DIRETTIVE

DIRETTIVA (UE) 2016/680 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16, paragrafo 2,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato delle regioni ([1]),

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

considerando quanto segue:

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

(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei loro dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. La presente direttiva è intesa a 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 raccolta e della condivisione di dati personali è aumentata in modo significativo. La tecnologia, come mai in precedenza, consente il trattamento di dati personali, come mai in precedenza, nello svolgimento di attività quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali.

(4) La libera circolazione dei dati personali tra le autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali, inclusi la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, all'interno dell'Unione e il trasferimento di tali dati personali verso paesi terzi e organizzazioni internazionali, dovrebbe essere agevolata garantendo al tempo stesso un elevato livello di protezione dei dati personali. Ciò richiede la costruzione di un quadro giuridico solido e più coerente in materia di protezione dei dati personali nell'Unione, affiancato da efficaci misure di attuazione.

(5) La direttiva 95/46/CE del Parlamento europeo e del Consiglio ([3]) si applica a qualsiasi trattamento di dati personali negli Stati membri sia nel settore pubblico che in quello privato. Non si applica invece ai trattamenti di dati personali effettuati per l'esercizio di attività che non rientrano nell'ambito di applicazione del diritto comunitario quali le attività nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia.

([1]) GU C 391 del 18.12.2012, pag. 127.
([2]) Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura dell'8 aprile 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 14 aprile 2016.
([3]) 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).

(6) La decisione quadro 2008/977/GAI del Consiglio ([1]) si applica ai settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia. L'ambito di applicazione di tale 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 giudiziaria in materia penale e di polizia. Per questo sarebbe auspicabile 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 di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento dei diritti degli interessati e degli obblighi di tutti coloro che trattano dati personali, nonché poteri equivalenti per controllare e garantire il rispetto delle norme di protezione dei dati personali negli Stati membri.

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

(9) Su tale base, il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([2]) stabilisce norme generali per la protezione delle persone fisiche in relazione al trattamento dei dati personali e per la libera circolazione dei dati personali nell'Unione.

(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 specificità dei settori in questione, norme specifiche sulla protezione dei dati personali e sulla libera circolazione di dati personali nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'articolo 16 TFUE.

(11) È pertanto opportuno per i settori in questione che una direttiva stabilisca le norme specifiche relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della natura specifica di tali attività. Tali autorità competenti possono includere non solo autorità pubbliche quali le autorità giudiziarie, la polizia o altre autorità incaricate dell'applicazione della legge, ma anche qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici ai fini della presente direttiva. Qualora tale organismo o entità trattino dati personali per finalità diverse da quelle della presente direttiva, si applica il regolamento (UE) 2016/679. Il regolamento (UE) 2016/679 si applica pertanto nei casi in cui un organismo o un'entità raccolgano dati personali per finalità diverse e procedano a un loro ulteriore trattamento per adempiere un obbligo legale cui sono soggetti. Ad esempio, a fini di indagine, accertamento o perseguimento di reati, gli istituti finanziari conservano determinati dati personali da essi trattati, e li trasmettono solo alle autorità nazionali competenti in casi specifici e conformemente al diritto dello Stato membro. Un organismo o un'entità che trattano dati personali per conto di tali autorità entro l'ambito di applicazione della presente direttiva dovrebbero essere vincolati da un contratto o altro atto giuridico e dalle disposizioni applicabili ai responsabili del trattamento a norma della presente direttiva; l'applicazione del regolamento (UE) 2016/679 rimane invece impregiudicata per le attività di trattamento svolte dal responsabile del trattamento di dati personali al di fuori dell'ambito di applicazione della presente direttiva.

(12) Le attività svolte dalla polizia o da altre autorità preposte all'applicazione della legge vertono principalmente sulla prevenzione, l'indagine, l'accertamento o il perseguimento di reati, comprese le attività di polizia condotte senza previa conoscenza della rilevanza penale di un fatto. Tali attività possono comprendere anche l'esercizio di poteri mediante l'adozione di misure coercitive quali le attività di polizia in occasione di manifestazioni, grandi eventi sportivi e sommosse. Esse comprendono anche il mantenimento dell'ordine pubblico quale compito conferito alla polizia o ad altre autorità incaricate dell'applicazione della legge ove necessario per la salvaguardia contro e la

([1]) 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).

([2]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (cfr. pagina 1 della presente Gazzetta ufficiale).

prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati. Gli Stati membri possono conferire alle autorità competenti altri compiti che non siano necessariamente svolti a fini di prevenzione, indagine, accertamento o perseguimento di reati, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, cosicché il trattamento di dati personali per tali altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientra nell'ambito di applicazione del regolamento (UE) 2016/679.

