UE in materia di protezione dei dati personali – è stata adottata nel 1995 con due obiettivi: salvaguardare il diritto fondamentale alla protezione dei dati e garantire la libera circolazione dei dati personali tra gli Stati membri. La direttiva è stata integrata da diversi strumenti che prevedono disposizioni specifiche per la protezione dei dati personali nei settori della cooperazione giudiziaria e di polizia in materia penale (ex terzo pilastro)<sup>2</sup>, compresa la decisione quadro 2008/977/GAI<sup>3</sup>.

Il Consiglio europeo ha invitato la Commissione a valutare il funzionamento degli strumenti giuridici dell'Unione in materia di protezione dei dati e a presentare, se necessario, nuove iniziative legislative e non legislative<sup>4</sup>. Nella sua risoluzione sul programma di Stoccolma<sup>5</sup> il Parlamento europeo ha accolto con favore la proposta relativa a un quadro giuridico completo in materia di protezione dei dati nell'UE chiedendo, tra l'altro, la revisione della decisione quadro. Nel piano d'azione per l'attuazione del programma di Stoccolma<sup>6</sup> la Commissione ha sottolineato la necessità di assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati personali nel contesto di tutte le politiche europee. Il piano d'azione ha sottolineato che: *“[i]n una società globalizzata, caratterizzata da un rapido progresso tecnologico in cui lo scambio d'informazioni non conosce confini, è quanto mai importante garantire il rispetto della vita privata. L'Unione deve assicurare l'applicazione sistematica del diritto fondamentale alla protezione dei dati. Occorre rafforzare la posizione dell'UE in*

---

<sup>1</sup> Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281 del 23.11.1995, pag. 31).

<sup>2</sup> Si veda l'elenco integrale di tali strumenti nell'allegato 3 della valutazione d'impatto (SEC(2012)72).

<sup>3</sup> Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale (GU L 350 del 30.12.2008, pag. 60).

<sup>4</sup> Nel programma di Stoccolma (GU C 115 del 4.5.2010, pag. 1).

<sup>5</sup> Risoluzione del Parlamento europeo sul programma di Stoccolma del 25 novembre 2009.

<sup>6</sup> COM(2010) 171 definitivo.

*relazione alla protezione dei dati personali in tutte le politiche europee, anche nel contrastare e prevenire la criminalità e nelle relazioni internazionali.”*

Nella comunicazione “Un approccio globale alla protezione dei dati personali nell’Unione europea”<sup>7</sup>, la Commissione è giunta alla conclusione che l’Unione europea ha bisogno di una politica più completa e coerente rispetto al diritto fondamentale alla protezione dei dati personali.

La decisione quadro 2008/977/GAI ha un campo di applicazione limitato, in quanto si applica solo al trattamento transfrontaliero dei dati e non alle attività di trattamento effettuate dalla polizia e dalle autorità giudiziarie a livello strettamente nazionale. Ciò può creare difficoltà per le forze di polizia e le altre autorità competenti nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia per le quali può non essere agevole stabilire il carattere puramente nazionale o transfrontaliero di un trattamento di dati o prevedere se i dati “nazionali” possano essere oggetto di un successivo scambio transfrontaliero (cfr. sezione 2). Inoltre, per sua natura e contenuto, la decisione quadro lascia un ampio margine di manovra alle legislazioni nazionali degli Stati membri nell’attuazione delle sue disposizioni. Inoltre, non prevede alcun meccanismo o gruppo consultivo analogo al gruppo di lavoro “articolo 29” inteso a promuovere un’interpretazione comune delle sue disposizioni, né conferisce competenze di esecuzione alla Commissione per garantire un approccio attuativo comune.

L’articolo 16, paragrafo 1, del trattato sul funzionamento dell’Unione europea (TFUE) stabilisce il principio secondo il quale ogni persona ha diritto alla protezione dei dati di carattere personale. Inoltre, all’articolo 16, paragrafo 2, TFUE, il trattato di Lisbona introduce una base giuridica specifica per l’adozione di norme in materia di protezione dei dati personali, anche nell’ambito della cooperazione di polizia e giudiziaria in materia penale. L’articolo 8 della Carta dei diritti fondamentali dell’Unione europea annovera la protezione dei dati personali tra i diritti fondamentali. L’articolo 16 del TFUE impone al legislatore di stabilire norme relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali anche nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, che contemplino il trattamento sia transfrontaliero sia nazionale dei dati personali. Ciò consentirà di tutelare i diritti e le libertà fondamentali delle persone fisiche e in particolare il diritto alla protezione dei dati personali, garantendo al tempo stesso lo scambio di dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e contribuendo a una più efficace cooperazione nella lotta contro la criminalità in Europa.

Data la specificità dei settori della cooperazione di polizia e giudiziaria in materia penale, la dichiarazione n. 21<sup>8</sup> ha riconosciuto che potrebbero rivelarsi necessarie norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia in base all’articolo 16 del TFUE.

---

<sup>7</sup> Comunicazione della Commissione europea “Un approccio globale alla protezione dei dati personali nell’Unione europea”, COM (2010) 609 definitivo, 4.11.2010.

<sup>8</sup> Cfr. Dichiarazione n. 21, relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, (allegato all’atto finale della conferenza intergovernativa che ha adottato il trattato di Lisbona, 13.12.2007).

## 2. CONSULTAZIONE DELLE PARTI INTERESSATE E VALUTAZIONE D'IMPATTO

La presente iniziativa è il risultato di estese consultazioni con tutte le principali parti in causa sul riesame del quadro giuridico esistente in materia di protezione dei dati personali, comprendenti due fasi di consultazione pubblica:

- dal 9 luglio al 31 dicembre 2009, la consultazione relativa al quadro giuridico del diritto fondamentale alla protezione dei dati personali, per la quale la Commissione ha ricevuto 168 risposte, 127 provenienti da privati cittadini, organizzazioni e associazioni imprenditoriali e 12 dalle autorità pubbliche; i contributi che non rivestono carattere riservato sono consultabili sul sito web della Commissione<sup>9</sup>;
- dal 4 novembre 2010 al 15 gennaio 2011, la consultazione sulla comunicazione della Commissione “Un approccio globale alla protezione dei dati personali nell’Unione europea”, per la quale la Commissione ha ricevuto 305 risposte, 54 da privati cittadini, 31 da autorità pubbliche e 220 da organizzazioni private, soprattutto associazioni d’imprese e organizzazioni non governative. I contributi che non rivestono carattere riservato sono consultabili sul sito web della Commissione<sup>10</sup>.

Mentre tali consultazioni vertevano sul riesame della direttiva 95/46/CE in termini ampi, con le autorità di contrasto interessate sono state condotte consultazioni più mirate, in particolare, un seminario organizzato il 29 giugno 2010 con le autorità degli Stati membri in merito all’applicazione delle norme di protezione dei dati alle autorità pubbliche, anche nel settore della cooperazione di polizia e la cooperazione giudiziaria in materia penale. Inoltre, il 2 febbraio 2011 la Commissione ha organizzato un seminario con le autorità degli Stati membri per discutere l’attuazione della decisione quadro 2008/977/GAI e, più in generale, la protezione dei dati personali nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale.

I cittadini europei sono stati consultati attraverso un sondaggio Eurobarometro effettuato nel novembre-dicembre 2010<sup>11</sup>, sono stati avviati diversi studi in materia<sup>12</sup> e il Gruppo di lavoro “Articolo 29”<sup>13</sup> ha dato numerosi pareri e un utile contributo alla Commissione<sup>14</sup>. Il garante

---

<sup>9</sup> [http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm)

<sup>10</sup> [http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104\\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm)

<sup>11</sup> Speciale Eurobarometro (EB) 359, *Data Protection and Electronic Identity in the EU* (2011): [http://ec.europa.eu/public\\_opinion/archives/ebs/ebs\\_359\\_en.pdf](http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf).

<sup>12</sup> Cfr. lo studio sui vantaggi economici delle tecnologie di rafforzamento della tutela della vita privata (Study on the economic benefits of privacy enhancing technologies, London Economics), luglio 2010 o lo studio comparativo sui diversi approcci alle nuove sfide per la privacy soprattutto alla luce degli sviluppi tecnologici (Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments), gennaio 2010, gennaio 2010. ([http://ec.europa.eu/justice/policies/privacy/docs/studies/new\\_privacy\\_challenges/final\\_report\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf)).

<sup>13</sup> Il Gruppo di lavoro è stato istituito nel 1996 (dall’articolo 29 della direttiva); è un organo consultivo composto da un rappresentante delle autorità di protezione dei dati per ciascuno Stato membro, dal Garante europeo della protezione dei dati e dalla Commissione. Per maggiori informazioni sulle sue attività, si consulti il sito: [http://ec.europa.eu/justice/policies/privacy/workinggroup/index\\_en.htm](http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm).

<sup>14</sup> Si vedano in particolare i pareri sui seguenti argomenti: il “futuro della vita privata” (2009, WP 168); i concetti di “responsabile del trattamento” e “incaricato del trattamento” (1/2010, WP 169); la pubblicità comportamentale on line (2/2010, WP 171); il principio di responsabilità (3/2010, WP 173); il diritto applicabile (8/2010, WP 179); il consenso (15/2011, WP 187). Su richiesta della Commissione, il Gruppo ha adottato anche i tre seguenti documenti, rispettivamente sulle notificazioni, sui dati sensibili e sull’attuazione pratica dell’articolo 28, paragrafo 6, della direttiva sulla protezione dei dati. I

europeo della protezione dei dati ha espresso un parere complessivo sulle questioni sollevate nella comunicazione della Commissione del mese di novembre 2010<sup>15</sup>.

Il Parlamento europeo ha approvato, con risoluzione del 6 luglio 2011, una relazione a sostegno dell'impostazione adottata dalla Commissione per la riforma del quadro normativo in materia di protezione dei dati<sup>16</sup>. Le conclusioni adottate il 24 febbraio 2011 dal Consiglio dell'Unione europea esprimono un consenso generale all'intento della Commissione di riformare il quadro sulla protezione dei dati e approvano diversi elementi della strategia della Commissione. Anche il Comitato economico e sociale europeo ha commentato favorevolmente l'impulso generale dato dalla Commissione per garantire un'applicazione più coerente della normativa dell'UE in materia di protezione dei dati in tutti gli Stati membri e un'adeguata revisione della direttiva 95/46/CE<sup>17</sup>.

In linea con l'iniziativa "Legiferare meglio", la Commissione ha proceduto a una valutazione dell'impatto delle diverse opzioni strategiche<sup>18</sup>. La valutazione d'impatto è stata incentrata su tre obiettivi: migliorare la dimensione di mercato interno della protezione dei dati; rendere più efficace l'esercizio del diritto alla protezione dei dati da parte dei privati; creare un quadro completo e coerente applicabile a tutti i settori di competenza dell'Unione, compresa la cooperazione di polizia e giudiziaria in materia penale. Per quanto riguarda quest'ultimo obiettivo in particolare, sono state valutate due opzioni: una prima è sostanzialmente l'estensione del campo di applicazione delle norme sulla protezione dei dati in questo settore per far fronte alle carenze individuate e rispondere ad altre questioni sollevate dalla decisione quadro, e una seconda di più ampia portata che stabilisce disposizioni molto prescrittive e rigorose e che implicherebbe anche l'immediata modifica di tutti gli altri strumenti del "terzo pilastro". Una terza opzione "minimalista", basata in larga misura su comunicazioni interpretative e misure di sostegno strategico, come programmi di finanziamento e strumenti tecnici, con un minimo intervento legislativo, non è stata considerata adeguata ad affrontare le questioni individuate in questo settore in relazione alla protezione dei dati.

Conformemente ad una metodologia consolidata, la Commissione, coadiuvata da un gruppo direttivo interservizi, ha valutato ciascuna opzione in funzione delle sue effettive possibilità di conseguire gli obiettivi strategici, dell'impatto economico sulle parti interessate (compreso sul bilancio delle istituzioni dell'Unione europea), delle ripercussioni sulla società e dell'effetto sui diritti fondamentali. Non sono emersi possibili impatti ambientali.

L'analisi dell'impatto complessivo ha portato a individuare l'opzione prescelta, integrata nella presente proposta. Stando alla valutazione d'impatto, la sua attuazione consentirà di rafforzare ulteriormente la protezione dei dati in questo settore, in particolare includendo il trattamento dei dati nazionali, garantendo così una maggiore certezza giuridica alle autorità competenti nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia.

---

documenti sono consultabili alla pagina: [http://ec.europa.eu/justice/data-protection/article-29/documentation/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/index_en.htm).

<sup>15</sup> Disponibile sul sito del GEPD: <http://www.edps.europa.eu/EDPSWEB/>.

<sup>16</sup> Risoluzione del Parlamento europeo del 6 luglio 2011 su un approccio globale in materia di protezione dei dati personali nell'Unione europea (2011/2025 (INI), <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=EN&ring=A7-2011-0244> (relatore: on. Axel Voss (PPE/DE).

<sup>17</sup> CESE 999/2011.

<sup>18</sup> SEC(2012)72.

In data 9 settembre 2011 il comitato per la valutazione d'impatto ha espresso il suo parere sul progetto di valutazione d'impatto. e conseguentemente la valutazione è stata così modificata:

- sono stati chiariti gli obiettivi dell'attuale quadro normativo (in che misura siano stati o non siano stati realizzati), così come gli obiettivi della proposta riforma;
- la sezione relativa alla definizione del problema è stata corredata di nuove prove e di spiegazioni/chiarimenti supplementari.

La Commissione ha inoltre preparato una relazione di attuazione relativa alla decisione quadro 2008/977/GAI, basata sull'articolo 29, paragrafo 2, che dovrebbe essere adottata come componente del presente pacchetto di misure sulla protezione dei dati<sup>19</sup>. Anche i risultati di tale relazione, redatta sulla base dei dati forniti dagli Stati membri, ha alimentato la preparazione della valutazione d'impatto.

### **3. ELEMENTI GIURIDICI DELLA PROPOSTA**

#### **3.1. Base giuridica**

La proposta si basa sull'articolo 16, paragrafo 2, del TFUE, la nuova base giuridica specifica introdotta dal trattato di Lisbona per l'adozione di norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, così come da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e per l'adozione di norme relative alla libera circolazione di tali dati.

La proposta è finalizzata a garantire un livello elevato e uniforme di protezione dei dati in questo settore, in modo da accrescere la fiducia reciproca tra le autorità di polizia e giudiziarie di diversi Stati membri e agevolare la libera circolazione dei dati e la cooperazione tra i servizi di polizia e le autorità giudiziarie.

#### **3.2. Sussidiarietà e proporzionalità**

In virtù del principio di sussidiarietà (articolo 5, paragrafo 3, del TUE) l'Unione interviene soltanto se e in quanto gli obiettivi dell'azione prevista non possono essere conseguiti in misura sufficiente dagli Stati membri, ma possono, a motivo della portata o degli effetti dell'azione in questione, essere conseguiti meglio a livello di Unione. Alla luce dei problemi sopra esposti, l'analisi della sussidiarietà indica che è necessario intervenire a livello di Unione nei settori della cooperazione di polizia e giudiziaria in materia penale per i seguenti motivi:

- il diritto alla protezione dei dati personali, sancito dall'articolo 8 della Carta dei diritti fondamentali e dall'articolo 16, paragrafo 1, del TFUE richiede il medesimo livello di protezione dei dati in tutta l'Unione di protezione dei dati scambiati e dei dati trattati a livello nazionale;
- le autorità incaricate dell'applicazione della legge negli Stati membri devono trattare e scambiare dati a ritmi sempre crescenti ai fini della prevenzione e della lotta contro la

---

<sup>19</sup> COM(2012) 12.

criminalità e il terrorismo transnazionali. In questo contesto norme chiare e coerenti sulla protezione dei dati a livello di Unione contribuiranno a promuovere la cooperazione fra tali autorità;

- inoltre, esistono difficoltà pratiche nell’attuare efficacemente la normativa in materia di protezione dei dati e occorre stabilire una cooperazione tra gli Stati membri e le autorità nazionali a livello di Unione, per garantire uniformità nell’applicazione del diritto dell’UE. L’Unione si trova inoltre nella posizione migliore per garantire in maniera efficace e coerente lo stesso livello di protezione alle persone fisiche i cui dati personali siano trasferiti verso paesi terzi;
- gli Stati membri non sono in grado da soli di risolvere i problemi posti dalla situazione attuale, in particolare dalla frammentazione delle legislazioni nazionali. Conseguentemente esiste la precisa esigenza di istituire un quadro armonizzato e coerente che consenta un agevole trasferimento transfrontaliero di dati personali all’interno dell’Unione europea e che garantisca nel contempo un’effettiva tutela di tutte le persone fisiche nell’intero territorio dell’UE;
- le proposte legislative dell’UE risulteranno più efficaci rispetto ad analoghi provvedimenti adottati dai singoli Stati membri, a motivo della natura e della dimensione dei problemi che non sono confinati a uno o più Stati membri.

Il principio di proporzionalità prevede che qualsiasi intervento sia mirato e si limiti a quanto è necessario per conseguire gli obiettivi. Tale principio ha guidato l’intera elaborazione della proposta legislativa, dall’individuazione e valutazione delle opzioni strategiche alternative fino alla sua stesura.

Una direttiva è pertanto lo strumento migliore per garantire l’armonizzazione a livello dell’UE in tale settore e per dare al tempo stesso la flessibilità necessaria agli Stati membri quando attuano i principi, le norme e le rispettive esenzioni a livello nazionale. Data la complessità delle normative nazionali in vigore per la protezione dei dati personali trattati nell’ambito della cooperazione di polizia e giudiziaria in materia penale e in vista dell’obiettivo generale di armonizzare tali norme con la presente direttiva, la Commissione dovrà chiedere agli Stati membri di fornirle documenti esplicativi sui rapporti fra gli elementi della direttiva e le corrispondenti parti degli strumenti nazionali di attuazione affinché possa adempiere ai propri compiti controllando l’attuazione della presente direttiva.

### **3.3. Sintesi degli aspetti inerenti ai diritti fondamentali**

Il diritto alla protezione dei dati personali è sancito dall’articolo 8 della Carta dei diritti fondamentali dell’Unione e dall’articolo 16 del TFUE e dall’articolo 8 della convenzione europea per la salvaguardia dei diritti dell’uomo e delle libertà fondamentali (CEDU). Come sottolinea la Corte di giustizia dell’Unione europea<sup>20</sup>, il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale<sup>21</sup>. La protezione dei dati è strettamente legata al rispetto della vita privata e familiare

---

<sup>20</sup> Cause riunite C-92/09 e C-93/09: Sentenza della Corte di giustizia dell’Unione europea 9 novembre 2010 - Volker und Markus Schecke e Eifert, Racc. 2010, pag. I-0000.

<sup>21</sup> 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

tutelata dall'articolo 7 della Carta. Tale principio è riflesso nell'articolo 1, paragrafo 1, della direttiva 95/46/CE, che prevede che gli Stati membri proteggano i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla vita privata con riguardo al trattamento dei dati personali.

Altri diritti fondamentali sanciti dalla Carta e potenzialmente interessati dalla presente normativa sono 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 dei minori (articolo 24), e il diritto a un ricorso effettivo e a un giudice imparziale (articolo 47).

### **3.4. Spiegazione dettagliata della proposta**

#### *3.4.1. CAPO I - DISPOSIZIONI GENERALI*

L'articolo 1 definisce l'oggetto della direttiva, cioè le norme relative al trattamento dei dati di carattere personale a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e ne stabilisce il duplice obiettivo: tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, garantendo nel contempo un elevato livello di sicurezza pubblica, e garantire lo scambio dei dati personali tra le autorità competenti all'interno dell'Unione.

L'articolo 2 definisce il campo di applicazione della direttiva, che non è limitato al trattamento transfrontaliero dei dati ma si applica a tutte le attività di trattamento svolte da "autorità competenti" (ai sensi dell'articolo 3, paragrafo 14) ai fini della direttiva. La direttiva non si applica né al trattamento di dati nel corso di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione, né al trattamento di dati da parte di istituzioni, organi, uffici e agenzie dell'Unione, che sono soggetti al regolamento (CE) n. 45/2001 e ad altre norme specifiche.

L'articolo 3 contiene le definizioni della terminologia utilizzata nella direttiva. Mentre alcune definizioni sono mutate dalla decisione quadro 2008/977/GAI, altre sono modificate, integrate con elementi aggiuntivi, o introdotte ex novo. Nuove definizioni sono introdotte per "violazione di dati personali", "dati genetici" e "dati biometrici", "autorità competenti" (sulla base dell'articolo 87, del TFUE e dell'articolo 2, lettera h), della decisione quadro 2008/977/GAI) e "minore", basata sulla convenzione delle Nazioni Unite sui diritti del fanciullo<sup>22</sup>.

#### *3.4.2. CAPO II - PRINCIPI*

L'articolo 4 stabilisce i principi relativi al trattamento dei dati personali, rifacendosi all'articolo 6 della direttiva 95/46/CE e all'articolo 3 della decisione quadro 2008/977/GAI e adeguandoli al contesto specifico della presente direttiva.

---

<sup>22</sup> 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. Di cui anche l'articolo 2, lettera a), della direttiva 2011/92/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011, relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e che sostituisce la decisione quadro 2004/68/GAI del Consiglio (GU L 335 del 17.12.2011, pag. 1).

L'articolo 5 dispone che, nella misura del possibile, si operi una distinzione tra i dati personali di diverse categorie di interessati. Questa disposizione di nuova introduzione - non figurava infatti né nella direttiva 95/46/CE né nella decisione quadro 2008/977/GAI - era tuttavia stata proposta dalla Commissione nella sua iniziale proposta di decisione quadro<sup>23</sup> e trova giustificazione nella raccomandazione del Consiglio d'Europa n. R (87) 15. Regole analoghe sono già applicate a Europol<sup>24</sup> ed Eurojust<sup>25</sup>.

L'articolo 6 verte sul diverso grado di esattezza e affidabilità dei dati personali e si ispira al principio 3.2 della raccomandazione del Consiglio d'Europa n. R (87) 15. Norme analoghe, anch'esse riprese nella proposta di decisione quadro della Commissione, esistono per Europol<sup>26</sup>.

L'articolo 7 definisce i criteri di liceità del trattamento, quando è necessario per l'esecuzione di un compito di un'autorità competente in base al diritto nazionale, per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, per proteggere gli interessi vitali dell'interessato o di un terzo o per prevenire un'immediata e grave minaccia alla sicurezza pubblica. Gli altri motivi di trattamento lecito indicati all'articolo 7 della direttiva 95/46/CE non sono congrui al trattamento dei dati nel settore della polizia e della giustizia penale.

L'articolo 8 pone un divieto generale al trattamento di categorie particolari di dati personali, prevedendo eccezioni alla norma generale sulla base dell'articolo 8 della direttiva 95/46/CE; tra i dati il cui trattamento è vietato la direttiva aggiunge anche i dati genetici, allineandosi così alla giurisprudenza della Corte europea dei diritti dell'uomo<sup>27</sup>.

L'articolo 9 stabilisce un divieto delle misure basate sul trattamento automatizzato dei dati personali, salvo se autorizzate da una legge che contenga adeguate garanzie, in linea con l'articolo 7 della decisione quadro 2008/977/GAI.

### 3.4.3. CAPO III - DIRITTI DELL'INTERESSATO

L'articolo 10 introduce l'obbligo per gli Stati membri di garantire informazioni comprensibili e facilmente accessibili, ispirandosi in particolare al principio n. 10 della risoluzione di Madrid sulle norme internazionali sulla protezione dei dati personali e della vita privata<sup>28</sup>, così come l'obbligo per i responsabili del trattamento di fornire procedure e meccanismi per facilitare l'esercizio dei diritti dell'interessato. Ciò implica, in linea di principio, il criterio della gratuità dell'esercizio dei diritti.

L'articolo 11 dispone che gli Stati membri sono tenuti a garantire che l'interessato riceva alcune informazioni. Tali obblighi richiamano gli articoli 10 e 11 della direttiva 95/46/CE, senza separare in articoli distinti i casi in cui la raccolta avviene direttamente presso l'interessato o meno, e ampliano la portata delle informazioni da fornire. Sono previste deroghe all'obbligo di informazione, quando costituiscano misure necessarie e proporzionate in una società democratica per l'adempimento dei compiti delle autorità competenti (ispirate

---

<sup>23</sup> COM(2005) 475 definitivo.

<sup>24</sup> Articolo 14 della decisione 2009/371/GAI sull'Europol.

<sup>25</sup> Articolo 15 della decisione 2009/426/GAI sull'Eurojust.

<sup>26</sup> Articolo 14 della decisione 2009/371/GAI sull'Europol.

<sup>27</sup> Corte europea dei diritti dell'uomo, sentenza 4.12.2008, S. e Marper/Regno Unito (istanze n. 30562/04 e 30566/04).

<sup>28</sup> Adottata il 5.11.2009 dalla Conferenza internazionale dei commissari in materia di protezione dei dati e della vita privata.

all'articolo 13 della direttiva 95/46/CE e all'articolo 17 della decisione quadro 2008/977/GAI).

L'articolo 12 prevede l'obbligo per gli Stati membri di garantire il diritto di accesso dell'interessato ai propri dati personali. Richiama l'articolo 12, lettera a), della direttiva 95/46/CE, con l'aggiunta di nuovi elementi di informazione all'interessato (il periodo di conservazione dei dati, il diritto di rettifica, cancellazione o limitazione dei dati e la possibilità di proporre reclamo).

L'articolo 13 dispone che gli Stati membri possono adottare misure legislative che limitano il diritto di accesso, se ciò è reso necessario dalla specifica natura del trattamento dei dati nei settori della cooperazione di polizia e della giustizia in materia penale, prevedendo che l'interessato sia informato della limitazione all'accesso, come da articolo 17, paragrafi 2 e 3, della decisione quadro 2008/977/GAI.

L'articolo 14 introduce la disposizione secondo la quale, nei casi in cui l'accesso diretto è limitato, l'interessato deve essere informato della possibilità di un accesso indiretto per il tramite dell'autorità di controllo, che dovrebbe esercitare il diritto in sua vece e comunicargli l'esito delle verifiche effettuate.

L'articolo 15 relativo al diritto di rettifica segue l'articolo 12, lettera b), della direttiva 95/46/CE e l'articolo 18, paragrafo 1, della decisione quadro 2008/977/GAI con riferimento agli obblighi in caso di rifiuto.

L'articolo 16 relativo al diritto di cancellazione si basa sull'articolo 12, lettera b), della direttiva 95/46/CE e sull'articolo 18, paragrafo 1, della decisione quadro 2008/977/GAI con riferimento agli obblighi in caso di rifiuto. La disposizione comprende anche il diritto di chiedere che il trattamento sia contrassegnato in alcuni casi; tale formulazione permette di sostituire l'ambiguo termine di "blocco" utilizzato dall'articolo 12, lettera b), della direttiva 95/46/CE e dall'articolo 18, paragrafo 1, della decisione quadro 2008/977/GAI.

L'articolo 17 sulla rettifica, cancellazione e limitazione del trattamento nei procedimenti penali costituisce un chiarimento dell'articolo 4, paragrafo 4, della decisione quadro 2008/977/GAI.

#### *3.4.4. CAPO IV - RESPONSABILE DEL TRATTAMENTO E INCARICATO DEL TRATTAMENTO*

##### *3.4.4.1. SEZIONE 1 - OBBLIGHI GENERALI*

L'articolo 18 descrive la responsabilità del responsabile del trattamento di conformarsi alla presente direttiva e di garantirne l'effettiva conformità, anche attraverso l'adozione di politiche e meccanismi adeguati a tal fine.

L'articolo 19 stabilisce che gli Stati membri devono provvedere affinché il responsabile del trattamento si conformi agli obblighi derivanti dai principi di protezione dei dati fin dalla progettazione e di protezione di default.

L'articolo 20 precisa le relazioni che intercorrono tra corresponsabili del trattamento.

L'articolo 21 chiarisce la posizione e l'obbligo degli incaricati del trattamento, basandosi in parte sull'articolo 17, paragrafo 2, della direttiva 95/46/CE, con l'aggiunta di nuovi elementi

come il fatto che un incaricato del trattamento che non si limiti a trattare i dati in base alle istruzioni del responsabile del trattamento va considerato corresponsabile del trattamento.

L'articolo 22 sul trattamento sotto l'autorità del responsabile e dell'incaricato del trattamento riflette l'articolo 16 della direttiva 95/46/CE.

L'articolo 23 enuncia l'obbligo per i responsabili del trattamento e gli incaricati del trattamento di conservare la documentazione di tutti i sistemi e procedure di trattamento sotto la propria responsabilità.

L'articolo 24 verte sulla registrazione, conformemente all'articolo 10, paragrafo 1, della decisione quadro 2008/977, fornendo ulteriori chiarimenti.

L'articolo 25 chiarisce gli obblighi del responsabile del trattamento e dell'incaricato del trattamento ai fini della cooperazione con l'autorità di controllo.

L'articolo 26 riguarda i casi in cui la consultazione preventiva dell'autorità di controllo è obbligatoria, sulla base dell'articolo 23 della decisione quadro 2008/977/GAI.

#### 3.4.4.2. SEZIONE 2 – SICUREZZA DEI DATI

L'articolo 27 sulla sicurezza del trattamento, basata sull'attuale articolo 17, paragrafo 1, della direttiva 95/46/CE sulla sicurezza del trattamento e sull'articolo 22 della decisione quadro 2008/977/GAI del Consiglio, estende i relativi obblighi all'incaricato del trattamento, indipendentemente dal contratto in atto con il responsabile del trattamento.

Gli articoli 28 e 29 introducono l'obbligo di notificazione di una violazione di dati personali, che richiama l'analogia disposizione di cui all'articolo 4, paragrafo 3, della direttiva 2002/58/CE, precisando e operando una distinzione tra l'obbligo di notificare la violazione all'autorità di controllo (articolo 28) e l'obbligo, in determinate circostanze, di darne comunicazione all'interessato (articolo 29). L'articolo 29 prevede anche deroghe a tale obbligo, con riferimento all'articolo 11, paragrafo 4.

#### 3.4.4.3. SEZIONE 3 - RESPONSABILE DELLA PROTEZIONE DEI DATI

L'articolo 30 fa obbligo al responsabile del trattamento di designare un responsabile della protezione dei dati incaricato dello svolgimento dei compiti di cui all'articolo 32. Se più autorità competenti agiscono sotto il controllo di un'autorità centrale, che funge da responsabile del trattamento, un responsabile della protezione dei dati deve essere designato almeno dall'autorità centrale. L'articolo 18, paragrafo 2, della direttiva 95/46/CE lascia agli Stati membri l'opzione di introdurre tale obbligo in sostituzione dell'obbligo generale di notificazione preventiva, come previsto dalla direttiva.

L'articolo 31 precisa la posizione del responsabile della protezione dei dati.

L'articolo 32 definisce i compiti del responsabile della protezione dei dati.