(13) Un reato ai sensi della presente direttiva dovrebbe costituire un concetto autonomo del diritto dell'Unione come interpretato dalla Corte di giustizia dell'Unione europea («Corte di giustizia»).

(14) Poiché la presente direttiva non dovrebbe applicarsi al trattamento di dati personali nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione, le attività concernenti la sicurezza nazionale, le attività delle agenzie o unità che si occupano di questioni connesse alla sicurezza nazionale e il trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività rientranti nell'ambito di applicazione del titolo V, capo 2, del trattato sull'Unione europea (TUE) non dovrebbero essere considerate attività rientranti nell'ambito di applicazione della presente direttiva.

(15) 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 personali tra le autorità competenti, è opportuno che la presente direttiva stabilisca norme armonizzate per la protezione e la libera circolazione dei dati personali trattati a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Il ravvicinamento delle legislazioni degli Stati membri non dovrebbe portare a una riduzione della protezione dei dati personali da esse assicurata, ma dovrebbe, al contrario, cercare di garantire un elevato livello di protezione all'interno dell'Unione. Agli Stati membri non dovrebbe essere preclusa la possibilità di prevedere garanzie più elevate di quelle stabilite nella presente direttiva per la tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali da parte delle autorità competenti.

(16) La presente direttiva non pregiudica il principio del pubblico accesso ai documenti ufficiali. A norma del regolamento (UE) 2016/679, i dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere divulgati da tale autorità o organismo conformemente al diritto dell'Unione o dello Stato membro cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali.

(17) È opportuno 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 loro dati personali.

(18) Al fine di evitare che si corrano gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione della presente direttiva i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine.

(19) Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio ([1]) si applica al trattamento di dati personali effettuato da istituzioni, organi, uffici e agenzie dell'Unione. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali dovrebbero essere adeguati ai principi e alle norme stabiliti nel regolamento (UE) 2016/679.

(20) La presente direttiva non pregiudica la facoltà degli Stati membri di specificare le operazioni e le procedure di trattamento nelle norme nazionali di procedura penale relativamente al trattamento dei dati personali effettuato da autorità giurisdizionali e da altre autorità giudiziarie, in particolare per quanto riguarda dati personali contenuti in una decisione giudiziaria o in documentazione relativa a procedimenti penali.

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

(21) È auspicabile applicare i principi di protezione dei dati 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, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da non consentire più l'identificazione dell'interessato.

(22) Le autorità pubbliche a cui i dati personali sono comunicati conformemente a un obbligo legale ai fini dell'esercizio della loro missione istituzionale, quali autorità fiscali e doganali, unità di indagine finanziaria, autorità amministrative indipendenti o autorità dei mercati finanziari, responsabili della regolamentazione e della vigilanza dei mercati dei valori mobiliari, non dovrebbero essere considerate destinatari qualora ricevano dati personali che sono necessari per svolgere una specifica indagine nell'interesse generale, conformemente al diritto dell'Unione o dello Stato membro. Le richieste di comunicazione inviate dalle autorità pubbliche dovrebbero sempre essere scritte, motivate e occasionali e non dovrebbero riguardare un intero archivio o condurre all'interconnessione di archivi. Il trattamento di tali dati personali da parte delle autorità pubbliche dovrebbe essere conforme alle norme in materia di protezione dei dati applicabili secondo le finalità del trattamento.

(23) È opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica che forniscono informazioni uniche sulla fisiologia o sulla salute della persona fisica considerata, ottenuti dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti. Tenuto conto della complessità e del carattere sensibile delle informazioni di natura genetica, il rischio di utilizzo improprio e di riutilizzo per varie finalità non autorizzate da parte del titolare del trattamento è elevato. In linea di principio dovrebbe essere vietata qualunque discriminazione basata su caratteristiche genetiche.

(24) Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono le informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio ([1]); un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

(25) Tutti gli Stati membri sono affiliati all'Organizzazione internazionale della polizia criminale (Interpol). Per svolgere la propria missione, Interpol riceve, conserva e diffonde dati personali nell'intento di aiutare le autorità competenti a prevenire e combattere la criminalità internazionale. È pertanto opportuno rafforzare la cooperazione tra l'Unione e Interpol promuovendo un efficace scambio di dati personali assicurando nel contempo il rispetto dei diritti e delle libertà fondamentali attinenti al trattamento automatizzato dei dati personali. Qualora i dati personali siano trasferiti dall'Unione a Interpol e a paesi che hanno distaccato membri presso Interpol, dovrebbe trovare applicazione la presente direttiva, in particolare le disposizioni relative ai trasferimenti internazionali. La presente direttiva dovrebbe lasciare impregiudicate le norme specifiche definite nella posizione comune 2005/69/GAI del Consiglio ([2]) e nella decisione 2007/533/GAI del Consiglio ([3]).

(26) Qualsiasi trattamento di dati personali dovrebbe essere lecito, corretto e trasparente nei confronti della persona fisica interessata e perseguire unicamente fini specifici previsti dalla legge. Ciò non impedisce di per sé alle autorità incaricate dell'applicazione della legge di svolgere attività quali operazioni di infiltrazione o videosorveglianza. Tali attività possono essere svolte a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica,

([1]) Direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera (GU L 88 del 4.4.2011, pag. 45).

([2]) Posizione comune 2005/69/GAI del Consiglio, del 24 gennaio 2005, sullo scambio con l'Interpol di alcuni dati (GU L 27 del 29.1.2005, pag. 61).

([3]) Decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) (GU L 205 del 7.8.2007, pag. 63).

purché siano previste dalla legge e costituiscano una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei legittimi interessi della persona fisica interessata. Il principio di trattamento corretto proprio della protezione dei dati è una nozione distinta dal diritto a un giudice imparziale sancito nell'articolo 47 della Carta e nell'articolo 6 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU). È opportuno che le persone fisiche siano sensibilizzate rispetto ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento dei loro dati personali, nonché alle modalità di esercizio dei loro diritti in relazione al trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta. I dati personali dovrebbero essere adeguati e pertinenti alle finalità del trattamento. Dovrebbe, in particolare, essere garantito che la raccolta dei dati personali non sia eccessiva e che i dati siano conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde garantire che i dati non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. Gli Stati membri dovrebbero stabilire garanzie adeguate per i dati personali conservati per periodi più lunghi per finalità di archiviazione nel pubblico interesse o per finalità scientifiche, storiche o statistiche.

(27) Nell'interesse della prevenzione, dell'indagine e del perseguimento di reati, è necessario che le autorità competenti 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 delle attività criminali e mettere in collegamento i diversi reati accertati.

(28) Per mantenere la sicurezza relativamente al trattamento e prevenire trattamenti che violano la presente direttiva, i dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche impedendo l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento, e da tenere conto dello stato dell'arte e della tecnologia disponibili, dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere.

(29) I dati personali dovrebbero essere raccolti per finalità determinate, esplicite e legittime rientranti nell'ambito di applicazione della presente direttiva e non dovrebbero essere trattati per finalità incompatibili con le finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Se i dati personali sono trattati dallo stesso o da un altro titolare del trattamento per una finalità rientrante nell'ambito di applicazione della presente direttiva diversa da quella per la quale sono stati raccolti, tale trattamento dovrebbe essere consentito purché sia autorizzato conformemente alle disposizioni giuridiche applicabili e sia necessario e proporzionato a tale altra finalità.

(30) Il principio dell'esattezza dei dati dovrebbe 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 dovrebbe pertanto riferirsi all'esattezza di una dichiarazione ma al semplice fatto che è stata rilasciata.

(31) È inerente al trattamento dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia che siano trattati dati personali relativi a diverse categorie di interessati. Pertanto dovrebbe essere operata, se del caso e per quanto possibile, una chiara distinzione tra i dati personali relativi a diverse categorie di interessati, quali: indiziati, condannati, persone offese e altri soggetti, quali testimoni, persone informate dei fatti, persone in contatto o collegate a indiziati o condannati. Ciò non dovrebbe impedire l'applicazione del diritto alla presunzione di innocenza garantito dalla Carta e dalla CEDU, come interpretato nella giurisprudenza rispettivamente della Corte di giustizia e della Corte europea dei diritti dell'uomo.

(32) Le autorità competenti dovrebbero provvedere affinché i dati personali inesatti, incompleti o non più aggiornati non siano trasmessi o resi disponibili. Al fine di garantire la protezione delle persone fisiche, l'esattezza, la completezza dei dati personali o la misura in cui essi sono aggiornati e l'affidabilità dei dati personali trasmessi o resi disponibili, le autorità competenti dovrebbero, nella misura del possibile, aggiungere le informazioni necessarie in tutte le trasmissioni di dati personali.