#### 3.4.5. *CAPO V - TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI*

L'articolo 33 stabilisce i principi generali per il trasferimento di dati verso paesi terzi o organizzazioni internazionali nel settore della cooperazione di polizia e giudiziaria in materia

penale, compresi i trasferimenti successivi. Precisa che i trasferimenti di dati verso i paesi terzi sono ammessi solo se necessari a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

L'articolo 34 stabilisce che i trasferimenti verso un paese terzo sono ammessi solo se la Commissione ha adottato una decisione di adeguatezza, conformemente al regolamento (UE) n. .../2012, nei confronti di tale paese terzo, o se ciò avviene specificamente nell'ambito della cooperazione di polizia o giudiziaria in materia penale, o, in mancanza di tale decisione, se sono state poste in essere adeguate garanzie. Nelle more di una decisione di adeguatezza, la direttiva garantisce che i trasferimenti possano continuare sulla base di deroghe e in presenza di adeguate garanzie. Inoltre l'articolo specifica i criteri applicabili dalla Commissione per valutare se esista un adeguato livello di protezione, ricomprendendovi espressamente lo stato di diritto, il diritto a un ricorso effettivo e l'esistenza di un'autorità di controllo indipendente. L'articolo dispone anche che la Commissione può valutare il livello di protezione offerto da un territorio o da un settore di trattamento all'interno del paese terzo. Una decisione di adeguatezza adottata secondo le procedure di cui all'articolo 38 del regolamento generale sulla protezione dei dati è applicabile nei limiti della presente direttiva. In alternativa, la Commissione può adottare una decisione di adeguatezza esclusivamente ai fini della presente direttiva.

L'articolo 35 definisce le adeguate garanzie che devono essere offerte ai fini di un trasferimento internazionale di dati, in assenza di una decisione di adeguatezza della Commissione. Tali garanzie possono essere poste in essere con uno strumento giuridicamente vincolante, ad esempio un accordo internazionale. In alternativa, il responsabile del trattamento può concludere che tali garanzie sussistano dopo aver valutato tutte le circostanze relative al trasferimento.

L'articolo 36 definisce le deroghe per il trasferimento di dati sulla base dell'articolo 26 della direttiva 95/46/CE e dell'articolo 13 della decisione quadro 2008/977/GAI.

L'articolo 37 fa obbligo agli Stati membri di provvedere a che il responsabile del trattamento informi il destinatario delle limitazioni del trattamento e adotti tutte le misure ragionevoli per assicurare che tali limitazioni siano rispettate dai destinatari dei dati personali nel paese terzo o dall'organizzazione internazionale.

L'articolo 38 prevede espressamente lo sviluppo di meccanismi di cooperazione internazionale per la protezione dei dati personali tra la Commissione e le autorità di controllo di paesi terzi, in particolare quelli che si ritiene offrano un adeguato livello di protezione, tenendo conto della raccomandazione dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) sulla cooperazione transfrontaliera nell'applicazione delle legislazioni in materia di privacy del 12 giugno 2007.

### *3.4.6. CAPO VI - AUTORITÀ DI CONTROLLO INDIPENDENTI*

#### *3.4.6.1. SEZIONE 1 – INDIPENDENZA*

L'articolo 39 obbliga gli Stati membri a istituire una o più autorità di controllo, come già previsto dall'articolo 28, paragrafo 1, della direttiva 95/46/CE e dall'articolo 25 della decisione quadro 2008/977/GAI, e ad ampliarne i compiti affinché possano contribuire alla coerente applicazione della direttiva in tutta l'Unione; tale autorità può essere la stessa istituita a norma del regolamento generale sulla protezione dei dati.

L'articolo 40 precisa le condizioni per l'indipendenza delle autorità di controllo, ai sensi della giurisprudenza della Corte di giustizia dell'Unione europea<sup>29</sup>, ispirandosi anche all'articolo 44 del regolamento (CE) n. 45/2001<sup>30</sup>.

L'articolo 41 dispone le condizioni generali per i membri dell'autorità di controllo, in applicazione della pertinente giurisprudenza<sup>31</sup>, ispirandosi anche all'articolo 42, paragrafi da 2 a 6, del regolamento (CE) n. 45/2001.

L'articolo 42 contiene disposizioni relative all'istituzione delle autorità di controllo, comprese le condizioni applicabili ai membri, che ciascuno Stato membro deve prevedere con legge.

L'articolo 43, sul segreto professionale a cui sono tenuti i membri e il personale delle autorità di controllo, segue articolo 28, paragrafo 7, della direttiva 95/46/CE e l'articolo 25, paragrafo 4, della decisione quadro 2008/977/GAI.

#### 3.4.6.2. SEZIONE 2 - FUNZIONI E POTERI

L'articolo 44 stabilisce le competenze delle autorità di controllo sulla base dell'articolo 28, paragrafo 6, della direttiva 95/46/CE e dell'articolo 25, paragrafo 1, della decisione quadro 2008/977/GAI. Le autorità giurisdizionali, nell'esercizio della loro funzione giurisdizionale, sono esentate dal controllo esercitato dall'autorità di controllo, ma non dall'applicazione delle norme sostanziali in materia di protezione dei dati.

L'articolo 45 impone agli Stati membri di stabilire le funzioni dell'autorità di controllo, compresa quella di ricevere ed esaminare i reclami o sensibilizzare il pubblico ai rischi, alla norme e misure di salvaguardia e ai diritti. Una particolare funzione dell'autorità di controllo nel contesto della presente direttiva consiste nell'esercitare il diritto di accesso per conto dell'interessato, qualora l'accesso diretto sia negato o limitato, e verificare la liceità del trattamento dei dati.

L'articolo 46 stabilisce i poteri dell'autorità di controllo, sulla base dell'articolo 28, paragrafo 3, della direttiva 95/46/CE e dell'articolo 25, paragrafi 2 e 3, della decisione quadro 2008/977/GAI. L'articolo 47 impone alle autorità di controllo di elaborare relazioni annuali di attività, sulla base dell'articolo 28, paragrafo 5, della direttiva 95/46/CE.

#### 3.4.7. CAPO VII – COOPERAZIONE

L'articolo 48 introduce norme sull'obbligo di assistenza reciproca, a differenza dell'articolo 28, paragrafo 6, secondo trattino, della direttiva 95/46/CE che prevedeva un mero obbligo generale di collaborazione, senza ulteriori specifiche.

L'articolo 49 prevede che il comitato consultivo europeo per la protezione dei dati, istituito dal regolamento generale sulla protezione dei dati, eserciti le sue funzioni anche in relazione ai trattamenti rientranti nel campo di applicazione della presente direttiva. A integrazione dei

---

<sup>29</sup> Causa C-518/07: Sentenza della Corte di giustizia dell'Unione europea 9.3.2010 - Commissione / Germania, Racc. 2010, pag. I-1885.

<sup>30</sup> 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).

<sup>31</sup> Op. cit., nota 27.

contributi ricevuti, la Commissione chiederà il parere dei rappresentanti di autorità competenti in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali degli Stati membri, nonché dei rappresentanti di Europol ed Eurojust, tramite un gruppo di esperti sulle questioni attinenti alla protezione dei dati nelle attività di polizia e giudiziarie.

#### *3.4.8. CAPO VIII - RICORSI GIURISDIZIONALI, RESPONSABILITÀ E SANZIONI*

L'articolo 50 stabilisce il diritto di proporre reclamo all'autorità di controllo, ai sensi dell'articolo 28, paragrafo 4, della direttiva 95/46/CE, e riguarda qualsiasi infrazione della direttiva nei confronti del ricorrente. L'articolo specifica anche gli organismi, le organizzazioni o associazioni che possono presentare reclamo per conto dell'interessato o, in caso di violazione di dati personali, indipendentemente dal reclamo dell'interessato.

L'articolo 51 riguarda il diritto di proporre ricorso giurisdizionale contro un'autorità di controllo, e, sulla base delle disposizioni generali di cui all'articolo 28, paragrafo 3, della direttiva 95/46/CE, prevede esplicitamente che l'interessato può proporre ricorso giurisdizionale per obbligare l'autorità di controllo a dare seguito a un reclamo.

L'articolo 52 riguarda il diritto di proporre ricorso giurisdizionale contro un responsabile del trattamento o un incaricato del trattamento, sulla base dell'articolo 22 della direttiva 95/46/CE e dell'articolo 20 della decisione quadro 2008/977/GAI.

L'articolo 53 introduce norme comuni per i procedimenti giurisdizionali, compreso il diritto degli organismi, organizzazioni o associazioni di rappresentare in giudizio un interessato e il diritto delle autorità di controllo di avviare azioni legali. L'obbligo, imposto agli Stati membri, di garantire la rapidità del procedimento si ispira all'articolo 18, paragrafo 1, della direttiva sul commercio elettronico 2000/31/CE<sup>32</sup>.

L'articolo 54 obbliga gli Stati membri a prevedere il diritto al risarcimento, sulla base dell'articolo 23 della direttiva 95/46/CE e dell'articolo 19, paragrafo 1, della decisione quadro 2008/977/GAI, esteso ai danni causati da un incaricato del trattamento, e chiarisce la responsabilità dei corresponsabili del trattamento e dei coincaricati del trattamento.

L'articolo 55 impone agli Stati membri di definire le sanzioni applicabili alle violazioni della direttiva e di garantirne l'effettiva attuazione.

#### *3.4.9. CAPO IX - ATTI DELEGATI E ATTI DI ESECUZIONE*

L'articolo 56 contiene le clausole standard per l'esercizio delle deleghe a norma dell'articolo 290 del TFUE. Ciò consente al legislatore di delegare alla Commissione il potere di adottare atti non legislativi di portata generale che integrano o modificano determinati elementi non essenziali di un atto legislativo (atti quasi legislativi).

L'articolo 57 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.

---

<sup>32</sup> Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico») (GU L 178 del 17.7.2000, pag.1).

### *3.4.10. CAPO X - DISPOSIZIONI FINALI*

L'articolo 58 abroga la decisione quadro 2008/977/GAI.

L'articolo 59 stabilisce che rimangono impregiudicate le disposizioni specifiche per la protezione dei dati personali 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, contenute in atti dell'Unione adottati prima della data di adozione della presente direttiva.

L'articolo 60 chiarisce il rapporto della presente direttiva con accordi internazionali conclusi precedentemente dagli Stati membri nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia.

L'articolo 61 dispone che la Commissione deve valutare l'attuazione della direttiva e redigere apposite relazioni, al fine di valutare la necessità di allineare alla presente direttiva le specifiche disposizioni adottate precedentemente di cui all'articolo 59.

L'articolo 62 stabilisce l'obbligo degli Stati membri di recepire la direttiva nel diritto nazionale e comunicare alla Commissione le disposizioni adottate in applicazione della direttiva.

L'articolo 63 specifica la data di entrata in vigore della direttiva.

L'articolo 64 stabilisce i destinatari della presente direttiva.

## **4. INCIDENZA SUL BILANCIO**

La scheda finanziaria legislativa che correda la proposta di regolamento generale per la protezione dei dati riporta le implicazioni di bilancio relative al regolamento e alla presente direttiva.

Proposta di

**DIRETTIVA DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

**concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati**

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,

sentito il garante europeo della protezione dei dati<sup>33</sup>,

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

- (1) La tutela delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
- (2) Il trattamento dei dati personali è al servizio dell'uomo; i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali devono rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato. Il trattamento dei dati personali dovrebbe contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia.
- (3) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso e la tecnologia attuale consente alle competenti autorità di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività.
- (4) Tale evoluzione impone di agevolare la libera circolazione dei dati tra le autorità competenti all'interno dell'Unione e il trasferimento verso paesi terzi e organizzazioni

---

<sup>33</sup> GU C [...] del [...], pag. [...].

internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali. Ciò richiede un quadro giuridico più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione.

- (5) La direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati<sup>34</sup>, si applica a tutte le attività di trattamento di dati personali negli Stati membri nel settore pubblico e in quello privato. Non si applica invece ai trattamenti di dati personali “effettuati per l’esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario” quali le attività nei settori della cooperazione di polizia e la cooperazione giudiziaria in materia penale.
- (6) La decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell’ambito della cooperazione giudiziaria e di polizia in materia penale<sup>35</sup> si applica ai settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia. Il campo di applicazione della decisione quadro si limita al trattamento dei dati personali trasmessi o resi disponibili tra Stati membri.
- (7) Assicurare un livello uniforme ed elevato di protezione dei dati personali delle persone fisiche e facilitare lo scambio di dati personali tra le autorità competenti degli Stati membri è essenziale al fine di garantire un’efficace cooperazione di polizia e giudiziaria in materia penale. Per questo occorre un livello di tutela equivalente in tutti gli Stati membri dei diritti e delle libertà 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 di esecuzione delle sanzioni penali. Un’efficace protezione dei dati personali in tutta l’Unione presuppone il rafforzamento dei diritti delle persone cui si riferiscono i dati e degli obblighi di coloro che trattano dati personali, ma anche poteri equivalenti per controllare e garantire il rispetto delle norme di protezione dei dati personali negli Stati membri.
- (8) L’articolo 16, paragrafo 2, del trattato sul funzionamento dell’Unione europea conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati.
- (9) Su tale base, il regolamento (UE) n. .../2012 del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) stabilisce norme generali per la tutela delle persone fisiche in relazione al trattamento dei dati personali e per la libera circolazione dei dati personali nell’Unione.
- (10) Nella dichiarazione n. 21, relativa alla protezione dei dati personali nel settore 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

---

<sup>34</sup> GU L 281 del 23.11.1995, pag. 31.

<sup>35</sup> GU L 350 del 30.12.2008, pag. 60.

specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 del trattato sul funzionamento dell'Unione europea.

- (11) Occorre pertanto che una distinta direttiva, conforme alla specificità dei settori in questione, stabilisca le norme relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
- (12) Per garantire un medesimo livello di protezione alle persone fisiche attraverso diritti azionabili in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati tra le autorità competenti, è necessario che la direttiva stabilisca norme armonizzate per la protezione e la libera circolazione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia.
- (13) La presente direttiva ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali.
- (14) È necessario che la protezione prevista dalla presente direttiva si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei dati personali.
- (15) La protezione delle persone fisiche deve essere neutrale sotto il profilo tecnologico e non dipendere dalle tecniche impiegate; in caso contrario, si correrebbero gravi rischi di elusione. La protezione delle persone fisiche deve applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nel campo di applicazione della presente direttiva i fascicoli o le serie di fascicoli, e le rispettive copertine, non strutturati secondo criteri specifici. La presente direttiva non dovrebbe applicarsi né al trattamento di dati personali effettuato nell'ambito di un'attività che non rientra nel campo di applicazione del diritto dell'Unione, in particolare la sicurezza nazionale, né ai dati trattati da istituzioni, organi, uffici e agenzie dell'Unione, quali Europol o Eurojust.
- (16) È necessario applicare i principi di protezione a tutte le informazioni relative a una persona fisica identificata o identificabile. Per stabilire l'identificabilità di una persona fisica, è opportuno considerare tutti i mezzi di cui il responsabile del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona. Non è necessario applicare i principi di protezione ai dati resi sufficientemente anonimi da impedire l'identificazione dell'interessato.
- (17) Nei dati personali relativi alla salute dovrebbero rientrare, in particolare, tutti i dati riguardanti lo stato di salute di un interessato, le informazioni sulle richieste di prestazione di servizi sanitari; le informazioni sui pagamenti o l'ammissibilità all'assistenza sanitaria; un numero, simbolo o elemento specifico attribuito per identificare l'interessato in modo univoco a fini sanitari; qualsiasi informazione raccolta nel corso della prestazione di servizi sanitari a detta persona; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i campioni biologici; l'identificazione di una persona come prestatore di assistenza sanitaria all'interessato; qualsiasi informazione riguardante, ad esempio,

una malattia, l'invalidità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o l'effettivo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, ad esempio un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

- (18) Qualsiasi trattamento di dati personali deve essere lecito ed equo nei confronti dell'interessato. In particolare, dovrebbero essere esplicitati gli scopi specifici per cui i dati sono trattati.
- (19) Nell'interesse della prevenzione, dell'indagine e del perseguimento di reati, è necessario che le autorità competenti conservino e trattino i dati personali raccolti a fini di prevenzione, indagine, accertamento o perseguimento di specifici reati al di là di tale contesto, per sviluppare conoscenze dei fenomeni e delle tendenze criminali, raccogliere intelligence sulle reti del crimine organizzato e mettere in collegamento diversi reati.
- (20) I dati personali non devono essere trattati per finalità incompatibili con la finalità per la quale sono stati raccolti. I dati personali devono essere adeguati, pertinenti e non eccedere le finalità per le quali sono elaborati. Occorre adottate tutte le misure ragionevoli per garantire che i dati personali inesatti siano rettificati o cancellati.
- (21) Il principio dell'esattezza dei dati deve essere applicato tenendo conto della natura e della finalità del trattamento in questione. In particolare nei procedimenti giudiziari, le dichiarazioni contenenti dati personali sono basate sulla percezione soggettiva delle persone e non sempre sono verificabili. Il requisito dell'esattezza non deve pertanto riferirsi all'esattezza di una dichiarazione ma al semplice fatto che è stata rilasciata.
- (22) Nell'interpretare e applicare i principi generali di trattamento dei dati personali a cura delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, occorre tener conto delle specificità del settore, compresi gli obiettivi specifici perseguiti.
- (23) È inerente al trattamento dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, che siano elaborati dati personali relativi a diverse categorie di interessati. Pertanto deve essere operata, per quanto possibile, una chiara distinzione tra i dati personali relativi a diverse categorie di interessati: indiziati, condannati, vittime di reato e terzi (testimoni, persone informate, persone in contatto o collegate a indiziati o condannati).
- (24) Per quanto possibile i dati di carattere personale vanno distinti in base al loro livello di accuratezza e affidabilità. Occorre che i fatti rimangano distinti dalle valutazioni personali, al fine di garantire la protezione delle persone così come la qualità e l'affidabilità delle informazioni trattate dalle autorità competenti.
- (25) Per essere lecito, il trattamento dei dati deve essere necessario per l'esecuzione di un compito di un'autorità competente in base al diritto nazionale, per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, per proteggere gli interessi vitali dell'interessato o di un terzo o per prevenire un'immediata e grave minaccia alla sicurezza pubblica.