(33) Qualora la presente direttiva faccia riferimento al diritto dello Stato membro, a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un parlamento, fatte salve

le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato. Tuttavia, tale diritto dello Stato membro, base giuridica o misura legislativa dovrebbero essere chiari e precisi, e la loro applicazione prevedibile, per coloro che vi sono sottoposti, come richiesto dalla giurisprudenza della Corte di giustizia e della Corte europea dei diritti dell'uomo. Il diritto dello Stato membro che disciplina il trattamento dei dati personali nell'ambito di applicazione della presente direttiva dovrebbe specificare quanto meno gli obiettivi, i dati personali da trattare, le finalità del trattamento e le procedure per preservare l'integrità e la riservatezza dei dati personali come pure le procedure per la loro distruzione, fornendo in tal modo sufficienti garanzie contro il rischio di abuso e arbitrarietà.

(34) Il trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, dovrebbe riguardare qualsiasi operazione o insieme di operazioni compiute nei confronti di dati personali o insiemi di dati personali per tali finalità, con l'ausilio di strumenti automatizzati o in altro modo, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, il raffronto o l'interconnessione, la limitazione del trattamento, la cancellazione o la distruzione. In particolare, le norme della presente direttiva dovrebbero applicarsi alla trasmissione di dati personali ai fini della presente direttiva a un destinatario a essa non soggetto. Per tale destinatario si dovrebbe intendere la persona fisica o giuridica, l'autorità pubblica, l'agenzia o qualsiasi altro organismo a cui i dati personali sono comunicati in modo lecito dall'autorità competente. Se i dati personali sono stati inizialmente raccolti da un'autorità competente per una delle finalità della presente direttiva, il regolamento (UE) 2016/679 dovrebbe applicarsi al trattamento di tali dati per finalità diverse da quelle della presente direttiva, qualora detto trattamento sia autorizzato dal diritto dell'Unione o dello Stato membro. In particolare, le norme del regolamento (UE) 2016/679 dovrebbero applicarsi alla trasmissione di dati personali per finalità che non rientrano nell'ambito di applicazione della presente direttiva. Al trattamento di dati personali da parte di un destinatario che non è un'autorità competente o che non esercita tale funzione ai sensi della presente direttiva e a cui i dati personali sono comunicati in modo lecito da un'autorità competente, dovrebbe applicarsi il regolamento (UE) 2016/679. Nell'attuare la presente direttiva, gli Stati membri dovrebbero poter precisare ulteriormente l'applicazione delle norme del regolamento (UE) 2016/679, fatte salve le condizioni in esso stabilite.

(35) Per essere lecito, il trattamento dei dati personali a norma della presente direttiva dovrebbe essere necessario per l'esecuzione di un compito svolto nell'interesse pubblico da un'autorità competente in base al diritto dell'Unione o dello Stato membro a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica. Tali attività dovrebbero comprendere la salvaguardia degli interessi vitali dell'interessato. L'adempimento dei compiti di prevenzione, indagine, accertamento e perseguimento di reati, affidato istituzionalmente per legge alle autorità competenti, consente a queste ultime di richiedere od ordinare alle persone fisiche di dare seguito alle richieste formulate. In tal caso il consenso dell'interessato, quale definito nel regolamento (UE) 2016/679, non dovrebbe costituire la base giuridica per il trattamento di dati personali da parte delle autorità competenti. Qualora sia tenuto ad adempiere un obbligo legale, l'interessato non è in grado di operare una scelta autenticamente libera, pertanto la sua reazione non potrebbe essere considerata una manifestazione di volontà libera. Ciò non dovrebbe impedire agli Stati membri di prevedere per legge che l'interessato possa acconsentire al trattamento dei propri dati personali ai fini della presente direttiva, ad esempio per test del DNA nell'ambito di indagini penali o per il monitoraggio della sua ubicazione mediante dispositivo elettronico per l'esecuzione di sanzioni penali.

(36) Gli Stati membri dovrebbero disporre che, nei casi in cui il diritto dell'Unione o dello Stato membro applicabile all'autorità competente che trasmette i dati preveda condizioni specifiche applicabili in circostanze specifiche al trattamento di dati personali, quali l'uso di codici di gestione, l'autorità competente che trasmette i dati informi il destinatario di tali dati personali di tali condizioni e dell'obbligo di rispettarle. Tali condizioni potrebbero ad esempio comprendere un divieto di trasmettere ulteriormente i dati personali ad altri, o di usarli per finalità diverse da quelle per le quali sono stati trasmessi al destinatario, o di informare l'interessato nei casi in cui vi sia una limitazione del diritto di informazione senza previa approvazione dell'autorità competente che trasmette i dati. Tali obblighi dovrebbero applicarsi anche ai trasferimenti da parte dell'autorità competente che trasmette i dati a destinatari di paesi terzi o organizzazioni internazionali. Gli Stati membri dovrebbero provvedere affinché l'autorità competente che trasmette i dati non applichi a destinatari di altri Stati membri o agenzie, uffici e organi istituiti a norma del titolo V, capi 4 e 5, TFUE condizioni diverse da quelle applicabili a trasmissioni di dati analoghe all'interno dello Stato membro di detta autorità competente.