- (26) Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti fondamentali o della vita privata, compresi i dati genetici. Tali dati non devono essere oggetto di trattamento, salvo che tale operazione sia espressamente autorizzata per legge, che preveda adeguate garanzie a tutela degli interessi legittimi dell'interessato, oppure quando il trattamento è necessario per salvaguardare un interesse vitale dell'interessato o di un terzo, o riguardi dati resi manifestamente pubblici dall'interessato.
- (27) Ogni persona ha il diritto di non essere oggetto di una misura basata unicamente su un trattamento automatizzato se ciò produce conseguenze giuridiche pregiudizievoli nei suoi confronti, salvo quando autorizzato da una legge che precisi le misure atte a salvaguardare gli interessi legittimi dell'interessato.
- (28) Affinché l'interessato possa esercitare i propri diritti, qualsiasi informazione a questi destinata deve essere di facile accesso e comprensione, il che presuppone l'utilizzo di un linguaggio semplice e chiaro.
- (29) Occorre predisporre modalità volte ad agevolare l'esercizio dei diritti di cui alla presente direttiva, compresi i meccanismi per la richiesta, gratuita, di accedere ai dati, rettificarli e cancellarli. Il responsabile del trattamento deve essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo.
- (30) Il principio di trattamento equo implica che l'interessato sia informato in particolare dell'esistenza del trattamento e delle sue finalità, del periodo di conservazione dei dati, del diritto di accesso, rettifica o cancellazione e del diritto di proporre un reclamo. In caso di dati raccolti direttamente presso l'interessato, questi deve inoltre essere informato dell'eventuale obbligo di fornire i propri dati e delle conseguenze a cui va incontro se si rifiuta di fornirli.
- (31) L'interessato deve ricevere le informazioni relative al trattamento di dati personali al momento della raccolta o, se i dati non sono raccolti direttamente presso l'interessato, all'atto della registrazione o entro un termine ragionevole, in funzione delle circostanze del caso.
- (32) Ogni persona deve avere il diritto di accedere ai dati raccolti che la riguardano e di esercitare tale diritto facilmente, per essere consapevole del trattamento e verificarne la liceità. Occorre pertanto che ogni interessato abbia il diritto di conoscere e ottenere comunicazioni specie in relazione alla finalità del trattamento, al periodo di conservazione, ai destinatari, anche nei paesi terzi. L'interessato deve poter ricevere copia dei dati personali oggetto del trattamento.
- (33) Gli Stati membri devono poter adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato o l'accesso di questi ai suoi dati personali nella misura e per la durata in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei legittimi interessi dell'interessato, per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o la sicurezza dello Stato, o per proteggere l'interessato o i diritti e le libertà altrui.

- (34) Qualsiasi rifiuto o limitazione di accesso è comunicato per iscritto all'interessato indicando i motivi di fatto o di diritto sui quali si basa la decisione.
- (35) Nei casi in cui gli Stati membri hanno adottato disposizioni legislative volte a limitare, in tutto o in parte, il suo diritto di accesso, l'interessato deve avere il diritto di chiedere all'autorità di controllo nazionale di verificare la liceità del trattamento. È opportuno che l'interessato sia informato di tale diritto. Quando esercita il diritto di accesso per conto dell'interessato, l'autorità di controllo deve informarlo, perlomeno, di aver eseguito tutte le verifiche necessarie e comunicargli l'esito riguardo alla liceità del trattamento in questione.
- (36) Ogni persona deve avere il diritto di ottenere la rettifica di dati personali inesatti che la riguardano e il diritto alla cancellazione quando il trattamento di tali dati non è conforme ai principi fondamentali previsti dalla presente direttiva. Se i dati personali sono trattati nel corso di un'indagine penale e di un procedimento penale, la rettifica, i diritti di informazione, accesso, cancellazione e limitazione di trattamento possono essere esercitati in conformità delle norme nazionali sui procedimenti giudiziari.
- (37) Occorre stabilire una responsabilità generale del responsabile del trattamento per qualsiasi trattamento di dati personali che abbia effettuato direttamente o altri abbia effettuato per suo conto. In particolare, il responsabile del trattamento deve garantire la conformità delle attività di trattamento alle disposizioni adottate in applicazione della presente direttiva.
- (38) La tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali richiede l'attuazione di adeguate misure tecniche e organizzative per garantire il rispetto delle disposizioni della presente direttiva. Al fine di garantire la conformità con le disposizioni adottate in applicazione della presente direttiva, il responsabile del trattamento deve adottare politiche e attuare misure adeguate, che soddisfino in particolare i principi della protezione fin dalla progettazione e della protezione di default.
- (39) La protezione dei diritti e delle libertà dell'interessato così come le responsabilità dei responsabili del trattamento e degli incaricati del trattamento, esigono una chiara attribuzione delle responsabilità ai sensi della presente direttiva, compresi i casi in cui un responsabile del trattamento stabilisca le condizioni, le finalità e i mezzi del trattamento congiuntamente con altri responsabili del trattamento o quando l'operazione viene eseguita per conto del responsabile del trattamento.
- (40) Le attività di trattamento devono essere documentate dal responsabile del trattamento o dall'incaricato del trattamento, al fine di monitorare il rispetto della presente direttiva. Bisognerebbe obbligare tutti i responsabili del trattamento e gli incaricati del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detta documentazione a sua disposizione affinché possa servire per monitorare i trattamenti.
- (41) Al fine di garantire un'efficace protezione dei diritti e delle libertà dell'interessato a titolo preventivo, il responsabile del trattamento o l'incaricato del trattamento deve consultare l'autorità di controllo in alcuni casi prima del trattamento.
- (42) Una violazione di dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni all'interessato, compreso alla sua reputazione. Pertanto, non appena

viene a conoscenza di un'avvenuta violazione, il responsabile del trattamento deve notificarla all'autorità nazionale competente. È opportuno che le persone i cui dati o la cui vita privata potrebbero essere compromessi da una siffatta violazione siano informate tempestivamente affinché possano prendere le precauzioni del caso. Si considera che una violazione pregiudica i dati personali o la vita privata dell'interessato quando ad esempio comporta, in connessione con il trattamento dei dati, il furto o l'usurpazione d'identità, un danno fisico, un'umiliazione grave o attenta alla sua reputazione.

- (43) Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notificazione delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze della violazione, in particolare stabilire se i dati personali fossero o meno protetti con opportuni dispositivi tecnici atti a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto degli interessi legittimi delle competenti autorità, nei casi in cui una diffusione prematura rischi di ostacolare inutilmente l'indagine sulle circostanze della violazione.
- (44) Il responsabile del trattamento o l'incaricato del trattamento deve designare una persona che lo assiste nel controllare il rispetto delle disposizioni adottate in applicazione della presente direttiva. Un responsabile della protezione dei dati può essere designato congiuntamente per più enti dell'autorità competente. I responsabili della protezione dei dati devono poter adempiere alle funzioni e ai compiti loro incombenti in piena indipendenza e in modo efficace.
- (45) Gli Stati membri devono garantire che un trasferimento verso un paese terzo avvenga unicamente se è necessario ai fini di prevenzione, indagine, accertamento o perseguimento dei reati o di esecuzione delle sanzioni penali, e il responsabile del trattamento nel paese terzo o l'organizzazione internazionale è un'autorità competente ai sensi della presente direttiva. Il trasferimento è ammesso se la Commissione ha deciso che il paese terzo o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato, o se sono state previste idonee garanzie.
- (46) La Commissione può decidere, con effetto nell'intera Unione europea, che taluni paesi terzi, o un territorio o settore di trattamento all'interno di un paese terzo o un'organizzazione internazionale offrono un livello adeguato di protezione dei dati, garantendo in tal modo la certezza del diritto e l'uniformità in tutta l'Unione nei confronti dei paesi terzi o delle organizzazioni internazionali che si ritiene offrano un livello di protezione adeguato. In questi casi, i trasferimenti di dati personali possono avere luogo senza ulteriori autorizzazioni.
- (47) In linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo, è opportuno che la Commissione tenga conto del modo in cui tale paese rispetta lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in materia di diritti dell'uomo.
- (48) Occorre che la Commissione sia altresì in grado di riconoscere che un paese terzo o un territorio o settore di trattamento all'interno di un paese terzo o un'organizzazione internazionale non offre un adeguato livello di protezione dei dati, nel qual caso il trasferimento di dati personali verso tale paese terzo deve essere vietato, salvo se effettuato sulla base di un accordo internazionale, in presenza di adeguate garanzie o

di una deroga. È opportuno prevedere procedure di consultazione tra la Commissione e detti paesi terzi o organizzazioni internazionali. Tuttavia, la decisione della Commissione non deve pregiudicare la possibilità di procedere a trasferimenti sulla base di adeguate garanzie o sulla base di una deroga prevista dalla direttiva.

- (49) I trasferimenti non effettuati sulla base di una decisione di adeguatezza devono essere autorizzati unicamente qualora siano offerte adeguate garanzie in uno strumento giuridicamente vincolante, atto ad assicurare la protezione dei dati personali, o qualora il responsabile del trattamento o l'interessato del trattamento abbia valutato tutte le circostanze relative a un'operazione o a un insieme di operazioni di trasferimento dei dati e, sulla base di tale valutazione, ritenga che esistano adeguate garanzie in materia di protezione dei dati personali. Qualora non esistano motivi per autorizzare un trasferimento, devono essere ammesse deroghe se necessario per salvaguardare i legittimi interessi dell'interessato, qualora lo preveda la legislazione dello Stato membro che trasferisce i dati personali o quando sia indispensabile per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo, o in singoli casi per prevenire, indagare, accertare o perseguire reati o eseguire sanzioni penali, o in singoli casi per accertare, esercitare o difendere un diritto in sede giudiziaria.
- (50) Con il trasferimento transfrontaliero di dati personali aumenta il rischio che l'interessato non possa esercitare il proprio diritto alla protezione dei dati per tutelarsi da usi o divulgazioni illecite di tali dati. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche scontrarsi con poteri insufficienti per prevenire e correggere e con regimi giuridici incoerenti. Pertanto vi è la necessità di promuovere una più stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni con le loro controparti all'estero.
- (51) La designazione di un'autorità di controllo che agisca in totale indipendenza in ciascuno Stato membro è un elemento essenziale della protezione delle persone con riguardo al trattamento di dati personali. Spetterebbe alle autorità di controllo controllare l'applicazione delle disposizioni della presente direttiva e contribuire alla sua coerente applicazione in tutta l'Unione, così da tutelare le persone fisiche in relazione al trattamento dei dati personali. A tal fine le autorità di controllo cooperano tra loro e con la Commissione.
- (52) Gli Stati membri possono prevedere che l'autorità di controllo già istituita negli Stati membri ai sensi del regolamento (UE) .../2012 possa assolvere anche i compiti che devono essere adempiuti dalle autorità di controllo nazionali da istituirsi a norma della presente direttiva.
- (53) È necessario che gli Stati membri possano istituire più di una autorità di controllo, al fine di rispecchiare la loro struttura costituzionale, organizzativa e amministrativa. Ciascuna autorità di controllo deve disporre di risorse umane e finanziarie adeguate, dei locali e delle infrastrutture necessarie per l'effettivo svolgimento dei propri compiti, compresi i compiti di assistenza reciproca e cooperazione con altre autorità di controllo in tutta l'Unione.

- (54) Le condizioni generali applicabili ai membri dell'autorità di controllo devono essere stabilite da ciascuno Stato membro e devono in particolare prevedere che i membri siano nominati dal parlamento o dal governo dello Stato membro e contenere disposizioni sulle qualifiche e sulle funzioni di tali membri.
- (55) Sebbene la presente direttiva si applichi anche alle attività dei giudici nazionali, non è opportuno che rientri nella competenza delle autorità di controllo il trattamento di dati personali effettuato dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali, al fine di salvaguardarne l'indipendenza. Tuttavia, tale esenzione deve essere limitata all'attività autenticamente giurisdizionale e non applicarsi ad altre attività a cui i giudici potrebbero partecipare in forza del diritto nazionale.
- (56) Al fine di garantire un monitoraggio e un'applicazione coerenti della presente direttiva in tutta l'Unione, le autorità di controllo devono godere in ciascuno Stato membro degli stessi diritti e poteri effettivi, fra cui poteri di indagine e d'intervento giuridicamente vincolanti, di decisione e sanzione, segnatamente in caso di reclamo, così come di agire in giudizio.
- (57) È necessario che ciascuna autorità di controllo tratti i reclami proposti da qualsiasi interessato e svolga le relative indagini; che a seguito di reclamo vada condotta un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nella fattispecie; che l'autorità di controllo informi l'interessato dei progressi e dei risultati del ricorso entro un termine ragionevole. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato deve ricevere informazioni interlocutorie.
- (58) Le autorità di controllo devono prestarsi reciproca assistenza nell'esercizio delle loro funzioni, in modo da garantire la coerente applicazione e attuazione delle disposizioni adottate in conformità della presente direttiva.
- (59) Il comitato europeo per la protezione dei dati istituito con regolamento (UE) n. .../2012 deve contribuire all'applicazione uniforme della presente direttiva in tutta l'Unione, in particolare dando consulenza alla Commissione e promuovendo la cooperazione delle autorità di controllo in tutta l'Unione.
- (60) Ciascun interessato deve avere il diritto di proporre reclamo a un'autorità di controllo di qualunque Stato membro e il diritto di proporre ricorso giurisdizionale qualora ritenga che siano stati violati i diritti di cui gode a norma della presente direttiva o se l'autorità di controllo non dà seguito a un reclamo o non agisce quando è necessario intervenire per proteggere i suoi diritti di interessato.
- (61) L'organismo, l'organizzazione o associazione che intenda tutelare i diritti e gli interessi di un interessato in relazione alla protezione dei dati personali e sia istituito o istituita a norma della legislazione di uno Stato membro deve avere il diritto di proporre reclamo o esercitare il diritto a un ricorso giurisdizionale per conto dell'interessato, su suo espresso mandato, o di proporre un proprio reclamo indipendente dall'azione dell'interessato, se ritiene che sussista violazione dei dati personali.
- (62) Ogni persona fisica o giuridica deve avere diritto di proporre ricorso giurisdizionale avverso la decisione dell'autorità di controllo che la riguarda. Le azioni contro

l'autorità di controllo devono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

- (63) Gli Stati membri devono assicurare che i ricorsi giurisdizionali, per essere efficaci, consentano di adottare rapidamente provvedimenti per porre fine a una violazione della presente direttiva o per prevenirla.
- (64) Il responsabile del trattamento o l'incaricato del trattamento deve risarcire i danni cagionati da un trattamento illecito ma può essere esonerato da tale responsabilità se prova che l'evento dannoso non gli è imputabile, segnatamente se dimostra che a causare l'errore è stato l'interessato o in caso di forza maggiore.
- (65) Dovrebbe essere punibile chiunque, persona di diritto pubblico o di diritto privato, non ottemperi alle disposizioni della presente direttiva. Gli Stati membri devono garantire sanzioni efficaci, proporzionate e dissuasive e adottare tutte le misure necessarie per la loro applicazione.
- (66) Al fine di conseguire gli obiettivi della direttiva, segnatamente tutelare i diritti fondamentali e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire il libero scambio di tali dati nell'Unione tra autorità competenti, occorre conferire alla Commissione il potere di adottare atti a norma dell'articolo 290 del trattato sul funzionamento dell'Unione europea. In particolare, è necessario adottare atti delegati con riferimento alle notificazioni relative a violazioni di dati personali alle autorità di controllo. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti. Nel contesto della preparazione e della stesura degli atti delegati, occorre che la Commissione garantisca contemporaneamente una trasmissione corretta e tempestiva dei documenti pertinenti al Parlamento europeo e al Consiglio.
- (67) Occorre conferire alla Commissione competenze di esecuzione al fine di garantire condizioni uniformi di applicazione della presente direttiva per quanto riguarda la documentazione conservata dai responsabili del trattamento e incaricati del trattamento, la sicurezza del trattamento con particolare riferimento agli standard di cifratura, la notificazione di una violazione di dati personali all'autorità di controllo e l'adeguato livello di protezione offerto da un paese terzo o da un territorio o settore di trattamento nel paese terzo o un'organizzazione internazionale. Tali competenze devono essere esercitate in conformità del 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<sup>36</sup>.
- (68) È opportuno applicare la procedura d'esame per l'adozione di misure concernenti la documentazione conservata dai responsabili del trattamento e incaricati del trattamento, la sicurezza del trattamento con particolare riferimento agli standard di cifratura, la notificazione di una violazione di dati personali all'autorità di controllo e l'adeguato livello di protezione offerto da un paese terzo o da un territorio o settore di trattamento nel paese terzo o un'organizzazione internazionale, data la portata generale di tali atti.

---

<sup>36</sup> GU L 55 del 28.2.2011, pag. 13.

- (69) È opportuno che la Commissione adotti atti di esecuzione immediatamente applicabili quando, in casi debitamente giustificati relativi a un paese terzo, o a un territorio o settore di trattamento dati nel paese terzo, o un'organizzazione internazionale che non garantisce un livello di protezione adeguato, ciò sia reso necessario da imperativi motivi di urgenza.
- (70) Poiché gli obiettivi della presente direttiva, segnatamente tutelare i diritti fondamentali e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire il libero scambio di tali dati nell'Unione tra autorità competenti, non possono essere conseguiti in misura sufficiente dagli Stati membri e possono dunque, a motivo della portata e degli effetti dell'azione in questione, essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. La presente direttiva si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.
- (71) La presente direttiva dovrebbe abrogare la decisione quadro 2008/977/GAI.
- (72) Occorre che rimangano impregiudicate le disposizioni specifiche relative al trattamento dei dati personali a cura delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione delle sanzioni penali, contenute in atti dell'Unione adottati prima della data di adozione della presente direttiva e che disciplinano il trattamento dei dati personali tra Stati membri e l'accesso delle autorità nazionali designate ai sistemi di informazione istituiti ai sensi dei trattati. È necessario che la Commissione valuti la situazione sotto il profilo del rapporto tra la presente direttiva e gli atti adottati precedentemente alla data di adozione della presente direttiva che disciplinano il trattamento dei dati personali tra Stati membri e l'accesso delle autorità nazionali designate ai sistemi d'informazione istituiti ai sensi dei trattati, al fine di verificare se sia necessario allineare dette specifiche disposizioni alla presente direttiva.
- (73) Per garantire una sistematica e coerente protezione dei dati personali nell'Unione, gli accordi internazionali conclusi dagli Stati membri prima dell'entrata in vigore della presente direttiva devono essere modificati e resi conformi alla presente direttiva.
- (74) La presente direttiva non pregiudica l'applicazione delle norme relative alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile stabilite dalla direttiva 2011/92/UE del Parlamento europeo e del Consiglio, del 13 dicembre 2011<sup>37</sup>.
- (75) A norma dell'articolo 6 bis del protocollo sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, il Regno Unito o l'Irlanda non saranno vincolati da norme stabilite nella presente direttiva laddove il Regno Unito o l'Irlanda non siano vincolati da norme dell'Unione che disciplinano forme di cooperazione giudiziaria in materia penale o di cooperazione di polizia nell'ambito delle quali devono essere rispettate le disposizioni stabilite in base all'articolo 16 del trattato sul funzionamento dell'Unione europea.

---

<sup>37</sup> GU L 335 del 17.12.2011, pag. 1.

- (76) A norma degli articoli 2 e 2 bis del protocollo sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non è vincolata dalla presente direttiva né è soggetta alla sua applicazione. Dato che la presente direttiva si basa sull'acquis di Schengen in applicazione della parte terza, titolo V, del trattato sul funzionamento dell'Unione europea, la Danimarca decide, ai sensi dell'articolo 4 di tale protocollo, entro un periodo di sei mesi dall'adozione della presente direttiva, se intende recepirla nel proprio diritto interno.
- (77) Per quanto riguarda l'Islanda e la Norvegia, la presente direttiva costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo concluso dal Consiglio dell'Unione europea con la Repubblica d'Islanda e il Regno di Norvegia sulla loro associazione all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen<sup>38</sup>.
- (78) Per quanto riguarda la Svizzera, la presente direttiva costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi dell'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione di quest'ultima all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen<sup>39</sup>.
- (79) Per quanto riguarda il Liechtenstein, la presente direttiva costituisce uno sviluppo delle disposizioni dell'acquis di Schengen, ai sensi del protocollo sottoscritto tra l'Unione europea, la Comunità europea, la Confederazione svizzera e il Principato del Liechtenstein sull'adesione del Principato del Liechtenstein all'accordo tra l'Unione europea, la Comunità europea e la Confederazione svizzera riguardante l'associazione della Confederazione svizzera all'attuazione, all'applicazione e allo sviluppo dell'acquis di Schengen<sup>40</sup>.
- (80) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea e sanciti dai trattati, in particolare il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali e il diritto a un ricorso effettivo e a un giudice imparziale. Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni di tali diritti possono essere apportate 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.
- (81) Conformemente alla dichiarazione politica congiunta degli Stati membri e della Commissione sui documenti esplicativi del 28 settembre 2011, gli Stati membri si sono impegnati ad accompagnare, ove ciò sia giustificato, la notifica delle loro misure di recepimento con uno o più documenti intesi a chiarire il rapporto tra gli elementi di una direttiva e le parti corrispondenti degli strumenti nazionali di recepimento. Per quanto riguarda la presente direttiva, il legislatore ritiene che la trasmissione di tali documenti sia giustificata.
- (82) La presente direttiva non deve pregiudicare la facoltà degli Stati membri di dare attuazione all'esercizio del diritto dell'interessato di informazione, accesso, rettifica,

---

<sup>38</sup> GU L 176 del 10.7.1999, pag. 36.

<sup>39</sup> GU L 53 del 27.2.2008, pag. 52.

<sup>40</sup> GU L 160 del 18.6.2011, pag. 19.

cancellazione e limitazione dei dati personali trattati nel corso di un procedimento penale, e alle loro eventuali limitazioni nelle norme nazionali di procedura penale,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

## **CAPO I**

### **DISPOSIZIONI GENERALI**

#### *Articolo 1*

##### ***Oggetto e finalità***

1. La presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
2. In conformità della presente direttiva gli Stati membri:
  - a) tutelano i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e
  - b) garantiscono che lo scambio dei dati personali da parte delle autorità competenti all'interno dell'Unione non sia limitato né vietato per motivi attinenti alla tutela delle persone fisiche con riguardo al trattamento dei dati personali.

#### *Articolo 2*

##### ***Campo d'applicazione***

1. La presente direttiva si applica al trattamento dei dati personali da parte delle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1.
2. La presente direttiva si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.
3. Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali:
  - a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, concernenti in particolare la sicurezza nazionale;
  - b) effettuati da istituzioni, organi e organismi dell'Unione.

#### *Articolo 3*

##### ***Definizioni***

Ai fini della presente direttiva si intende per:

- (1) “interessato”: la persona fisica identificata o identificabile, direttamente o indirettamente, con mezzi che il responsabile del trattamento o altra persona fisica o giuridica ragionevolmente può utilizzare, con particolare riferimento a un numero di identificazione, a dati relativi all’ubicazione, a un identificativo on line o a uno o più elementi caratteristici della sua identità genetica, fisica, fisiologica, psichica, economica, culturale o sociale;
- (2) “dati personali”: qualsiasi informazione concernente l’interessato;
- (3) “trattamento”: qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la memorizzazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione;
- (4) “limitazione di trattamento”: contrassegno dei dati personali memorizzati con l’obiettivo di limitarne il trattamento in futuro;
- (5) “archivio”: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- (6) “responsabile del trattamento”: l’autorità pubblica competente che, singolarmente o insieme ad altri, determina le finalità, le condizioni e i mezzi del trattamento di dati personali; quando le finalità, le condizioni e i mezzi del trattamento sono determinati dal diritto dell’Unione o dal diritto di uno Stato membro, il responsabile del trattamento o i criteri specifici applicabili alla sua nomina possono essere designati dal diritto dell’Unione o dal diritto dello Stato membro;
- (7) “incaricato del trattamento”: la persona fisica o giuridica, l’autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento;
- (8) “destinatario”: la persona fisica o giuridica, l’autorità pubblica, il servizio o qualsiasi altro organismo che riceve comunicazione di dati personali;
- (9) “violazione dei dati personali”: violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l’accesso ai dati personali trasmessi, memorizzati o comunque elaborati;
- (10) “dati genetici”: tutti i dati, di qualsiasi natura, riguardanti le caratteristiche di una persona fisica che siano ereditarie o acquisite in uno stadio precoce di sviluppo prenatale;
- (11) “dati biometrici”: i dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona che ne consentono l’identificazione univoca, quali l’immagine facciale o i rilievi dattiloscopici;
- (12) “dati relativi alla salute”: qualsiasi informazione attinente alla salute fisica o mentale di una persona o alla prestazione di servizi sanitari a detta persona;

- (13) “minore”: persona di età inferiore agli anni diciotto;
- (14) “autorità competenti”: qualsiasi autorità pubblica competente a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali;
- (15) “autorità di controllo”: l’autorità pubblica istituita da uno Stato membro in conformità dell’articolo 39.

## **CAPO II**

### **PRINCIPI**

#### *Articolo 4*

#### ***Principi applicabili al trattamento di dati personali***

Gli Stati membri dispongono che i dati personali siano:

- a) trattati in modo lecito ed equo;
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità;
- c) adeguati, pertinenti e limitati al minimo necessario rispetto alle finalità perseguite;
- d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- 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;
- f) trattati sotto la responsabilità del responsabile del trattamento, che assicura la conformità alle disposizioni adottate ai sensi della presente direttiva.

#### *Articolo 5*

#### ***Distinzione tra diverse categorie di interessati***

1. Gli Stati membri dispongono che, nella misura del possibile, il responsabile del trattamento operi una chiara distinzione tra i dati personali di diverse categorie di interessati, quali:
  - a) le persone per le quali vi sono fondati motivi di ritenere che abbiano commesso o stiano per commettere un reato;
  - b) le persone condannate per un reato;
  - c) le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato;

- d) i terzi coinvolti nel reato, quali le persone che potrebbero essere chiamate a testimoniare nel corso di indagini su reati o di procedimenti penali conseguenti, le persone che possono fornire informazioni su reati, o le persone in contatto o collegate alle persone di cui alle lettere a) e b), e
- e) le persone che non rientrano in nessuna delle precedenti categorie.

#### *Articolo 6*

#### ***Diverso grado di esattezza e affidabilità dei dati personali***

1. Gli Stati membri provvedono affinché, nella misura del possibile, sia effettuata una distinzione tra diverse categorie di dati personali oggetto di trattamento in base al loro grado di esattezza e affidabilità.
2. Gli Stati membri provvedono affinché, nella misura del possibile, i dati personali fondati su fatti siano differenziati da quelli fondati su valutazioni personali.

#### *Articolo 7*

#### ***Liceità del trattamento***

Gli Stati membri dispongono che il trattamento dei dati personali sia lecito solo se e nella misura in cui è necessario:

- (a) per l'esecuzione di un compito di un'autorità competente, previsto per legge per le finalità di cui all'articolo 1, paragrafo 1, oppure
- (b) per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, oppure
- (c) per la salvaguardia degli interessi vitali dell'interessato o di un terzo, oppure
- (d) per la prevenzione di un'immediata e grave minaccia alla sicurezza pubblica.

#### *Articolo 8*

#### ***Trattamento di categorie particolari di dati personali***

1. Gli Stati membri vietano il trattamento di dati personali che rivelino la razza, l'origine etnica, le opinioni politiche, la religione o le convinzioni personali, l'appartenenza sindacale, come pure il trattamento di dati genetici o dati relativi alla salute e alla vita sessuale.
2. Il paragrafo 1 non si applica quando:
  - a) il trattamento è autorizzato da disposizioni di legge che prevedono garanzie adeguate, oppure
  - b) il trattamento è necessario per salvaguardare un interesse vitale dell'interessato o di un terzo, oppure
  - c) il trattamento riguarda dati resi manifestamente pubblici dall'interessato.

*Articolo 9*  
**Misure basate sulla profilazione e trattamento automatizzato**

1. Gli Stati membri dispongono che la misura che produca effetti giuridici negativi o significativamente incida sull'interessato e sia basata unicamente su un trattamento automatizzato di dati personali destinato a valutarne aspetti della personalità, sia vietata salvo che sia autorizzata da disposizioni di legge che precisino misure a salvaguardia dei legittimi interessi dell'interessato.
2. Il trattamento automatizzato di dati personali destinato a valutare taluni aspetti della personalità dell'interessato non può basarsi unicamente sulle categorie particolari di dati personali di cui all'articolo 8.

**CAPO III**  
**DIRITTI DELL'INTERESSATO**

*Articolo 10*  
**Modalità per l'esercizio dei diritti dell'interessato**

1. Gli Stati membri dispongono che il responsabile del trattamento prenda tutte le misure ragionevoli per applicare politiche trasparenti e facilmente accessibili con riguardo al trattamento dei dati personali e ai fini dell'esercizio dei diritti dell'interessato.
2. Gli Stati membri dispongono che il responsabile del trattamento fornisca all'interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in forma intelligibile, con linguaggio semplice e chiaro.
3. Gli Stati membri dispongono che il responsabile del trattamento prenda tutte le misure ragionevoli per stabilire le procedure d'informazione di cui all'articolo 11 e le procedure per l'esercizio dei diritti dell'interessato di cui agli articoli da 12 a 17.
4. Gli Stati membri dispongono che il responsabile del trattamento informi l'interessato senza ingiustificato ritardo del seguito dato alle sue richieste.
5. Gli Stati membri dispongono che le informazioni e le misure prese dal responsabile del trattamento a seguito di una richiesta ai sensi dei paragrafi 3 e 4 siano gratuite. Se le richieste sono vessatorie, in particolare per il carattere ripetitivo, la lunghezza o il volume, il responsabile del trattamento può esigere un contributo spese per le informazioni o l'azione richiesta; in alternativa, può non effettuare quanto richiesto. In tale caso, incombe al responsabile del trattamento dimostrare il carattere vessatorio della richiesta.

*Articolo 11*  
**Informazione dell'interessato**

1. In caso di raccolta di dati personali, gli Stati membri provvedono affinché il responsabile del trattamento predisponga adeguate misure per fornire all'interessato almeno le seguenti informazioni:
  - a) l'identità e le coordinate di contatto del responsabile del trattamento e del responsabile della protezione dei dati;
  - b) le finalità del trattamento cui sono destinati i dati personali;
  - c) il periodo per il quale i dati personali saranno conservati;
  - d) l'esistenza del diritto dell'interessato di chiedere al responsabile del trattamento l'accesso ai dati e la rettifica o la cancellazione dei dati personali che lo riguardano o la limitazione di trattamento;
  - e) il diritto di proporre reclamo all'autorità di controllo di cui all'articolo 39 e le coordinate di contatto di detta autorità;
  - f) i destinatari o le categorie di destinatari dei dati personali, anche in paesi terzi o in seno a organizzazioni internazionali;
  - g) ogni altra informazione necessaria per garantire un trattamento equo nei confronti dell'interessato, in considerazione delle specifiche circostanze in cui i dati personali vengono trattati.
2. Quando i dati personali sono raccolti direttamente presso l'interessato, il responsabile del trattamento lo informa, in aggiunta a quanto disposto al paragrafo 1, dell'obbligatorietà o meno della comunicazione dei dati personali e delle possibili conseguenze di una mancata comunicazione.
3. Il responsabile del trattamento fornisce le informazioni di cui al paragrafo 1:
  - a) al momento in cui i dati personali sono ottenuti dall'interessato, oppure
  - b) quando i dati personali non sono raccolti direttamente presso l'interessato, al momento della registrazione o entro un termine ragionevole dopo la raccolta, in considerazione delle specifiche circostanze in cui i dati vengono trattati.
4. Gli Stati membri possono adottare misure legislative volte a ritardare, limitare o omettere l'informazione dell'interessato nella misura e per la durata in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei legittimi interessi dell'interessato:
  - (a) per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
  - (b) per non compromettere la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali;
  - (c) per proteggere la sicurezza pubblica;
  - (d) per proteggere la sicurezza dello Stato;

- (e) per proteggere i diritti e le libertà di terzi.
5. Gli Stati membri hanno facoltà di determinare le categorie di trattamenti di dati cui possono applicarsi, in tutto o in parte, le deroghe di cui al paragrafo 4.

#### *Articolo 12*

#### ***Diritto di accesso dell'interessato***

1. Gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal responsabile del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano. Se è in corso un trattamento, il responsabile del trattamento fornisce le 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 comunicati, in particolare se destinatari di paesi terzi;
  - d) il periodo per il quale saranno conservati i dati personali;
  - e) l'esistenza del diritto dell'interessato di chiedere al responsabile del trattamento la rettifica o la cancellazione dei dati personali che lo riguardano o la limitazione di trattamento;
  - f) il diritto di proporre reclamo all'autorità di controllo e le coordinate di contatto di detta autorità;
  - g) la comunicazione dei dati personali oggetto del trattamento e di tutte le informazioni disponibili sulla loro origine.
2. Gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal responsabile del trattamento copia dei dati personali oggetto del trattamento.

#### *Articolo 13*

#### ***Limitazioni del diritto di accesso***

1. Gli Stati membri possono adottare misure legislative volte a limitare, in tutto o in parte, il diritto di accesso dell'interessato nella misura in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei legittimi interessi dell'interessato:
- (a) per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
  - (b) per non compromettere la prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali;
  - (c) per proteggere la sicurezza pubblica;
  - (d) per proteggere la sicurezza dello Stato;

- (e) per proteggere i diritti e le libertà di terzi.
2. Gli Stati membri hanno facoltà di determinare con legge le categorie di trattamenti di dati cui possono applicarsi, in tutto o in parte, le deroghe di cui al paragrafo 1.
  3. Nei casi di cui ai paragrafi 1 e 2, gli Stati membri dispongono che il responsabile del trattamento informi per iscritto l'interessato di ogni rifiuto o limitazione dell'accesso, dei motivi del rifiuto e delle possibilità di proporre reclamo all'autorità di controllo e di proporre ricorso giurisdizionale. Le informazioni sui motivi di fatto o di diritto su cui si basa la decisione possono essere omesse qualora la loro comunicazione rischi di compromettere una delle finalità di cui al paragrafo 1.
  4. Gli Stati membri provvedono affinché il responsabile del trattamento documenti i motivi per cui ha omesso di comunicare i motivi di fatto o di diritto su cui si basa la decisione.

#### *Articolo 14*

##### ***Modalità per l'esercizio del diritto di accesso***

1. Gli Stati membri dispongono che l'interessato abbia il diritto di chiedere, in particolare nei casi di cui all'articolo 13, che l'autorità di controllo verifichi la liceità del trattamento.
2. Gli Stati membri dispongono che il responsabile del trattamento informi l'interessato del diritto di chiedere l'intervento dell'autorità di controllo ai sensi del paragrafo 1.
3. Qualora l'interessato eserciti il diritto di cui al paragrafo 1, l'autorità di controllo lo informa quanto meno dell'avvenuto espletamento di tutte le verifiche necessarie e del loro esito riguardo alla liceità del trattamento in questione.

#### *Articolo 15*

##### ***Diritto di rettifica***

1. Gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal responsabile del trattamento la rettifica di dati personali inesatti. L'interessato ha il diritto di ottenere l'integrazione di dati personali incompleti, anche mediante una dichiarazione rettificativa.
2. Gli Stati membri dispongono che il responsabile del trattamento informi per iscritto l'interessato di ogni rifiuto di rettifica, dei motivi del rifiuto e delle possibilità di proporre reclamo all'autorità di controllo e di proporre ricorso giurisdizionale.

#### *Articolo 16*

##### ***Diritto alla cancellazione***

1. Gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali qualora il trattamento non sia conforme alle disposizioni adottate ai sensi dell'articolo 4, lettere da a) a e), dell'articolo 7 e dell'articolo 8, della presente direttiva.

2. Il responsabile del trattamento provvede senza ritardo alla cancellazione.
3. Invece di provvedere alla cancellazione, il responsabile del trattamento contrassegna i dati personali:
  - (a) quando l'interessato ne contesta l'esattezza, per il periodo necessario ad effettuare le opportune verifiche;
  - (b) quando i dati personali devono essere conservati a fini probatori;
  - (c) quando l'interessato si oppone alla loro cancellazione e chiede invece che ne sia limitato l'utilizzo.
4. Gli Stati membri dispongono che il responsabile del trattamento informi per iscritto l'interessato di ogni rifiuto di cancellare o contrassegnare i dati trattati, dei motivi del rifiuto e delle possibilità di proporre reclamo all'autorità di controllo e di proporre ricorso giurisdizionale.

#### *Articolo 17*

#### ***Diritti dell'interessato nel corso di indagini e procedimenti penali***

Gli Stati membri possono disporre che il diritto di informazione, accesso, rettifica, cancellazione e limitazione di trattamento di cui agli articoli da 11 a 16 sia esercitato in conformità delle norme nazionali sui procedimenti giudiziari qualora i dati personali figurino in una decisione giudiziaria o in un casellario giudiziario oggetto di trattamento nel corso di un'indagine o di un procedimento penale.

## **CAPO IV RESPONSABILE DEL TRATTAMENTO E INCARICATO DEL TRATTAMENTO**

### **SEZIONE 1 OBBLIGHI GENERALI**

#### *Articolo 18*

#### ***Responsabilità del responsabile del trattamento***

1. Gli Stati membri dispongono che il responsabile del trattamento adotti politiche e attui misure adeguate per garantire che il trattamento dei dati personali effettuato sia conforme alle disposizioni adottate ai sensi della presente direttiva.
2. Le misure di cui al paragrafo 1 comprendono, in particolare:
  - a) la conservazione della documentazione ai sensi dell'articolo 23;
  - b) il rispetto dei requisiti di consultazione preventiva ai sensi dell'articolo 26;
  - c) l'attuazione dei requisiti di sicurezza dei dati di cui all'articolo 27;

- d) la designazione di un responsabile della protezione dei dati ai sensi dell'articolo 30.
3. Il responsabile del trattamento mette in atto meccanismi per assicurare la verifica dell'efficacia delle misure di cui al paragrafo 1. Qualora ciò sia proporzionato, la verifica è effettuata da revisori interni o esterni indipendenti.

#### *Articolo 19*

#### ***Protezione dei dati fin dalla progettazione e protezione di default***

1. Gli Stati membri dispongono che il responsabile del trattamento, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, metta in atto adeguate misure e procedure tecniche e organizzative in modo tale che il trattamento sia conforme alle disposizioni adottate ai sensi della presente direttiva e assicuri la tutela dei diritti dell'interessato.
2. Il responsabile del trattamento mette in atto meccanismi per garantire che siano trattati, di default, solo i dati personali necessari per le finalità del trattamento.

#### *Articolo 20*

#### ***Corresponsabili del trattamento***

Gli Stati membri dispongono che se il responsabile del trattamento determina le finalità, le condizioni e i mezzi del trattamento dei dati personali insieme ad altri, i corresponsabili del trattamento determinino, mediante accordi interni, le rispettive responsabilità in merito al rispetto delle disposizioni adottate ai sensi della presente direttiva, con particolare riguardo alle procedure e ai meccanismi per l'esercizio dei diritti dell'interessato.

#### *Articolo 21*

#### ***Incaricato del trattamento***

1. Gli Stati membri dispongono che qualora il trattamento debba essere effettuato per conto del responsabile del trattamento, questi scelga un incaricato del trattamento che presenti garanzie sufficienti per mettere in atto misure e procedure tecniche e organizzative adeguate in modo tale che il trattamento sia conforme alle disposizioni adottate ai sensi della presente direttiva e assicuri la tutela dei diritti dell'interessato.
2. Gli Stati membri dispongono che l'esecuzione dei trattamenti su commissione sia disciplinata da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente che l'incaricato del trattamento agisca soltanto su istruzione del responsabile del trattamento, in particolare qualora sia vietato il trasferimento dei dati personali usati.
3. L'incaricato del trattamento che tratta i dati personali diversamente da quanto indicato nelle istruzioni del responsabile del trattamento è considerato responsabile del trattamento per tale trattamento ed è soggetto alle norme sui corresponsabili del trattamento di cui all'articolo 20.

*Articolo 22*  
**Trattamento sotto l'autorità del responsabile del trattamento e dell'incaricato del trattamento**

Gli Stati membri dispongono che l'incaricato del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento, che abbia accesso a dati personali non possa trattare tali dati se non è istruito in tal senso dal responsabile del trattamento, salvo che lo richieda il diritto dell'Unione o di uno Stato membro.

*Articolo 23*  
**Documentazione**

1. Gli Stati membri dispongono che ogni responsabile del trattamento e incaricato del trattamento conservi la documentazione di tutti i sistemi e procedure di trattamento sotto la propria responsabilità.
2. La documentazione contiene almeno le seguenti informazioni:
  - a) nome e coordinate di contatto del responsabile del trattamento, o di ogni coresponsabile del trattamento o incaricato del trattamento;
  - b) finalità del trattamento;
  - c) indicazione dei destinatari o delle categorie di destinatari dei dati personali;
  - d) indicazione dei trasferimenti di dati verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale.
3. Il responsabile del trattamento e l'incaricato del trattamento mettono la documentazione a disposizione dell'autorità di controllo, su richiesta.

*Articolo 24*  
**Registrazione**

1. Gli Stati membri provvedono affinché siano registrati almeno i seguenti trattamenti: raccolta, modifica, consultazione, comunicazione, interconnessione e cancellazione. Le registrazioni delle consultazioni e delle comunicazioni indicano in particolare la finalità, la data e l'ora del trattamento e, nella misura del possibile, l'identificazione della persona che ha consultato o comunicato i dati personali.
2. Le registrazioni sono usate esclusivamente ai fini della verifica della liceità del trattamento dei dati, dell'autocontrollo e per garantire l'integrità e la sicurezza dei dati.

*Articolo 25*  
**Cooperazione con l'autorità di controllo**

1. Gli Stati membri dispongono che il responsabile del trattamento e l'incaricato del trattamento cooperino, su richiesta, con l'autorità di controllo nell'esercizio delle sue

funzioni, fornendo in particolare tutte le informazioni necessarie all'esercizio delle sue funzioni.

2. Quando l'autorità di controllo esercita i poteri a norma dell'articolo 46, lettere a) e b), il responsabile del trattamento e l'incaricato del trattamento rispondono a una a sua richiesta entro un termine ragionevole. La risposta comprende una descrizione delle misure prese a seguito delle osservazioni dell'autorità di controllo e dei risultati raggiunti.

#### *Articolo 26*

#### ***Consultazione preventiva dell'autorità di controllo***

1. Gli Stati membri provvedono affinché il responsabile del trattamento o l'incaricato del trattamento consulti l'autorità di controllo prima di trattare dati personali che figureranno in un nuovo archivio di prossima creazione se:
  - a) si tratta delle categorie particolari di dati di cui all'articolo 8;
  - b) il tipo di trattamento, in particolare il ricorso a tecnologie, procedure o meccanismi nuovi, comporta per altri versi rischi specifici per i diritti e le libertà fondamentali dell'interessato, segnatamente per quanto attiene alla protezione dei dati personali.
2. Gli Stati membri possono disporre che l'autorità di controllo stabilisca un elenco di trattamenti soggetti a consultazione preventiva ai sensi del paragrafo 1.

## **SEZIONE 2 SICUREZZA DEI DATI**

#### *Articolo 27*

#### ***Sicurezza del trattamento***

1. Gli Stati membri dispongono che, tenuto conto dell'evoluzione tecnica e dei costi di attuazione, il responsabile del trattamento e l'incaricato del trattamento mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza appropriato, in relazione ai rischi che il trattamento comporta e alla natura dei dati personali da proteggere.
2. Ciascuno Stato membro dispone che per il trattamento automatizzato dei dati il responsabile del trattamento o l'incaricato del trattamento, previa valutazione dei rischi, metta in atto misure volte a:
  - (a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento di dati personali (controllo dell'accesso alle attrezzature);
  - (b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate (controllo dei supporti di dati);

- (c) impedire che i dati siano inseriti senza autorizzazione e che i dati personali memorizzati siano visionati, modificati o cancellati senza autorizzazione (controllo della memorizzazione);
  - (d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato di dati mediante attrezzature per la trasmissione di dati (controllo dell'utente);
  - (e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato di dati abbiano accesso solo ai dati cui si riferisce la loro autorizzazione d'accesso (controllo dell'accesso ai dati);
  - (f) garantire la possibilità di verificare e accertare a quali organismi siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati (controllo della trasmissione);
  - (g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato dei dati, il momento dell'introduzione e la persona che l'ha effettuata (controllo dell'introduzione);
  - (h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati da persone non autorizzate durante i trasferimenti di dati personali o il trasporto di supporti di dati (controllo del trasporto);
  - (i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati (recupero);
  - (j) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati (affidabilità) e che i dati personali memorizzati non possano essere falsati da un errore di funzionamento del sistema (autenticità).
3. Se necessario, la Commissione può adottare atti di esecuzione per precisare i requisiti di cui ai paragrafi 1 e 2 in varie situazioni, in particolare gli standard di cifratura. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 57, paragrafo 2.

#### *Articolo 28*

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

1. Gli Stati membri dispongono che, in caso di violazione dei dati personali, il responsabile del trattamento notifichi la violazione all'autorità di controllo senza ritardo, ove possibile entro 24 ore dal momento in cui ne è venuto a conoscenza. Qualora non proceda alla notificazione entro 24 ore, il responsabile del trattamento trasmette, su richiesta, all'autorità di controllo una giustificazione motivata.
2. L'incaricato del trattamento allerta e informa il responsabile del trattamento immediatamente dopo aver accertato la violazione.
3. La notificazione di cui al paragrafo 1 deve come minimo:

- a) descrivere la natura della violazione dei dati personali, compresi le categorie e il numero di interessati in questione e le categorie e il numero di registrazioni dei dati in questione;
  - b) indicare l'identità e le coordinate di contatto del responsabile della protezione dei dati di cui all'articolo 30 o di altro punto di contatto presso cui ottenere più informazioni;
  - c) elencare le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione dei dati personali;
  - d) descrivere le possibili conseguenze della violazione dei dati personali;
  - e) descrivere le misure proposte o adottate dal responsabile del trattamento per porre rimedio alla violazione dei dati personali.
4. Gli Stati membri dispongono che il responsabile del trattamento documenti la violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. La documentazione deve consentire all'autorità di controllo di verificare il rispetto del presente articolo. In essa figurano unicamente le informazioni necessarie a tal fine.
5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 56 al fine di precisare i criteri e i requisiti concernenti l'accertamento della violazione di dati personali di cui ai paragrafi 1 e 2 e le circostanze particolari in cui il responsabile del trattamento e l'incaricato del trattamento sono tenuti a notificare la violazione.
6. La Commissione può stabilire il formato standard di tale notificazione all'autorità di controllo, le procedure applicabili all'obbligo di notificazione e la forma e le modalità della documentazione di cui al paragrafo 4, compresi i termini per la cancellazione delle informazioni ivi contenute. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 57, paragrafo 2.

#### *Articolo 29*

##### ***Comunicazione di una violazione dei dati personali all'interessato***

1. Gli Stati membri dispongono che quando la violazione dei dati personali rischia di pregiudicare i dati personali o di attentare alla vita privata dell'interessato, il responsabile del trattamento, dopo aver provveduto alla notificazione di cui all'articolo 28, comunichi la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 descrive la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'articolo 28, paragrafo 3, lettere b) e c).
3. Non è richiesta la comunicazione di una violazione dei dati personali all'interessato se il responsabile del trattamento dimostra in modo convincente all'autorità di controllo che ha utilizzato le opportune misure tecnologiche di protezione e che tali misure erano state applicate ai dati violati. Tali misure tecnologiche di protezione devono rendere i dati incomprensibili a chiunque non sia autorizzato ad accedervi.

4. La comunicazione all'interessato può essere ritardata, limitata od omessa per i motivi di cui all'articolo 11, paragrafo 4.

### **SEZIONE 3**

## **RESPONSABILE DELLA PROTEZIONE DEI DATI**

#### *Articolo 30*

#### ***Designazione del responsabile della protezione dei dati***

1. Gli Stati membri dispongono che il responsabile del trattamento o l'incaricato del trattamento designi un responsabile della protezione dei dati.
2. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti di cui all'articolo 32.
3. Il responsabile della protezione dei dati può essere designato per più enti, tenuto conto della struttura organizzativa dell'autorità competente.

#### *Articolo 31*

#### ***Posizione del responsabile della protezione dei dati***

1. Gli Stati membri dispongono che il responsabile del trattamento o l'incaricato del trattamento si assicuri che il responsabile della protezione dei dati sia prontamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il responsabile del trattamento o l'incaricato del trattamento si assicura che il responsabile della protezione dei dati disponga dei mezzi per adempiere alle funzioni e ai compiti di cui all'articolo 32 in modo efficace ed indipendente e non riceva istruzione alcuna per quanto riguarda l'esercizio della carica.

#### *Articolo 32*

#### ***Compiti del responsabile della protezione dei dati***

Gli Stati membri dispongono che il responsabile del trattamento o l'incaricato del trattamento conferisca al responsabile della protezione dei dati almeno i seguenti compiti:

- (a) informare e consigliare il responsabile del trattamento o l'incaricato del trattamento in merito agli obblighi derivanti dalle disposizioni adottate ai sensi della presente direttiva e conservare la documentazione relativa a tale attività e alle risposte ricevute;
- (b) sorvegliare l'attuazione e l'applicazione delle politiche in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi;

- (c) sorvegliare l'attuazione e l'applicazione delle disposizioni adottate ai sensi della presente direttiva, con particolare riguardo ai requisiti concernenti la protezione fin dalla progettazione, la protezione di default, la sicurezza dei dati, l'informazione dell'interessato e le richieste degli interessati di esercitare i diritti riconosciuti dalle disposizioni adottate ai sensi della presente direttiva;
- (d) garantire la conservazione della documentazione di cui all'articolo 23;
- (e) controllare che le violazioni dei dati personali siano documentate, notificate e comunicate ai sensi degli articoli 28 e 29;
- (f) controllare che sia presentata domanda di consultazione preventiva all'autorità di controllo nei casi previsti dall'articolo 26;
- (g) controllare che sia dato seguito alle richieste dell'autorità di controllo e, nell'ambito delle sue competenze, cooperare con l'autorità di controllo di propria iniziativa o su sua richiesta;
- (h) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento e, se del caso, consultare l'autorità di controllo di propria iniziativa.

## **CAPO V**

### **TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI**

#### *Articolo 33*

#### ***Principi generali per il trasferimento***

Gli Stati membri dispongono che sia ammesso il trasferimento, a cura di un'autorità competente, 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, compreso il trasferimento successivo verso un altro paese terzo o un'altra organizzazione internazionale, soltanto se:

- a) è necessario a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e
- b) il responsabile del trattamento e l'incaricato del trattamento rispettano le condizioni indicate nel presente capo.

#### *Articolo 34*

#### ***Trasferimento previa decisione di adeguatezza***

1. Gli Stati membri dispongono che sia ammesso il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale se la Commissione ha deciso, conformemente all'articolo 41 del regolamento (UE) .../2012 o al paragrafo 3 del presente articolo, che il paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o l'organizzazione internazionale in questione garantisce un livello

di protezione adeguato. In tal caso il trasferimento non necessita di ulteriori autorizzazioni.

2. In mancanza di decisione adottata conformemente all'articolo 41 del regolamento (UE) ..../2012, la Commissione valuta l'adeguatezza del livello di protezione prendendo in considerazione i seguenti elementi:
  - a) lo stato di diritto, la pertinente legislazione generale e settoriale vigente, anche in materia penale, di pubblica sicurezza, difesa e sicurezza nazionale, e le misure di sicurezza osservate nel paese terzo o dall'organizzazione internazionale in questione, nonché i diritti effettivi e azionabili, compreso il diritto degli interessati a un ricorso effettivo in sede amministrativa e giudiziaria, in particolare quelli che risiedono nell'Unione e i cui dati personali sono oggetto di trasferimento;
  - b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o nell'organizzazione internazionale in questione, incaricate di garantire il rispetto delle norme di protezione dei dati, assistere e consigliare gli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo dell'Unione e degli Stati membri, e
  - c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione.
3. La Commissione può decidere, nei limiti della presente direttiva, che un paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o un'organizzazione internazionale garantisce un livello di protezione adeguato ai sensi del paragrafo 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 57, paragrafo 2.
4. L'atto di esecuzione specifica il proprio campo di applicazione geografico e settoriale e, se del caso, identifica l'autorità di controllo di cui al paragrafo 2, lettera b).
5. La Commissione può decidere, nei limiti della presente direttiva, che un paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o un'organizzazione internazionale non garantisce un livello di protezione adeguato ai sensi del paragrafo 2, in particolare nei casi in cui la pertinente legislazione generale e settoriale vigente nel paese terzo o per l'organizzazione internazionale in questione non garantisce diritti effettivi e azionabili, compreso il diritto degli interessati a un ricorso effettivo in sede amministrativa e giudiziaria, in particolare quelli i cui dati personali sono oggetto di trasferimento. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 57, paragrafo 2, o, in casi di estrema urgenza per gli interessati relativamente al loro diritto alla protezione dei dati, secondo la procedura di cui all'articolo 57, paragrafo 3.
6. Gli Stati membri provvedono affinché quando la Commissione decide, ai sensi del paragrafo 5, che è vietato il trasferimento di dati personali verso il paese terzo, o un territorio o settore di trattamento all'interno del paese terzo, o verso l'organizzazione internazionale in questione, tale decisione faccia salvi i trasferimenti ai sensi dell'articolo 35, paragrafo 1, o dell'articolo 36. La Commissione avvia, al momento

opportuno, consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla situazione risultante dalla decisione di cui al paragrafo 5.

7. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* l'elenco dei paesi terzi, dei territori e settori di trattamento all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è garantito un livello di protezione adeguato.
8. La Commissione sorveglia l'applicazione degli atti di esecuzione di cui ai paragrafi 3 e 5.

#### *Articolo 35*

#### ***Trasferimento in presenza di garanzie adeguate***

1. Se la Commissione non ha preso alcuna decisione ai sensi dell'articolo 34, gli Stati membri dispongono che il trasferimento di dati personali a un destinatario in un paese terzo o presso un'organizzazione internazionale possa aver luogo se:
  - a) sono offerte garanzie adeguate per la protezione dei dati personali in uno strumento giuridicamente vincolante, oppure
  - b) il responsabile del trattamento o l'incaricato del trattamento ha valutato tutte le circostanze relative al trasferimento dei dati personali e ritiene che sussistano garanzie adeguate per la protezione dei dati personali.
2. La decisione di trasferimento ai sensi del paragrafo 1, lettera b), è presa da personale debitamente autorizzato. Il trasferimento è documentato e, su richiesta, la documentazione è messa a disposizione dell'autorità di controllo.

#### *Articolo 36*

#### ***Deroghe***

In deroga agli articoli 34 e 35, gli Stati membri dispongono che sia ammesso il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale soltanto a condizione che:

- a) il trasferimento sia necessario per salvaguardare un interesse vitale dell'interessato o di un terzo, oppure
- b) il trasferimento sia necessario per salvaguardare i legittimi interessi dell'interessato qualora lo preveda la legislazione dello Stato membro che trasferisce i dati personali, oppure
- c) il trasferimento dei dati sia essenziale per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo, oppure
- d) il trasferimento sia necessario, in singoli casi, per prevenire, indagare, accertare o perseguire reati o eseguire sanzioni penali, oppure

- e) il trasferimento sia necessario, in singoli casi, per accertare, esercitare o difendere un diritto in sede giudiziaria in relazione alla prevenzione, all'indagine, all'accertamento o al perseguimento di uno specifico reato o all'esecuzione di una specifica sanzione penale.

*Articolo 37*

***Condizioni specifiche per il trasferimento di dati personali***

Gli Stati membri prevedono che il responsabile del trattamento informi il destinatario dei dati personali di ogni limitazione di trattamento e prenda tutte le misure ragionevoli per garantirne il rispetto.

*Articolo 38*

***Cooperazione internazionale per la protezione dei dati personali***

1. In relazione ai paesi terzi e alle organizzazioni internazionali, la Commissione e gli Stati membri adottano misure appropriate per:
  - (a) sviluppare efficaci meccanismi di cooperazione internazionale per facilitare l'applicazione della legislazione sulla protezione dei dati personali;
  - (b) prestare assistenza reciproca a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, in particolare mediante notificazione, deferimento dei reclami, assistenza alle indagini e scambio di informazioni, fatte salve garanzie adeguate per la protezione dei dati personali e gli altri diritti e libertà fondamentali;
  - (c) coinvolgere le parti interessate pertinenti in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione sulla protezione dei dati personali;
  - (d) promuovere lo scambio e la documentazione delle legislazioni e pratiche in materia di protezione dei dati personali.
2. Ai fini del paragrafo 1, la Commissione adotta le misure appropriate per intensificare i rapporti con quei paesi terzi e quelle organizzazioni internazionali, in particolare le loro autorità di controllo, per cui abbia deciso che garantiscono un livello adeguato di protezione ai sensi dell'articolo 34, paragrafo 3.

**CAPO VI**  
**AUTORITÀ DI CONTROLLO INDIPENDENTI**  
**SEZIONE 1**  
**INDIPENDENZA**

*Articolo 39*  
***Autorità di controllo***

1. Ogni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare l'applicazione delle disposizioni adottate ai sensi della presente direttiva e di contribuire alla sua coerente applicazione in tutta l'Unione, al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali e di agevolare la libera circolazione dei dati personali all'interno dell'Unione. A tale scopo le autorità di controllo cooperano tra loro e con la Commissione.
2. Gli Stati membri possono disporre che l'autorità di controllo istituita negli Stati membri ai sensi del regolamento (UE) ..../2012 assolva i compiti dell'autorità di controllo da istituirsi ai sensi del paragrafo 1
3. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che funge da punto di contatto unico per l'effettiva partecipazione di tali autorità al comitato europeo per la protezione dei dati.

*Articolo 40*  
***Indipendenza***

1. Gli Stati membri provvedono affinché l'autorità di controllo eserciti le sue funzioni e i suoi poteri in piena indipendenza.
2. Ogni Stato membro dispone che nell'adempimento delle loro funzioni i membri dell'autorità di controllo non sollecitino né accettino istruzioni da alcuno.
3. Per tutta la durata del mandato, i membri dell'autorità di controllo si astengono da qualunque azione incompatibile con le loro funzioni e non possono esercitare alcuna altra attività professionale incompatibile, remunerata o meno.
4. Al termine del mandato i membri dell'autorità di controllo agiscono con integrità e discrezione nell'accettazione di nomine e altri benefici.
5. Ogni Stato membro provvede affinché l'autorità di controllo sia dotata di risorse umane, tecniche e finanziarie adeguate, dei locali e delle infrastrutture necessarie per l'effettivo esercizio delle sue funzioni e dei suoi poteri, compresi quelli nell'ambito dell'assistenza reciproca, della cooperazione e della partecipazione attiva al comitato europeo per la protezione dei dati.

6. Ogni Stato membro provvede affinché l'autorità di controllo abbia il proprio personale, nominato dal responsabile dell'autorità di controllo e soggetto alla direzione di quest'ultimo.
7. Gli Stati membri garantiscono che l'autorità di controllo sia soggetta a un controllo finanziario che non ne pregiudichi l'indipendenza. Gli Stati membri garantiscono che l'autorità di controllo disponga di bilanci annuali separati. I bilanci sono pubblicati.

#### *Articolo 41*

#### ***Condizioni generali per i membri dell'autorità di controllo***

1. Ogni Stato membro dispone che a nominare i membri dell'autorità di controllo debba essere il proprio parlamento o governo.
2. I membri sono scelti tra personalità che offrono ogni garanzia di indipendenza e che possiedono un'esperienza e competenze notorie per l'esercizio delle loro funzioni.
3. Il mandato dei membri cessa alla scadenza del termine o in caso di dimissioni o di provvedimento d'ufficio, a norma del paragrafo 5.
4. I membri possono essere rimossi o privati del diritto a pensione o di altri vantaggi sostitutivi dall'autorità giurisdizionale nazionale competente qualora non siano più in possesso dei requisiti necessari per l'esercizio delle loro funzioni o abbiano commesso una colpa grave.
5. Allo scadere del mandato o qualora rassegni le sue dimissioni, il membro continua a esercitare le sue funzioni fino alla nomina di un nuovo membro.

#### *Articolo 42*

#### ***Norme sull'istituzione dell'autorità di controllo***

Ogni Stato membro prevede con legge:

- a) l'istituzione e lo status dell'autorità di controllo in conformità degli articoli 39 e 40;
- b) le qualifiche, l'esperienza e le competenze richieste per l'esercizio delle funzioni di membro dell'autorità di controllo;
- c) le norme e le procedure per la nomina dei membri dell'autorità di controllo, e le norme sulle attività o professioni incompatibili con le loro funzioni;
- d) la durata del mandato dei membri dell'autorità di controllo, che non può essere inferiore a quattro anni, salvo per le prime nomine dopo l'entrata in vigore della presente direttiva, alcune delle quali possono avere una durata inferiore;
- e) l'eventuale rinnovabilità del mandato dei membri dell'autorità di controllo;
- f) le regole e le condizioni comuni che disciplinano le funzioni dei membri e del personale dell'autorità di controllo;

- g) le norme e le procedure relative alla cessazione delle funzioni dei membri dell'autorità di controllo, anche per il caso in cui non siano più in possesso dei requisiti necessari per l'esercizio delle loro funzioni o abbiano commesso una colpa grave.

*Articolo 43*  
***Segreto professionale***

Gli Stati membri dispongono che durante e dopo il mandato i membri e il personale dell'autorità di controllo siano tenuti al segreto professionale in merito alle informazioni riservate cui hanno avuto accesso nell'esercizio delle loro funzioni.

**SEZIONE 2**  
**FUNZIONI E POTERI**

*Articolo 44*  
***Competenza***

1. Gli Stati membri dispongono che ogni autorità di controllo eserciti, nel territorio del suo Stato membro, i poteri di cui gode a norma della presente direttiva.
2. Gli Stati membri dispongono che l'autorità di controllo non sia competente per il controllo dei trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali.

*Articolo 45*  
***Funzioni***

1. Gli Stati membri dispongono che l'autorità di controllo:
  - (a) sorvegli e garantisca l'applicazione delle disposizioni adottate ai sensi della presente direttiva e delle relative misure di esecuzione;
  - (b) tratti i reclami proposti dagli interessati o da associazioni che li rappresentano e che siano da questi debitamente autorizzate ai sensi dell'articolo 50, svolga le indagini opportune e informi l'interessato o l'associazione dello stato e dell'esito del reclamo entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;
  - (c) verifichi la liceità del trattamento dei dati ai sensi dell'articolo 14 e informi l'interessato entro un termine ragionevole dell'esito della verifica o dei motivi per cui non è stata effettuata;
  - (d) presti assistenza reciproca alle altre autorità di controllo e garantisca l'applicazione e l'attuazione coerente delle disposizioni adottate ai sensi della presente direttiva;

- (e) svolga indagini di propria iniziativa oppure a seguito di un reclamo o su richiesta di un'altra autorità di controllo, ed entro un termine ragionevole ne comunichi l'esito all'interessato che abbia proposto reclamo;
  - (f) sorvegli gli sviluppi che presentano un interesse, se ed in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione;
  - (g) sia consultata dalle istituzioni e dagli organismi degli Stati membri in merito alle misure legislative e amministrative relative alla tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali;
  - (h) sia consultata in merito ai trattamenti conformemente all'articolo 26;
  - (i) partecipi alle attività del comitato europeo per la protezione dei dati.
2. Ogni autorità di controllo promuove la sensibilizzazione del pubblico ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori.
  3. L'autorità di controllo, su richiesta, consiglia l'interessato in merito all'esercizio dei diritti derivanti dalle disposizioni adottate ai sensi della presente direttiva e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri.
  4. L'autorità di controllo fornisce un modulo compilabile elettronicamente per la proposizione dei reclami di cui al paragrafo 1, lettera b), senza escludere altri mezzi di comunicazione.
  5. Gli Stati membri dispongono che l'autorità di controllo svolga le proprie funzioni senza spese per l'interessato.
  6. Qualora le richieste siano vessatorie, in particolare per il loro carattere ripetitivo, l'autorità di controllo può esigere un contributo spese o non effettuare quanto richiesto dall'interessato. Incombe all'autorità di controllo dimostrare il carattere vessatorio della richiesta.

#### *Articolo 46* **Poteri**

Gli Stati membri dispongono che a ogni autorità di controllo siano riconosciuti in particolare:

- a) poteri investigativi, come la facoltà di accedere ai dati oggetto di trattamento e di raccogliere qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;
- b) poteri effettivi d'intervento, come quello di esprimere pareri prima dell'avvio di trattamenti e di dar loro adeguata pubblicità, o quello di ordinare la limitazione, la cancellazione o la distruzione dei dati o di vietare a titolo provvisorio o definitivo un trattamento, oppure quello di rivolgere un avvertimento o un monito al responsabile del trattamento o di adire i parlamenti o altre istituzioni politiche nazionali;

- c) il potere di agire in sede giudiziale o stragiudiziale in caso di violazione delle disposizioni adottate ai sensi della presente direttiva.

*Articolo 47*

***Relazione di attività***

Gli Stati membri dispongono che ogni autorità di controllo elabori una relazione annuale sulla propria attività. La relazione è messa a disposizione della Commissione e del comitato europeo per la protezione dei dati.

**CAPO VII  
COOPERAZIONE**

*Articolo 48*

***Assistenza reciproca***

1. Gli Stati membri dispongono che le autorità di controllo si prestino assistenza reciproca al fine di attuare e applicare le disposizioni adottate ai sensi della presente direttiva in maniera coerente, e prendano misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di consultazione preventiva, le ispezioni e le indagini.
2. Gli Stati membri dispongono che l'autorità di controllo prenda tutte le misure opportune necessarie per dare seguito alle richieste delle altre autorità di controllo.
3. L'autorità di controllo richiesta informa l'autorità di controllo richiedente dell'esito, se del caso, dei progressi o delle misure prese per rispondere alla sua richiesta.

*Articolo 49*

***Compiti del comitato europeo per la protezione dei dati***

1. Il comitato europeo per la protezione dei dati istituito con regolamento (UE).../2012 esercita i seguenti compiti in relazione ai trattamenti rientranti nel campo di applicazione della presente direttiva:
  - (a) consiglia la Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, comprese eventuali proposte di modifica della presente direttiva;
  - (b) esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione delle disposizioni adottate ai sensi della presente direttiva e pubblica linee direttrici, raccomandazioni e migliori pratiche destinate alle autorità di controllo al fine di promuovere l'applicazione coerente di tali disposizioni;
  - (c) valuta l'applicazione pratica delle linee direttrici, raccomandazioni e migliori pratiche di cui alla lettera b), riferendo regolarmente alla Commissione;

- (d) fornisce alla Commissione pareri sul livello di protezione garantito da paesi terzi o organizzazioni internazionali;
  - (e) promuove la cooperazione e l'effettivo scambio di informazioni e pratiche tra le autorità di controllo a livello bilaterale e multilaterale;
  - (f) promuove programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di organizzazioni internazionali;
  - (g) promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle pratiche in materia di protezione dei dati tra autorità di controllo di tutto il mondo.
2. Qualora chieda consulenza al comitato europeo per la protezione dei dati, la Commissione può fissare un termine entro il quale questo deve rispondere alla richiesta, tenuto conto dell'urgenza della questione.
  3. Il Comitato europeo per la protezione dei dati trasmette i propri pareri, linee direttrici, raccomandazioni e migliori pratiche alla Commissione e al comitato di cui all'articolo 57, paragrafo 1, e li rende pubblici.
  4. La Commissione informa il comitato europeo per la protezione dei dati del seguito dato ai suoi pareri, linee direttrici, raccomandazioni e migliori pratiche.

## **CAPO VIII**

### **RICORSI, RESPONSABILITÀ E SANZIONI**

#### *Articolo 50*

#### ***Diritto di proporre reclamo all'autorità di controllo***

1. Gli Stati membri dispongono che, fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento dei suoi dati personali non sia conforme alle disposizioni adottate ai sensi della presente direttiva abbia il diritto di proporre reclamo all'autorità di controllo di qualunque Stato membro.
2. Gli Stati membri dispongono che ogni organismo, organizzazione o associazione che tuteli i diritti e gli interessi degli interessati in relazione alla protezione dei loro dati personali e che sia debitamente costituito o costituita secondo la legislazione di uno Stato membro abbia il diritto di proporre reclamo all'autorità di controllo di qualunque Stato membro per conto di uno o più interessati qualora ritenga che siano stati violati diritti derivanti dalla presente direttiva a seguito del trattamento di dati personali. L'organizzazione o associazione deve essere debitamente autorizzata dall'interessato.
3. Gli Stati membri dispongono che, indipendentemente dall'eventuale reclamo dell'interessato, ogni organismo, organizzazione o associazione di cui al paragrafo 2 che ritenga che sussista violazione dei dati personali abbia il diritto di proporre reclamo all'autorità di controllo di qualunque Stato membro.

*Articolo 51*

***Diritto a un ricorso giurisdizionale contro l'autorità di controllo***

1. Gli Stati membri prevedono il diritto di proporre ricorso giurisdizionale avverso le decisioni dell'autorità di controllo.
2. Ogni interessato ha il diritto di proporre ricorso giurisdizionale per obbligare l'autorità di controllo a dare seguito a un reclamo qualora tale autorità non abbia preso una decisione necessaria per tutelarne i diritti o non lo abbia informato entro tre mesi dello stato o dell'esito del reclamo ai sensi dell'articolo 45, paragrafo 1, lettera b).
3. Gli Stati membri dispongono che le azioni contro l'autorità di controllo siano promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

*Articolo 52*

***Diritto a un ricorso giurisdizionale contro il responsabile del trattamento o l'incaricato del trattamento***

Gli Stati membri dispongono che, fatto salvo ogni altro ricorso amministrativo disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo, chiunque abbia il diritto di proporre ricorso giurisdizionale qualora ritenga che siano stati violati i diritti di cui gode a norma delle disposizioni adottate ai sensi della presente direttiva in seguito a un trattamento dei suoi dati personali non conforme a tali disposizioni.

*Articolo 53*

***Norme comuni per i procedimenti giurisdizionali***

1. Gli Stati membri dispongono che ogni organismo, organizzazione o associazione di cui all'articolo 50, paragrafo 2, abbia il diritto di esercitare i diritti di cui agli articoli 51 e 52 per conto di uno o più interessati.
2. Ogni autorità di controllo ha il diritto di agire in sede giudiziale o stragiudiziale per far rispettare le disposizioni adottate ai sensi della presente direttiva o garantire la coerenza della protezione dei dati personali all'interno dell'Unione.
3. Gli Stati membri provvedono affinché i ricorsi giurisdizionali previsti dal diritto nazionale consentano di prendere rapidamente provvedimenti, anche provvisori, atti a porre fine alle asserite violazioni e impedire ulteriori danni agli interessi in causa.

*Articolo 54*

***Diritto al risarcimento e responsabilità***

1. Gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da altro atto incompatibile con le disposizioni adottate ai sensi della presente direttiva abbia il diritto di ottenere il risarcimento del danno dal responsabile del trattamento o dall'incaricato del trattamento.

2. Qualora il trattamento coinvolga più responsabili del trattamento o incaricati del trattamento, ogni responsabile del trattamento o incaricato del trattamento risponde in solido per l'intero ammontare del danno.
3. Il responsabile del trattamento o l'incaricato del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile.

*Articolo 55*  
**Sanzioni**

Gli Stati membri determinano le sanzioni per violazione delle disposizioni adottate ai sensi della presente direttiva e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste devono essere efficaci, proporzionate e dissuasive.

**CAPO IX**  
**ATTI DELEGATI E ATTI DI ESECUZIONE**

*Articolo 56*  
**Esercizio della delega**

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.
2. La delega di potere di cui all'articolo 28, paragrafo 5, è conferita alla Commissione per un periodo indeterminato a decorrere dalla data di entrata in vigore della presente direttiva.
3. La delega di potere di cui all'articolo 28, paragrafo 5, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.
4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.
5. L'atto delegato adottato ai sensi dell'articolo 28, paragrafo 5, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

*Articolo 57*  
**Procedura di comitato**

1. La Commissione è assistita da un comitato. Tale comitato è un comitato ai sensi del regolamento (UE) n. 182/2011.
2. Nel caso in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.
3. Nel caso in cui è fatto riferimento al presente paragrafo, si applica l'articolo 8 del regolamento (UE) n. 182/2011, in combinato disposto con l'articolo 5 del medesimo regolamento.

**CAPO X**  
**DISPOSIZIONI FINALI**

*Articolo 58*  
**Abrogazione**

1. La decisione quadro 2008/977/GAI del Consiglio è abrogata.
2. I riferimenti alla decisione quadro di cui al paragrafo 1 si intendono fatti alla presente direttiva.

*Articolo 59*  
**Rapporto con altri atti dell'Unione già adottati nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia**

Rimangono impregiudicate le disposizioni specifiche per la protezione dei dati personali 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, contenute in atti dell'Unione adottati prima della data di adozione della presente direttiva e che disciplinano il trattamento dei dati personali tra Stati membri e l'accesso delle autorità nazionali designate ai sistemi d'informazione istituiti ai sensi dei trattati, nell'ambito della presente direttiva.

*Articolo 60*  
**Rapporto con gli accordi internazionali già conclusi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia**

Gli accordi internazionali conclusi dagli Stati membri prima dell'entrata in vigore della presente direttiva sono modificati, ove necessario, entro cinque anni dall'entrata in vigore della presente direttiva.

*Articolo 61*  
**Valutazione**

1. La Commissione valuta l'applicazione della presente direttiva.

2. Entro tre anni dall'entrata in vigore della presente direttiva, la Commissione riesamina gli altri atti adottati dall'Unione europea che disciplinano il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione delle sanzioni penali, in particolare quelli richiamati all'articolo 59, al fine di valutare la necessità di allinearli alla presente direttiva e formulare, ove opportuno, le proposte necessarie per modificarli in modo da garantire un approccio coerente alla protezione dei dati personali nell'ambito della presente direttiva.
3. La Commissione trasmette al Parlamento europeo e al Consiglio, a scadenze regolari, relazioni di valutazione e sul riesame della presente direttiva ai sensi del paragrafo 1. La prima relazione è presentata entro quattro anni dall'entrata in vigore della presente direttiva, le successive sono trasmesse ogni quattro anni. Se del caso, la Commissione presenta opportune proposte di modifica della presente direttiva e per l'allineamento di altri strumenti giuridici. Le relazioni sono pubblicate.

#### *Articolo 62*

##### *Attuazione*

1. Gli Stati membri adottano e pubblicano, entro il [data/due anni dopo l'entrata in vigore], le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni.

Gli Stati membri applicano tali disposizioni a decorrere dal xx.xx.201x [data/due anni dopo l'entrata in vigore].

Quando gli Stati membri adottano tali disposizioni, queste contengono un riferimento alla presente direttiva o sono corredate di un siffatto riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono decise dagli Stati membri.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni essenziali di diritto interno adottate nella materia disciplinata dalla presente direttiva.

#### *Articolo 63*

##### *Entrata in vigore e applicazione*

La presente direttiva entra in vigore il giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

*Articolo 64*  
***Destinatari***

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, il 25.1.2012

*Per il Parlamento europeo*  
*Il presidente*

*Per il Consiglio*  
*Il presidente*