(37) Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare

rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini «origine razziale» nella presente direttiva non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane distinte. Detti dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia soggetto a garanzie adeguate per i diritti e le libertà dell'interessato stabilite per legge e non sia autorizzato in casi consentiti dalla legge; se non già autorizzato per legge, salvo che non sia necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona; o riguardi dati resi manifestamente pubblici dall'interessato. Garanzie adeguate per i diritti e le libertà dell'interessato potrebbero comprendere la possibilità di raccogliere tali dati unicamente in connessione con altri dati relativi alla persona fisica interessata, la possibilità di provvedere adeguatamente alla sicurezza dei dati raccolti, norme più severe riguardo all'accesso ai dati da parte del personale dell'autorità competente e il divieto di trasmissione di tali dati. Il trattamento di tali dati dovrebbe inoltre essere autorizzato per legge qualora l'interessato abbia esplicitamente dato il proprio consenso al trattamento che sia particolarmente invasivo per questi. Il consenso dell'interessato non dovrebbe tuttavia costituire di per sé la base giuridica per il trattamento di tali dati personali sensibili da parte delle autorità competenti.

(38) L'interessato dovrebbe avere il diritto di non essere oggetto di una decisione che valuta aspetti personali che lo concernono basata esclusivamente su un trattamento automatizzato e che produca effetti giuridici negativi nei suoi confronti o incida significativamente sulla sua persona. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, compresi il rilascio di specifiche informazioni all'interessato e il diritto di ottenere l'intervento umano, in particolare di esprimere la propria opinione, di ottenere una spiegazione della decisione raggiunta dopo tale valutazione e di impugnare la decisione. La profilazione che porti alla discriminazione di persone fisiche sulla base di dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali dovrebbe essere vietata alle condizioni stabilite negli articoli 21 e 52 della Carta.

(39) Affinché l'interessato possa esercitare i propri diritti, qualsiasi informazione a questi destinata dovrebbe essere di facile accesso, anche sul sito web del titolare del trattamento, e di facile comprensione, utilizzando un linguaggio semplice e chiaro. Tali informazioni dovrebbero essere adattate alle esigenze delle persone vulnerabili, come i minori.

(40) È opportuno predisporre modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei propri diritti conformemente alle disposizioni adottate a norma della presente direttiva, compresi i meccanismi per richiedere e, se possibile, ottenere, gratuitamente, in particolare, l'accesso ai propri dati personali, la loro rettifica o cancellazione e la limitazione del trattamento. Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo, a meno che applichi limitazioni ai diritti dell'interessato conformemente alla presente direttiva. Inoltre, nel caso in cui le richieste siano manifestamente infondate o eccessive, come nel caso in cui l'interessato richieda informazioni in modo irragionevole e ripetitivo oppure qualora l'interessato abusi del suo diritto di ricevere informazioni, ad esempio fornendo informazioni false o ingannevoli al momento della presentazione della richiesta, il titolare del trattamento dovrebbe poter addebitare un contributo spese ragionevole o rifiutare di soddisfare la richiesta.

(41) Qualora il titolare del trattamento richieda ulteriori informazioni necessarie per confermare l'identità dell'interessato, tali informazioni dovrebbero essere trattate solo per tale specifica finalità e non dovrebbero essere conservate più a lungo di quanto necessario per tale finalità.

(42) Dovrebbero essere messe a disposizione dell'interessato almeno le seguenti informazioni: l'identità del titolare del trattamento, l'esistenza del trattamento, le finalità del trattamento, il diritto di proporre reclamo e l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati e la rettifica o la cancellazione degli stessi ovvero la limitazione del trattamento. Ciò potrebbe avvenire sul sito web dell'autorità competente. Inoltre, in casi specifici e per consentire l'esercizio dei suoi diritti, l'interessato dovrebbe essere informato della base giuridica del trattamento e del periodo di conservazione dei dati, nella misura in cui tali ulteriori informazioni siano necessarie, tenuto conto delle specifiche circostanze in cui i dati vengono trattati, per garantire un trattamento corretto nei confronti dell'interessato.

(43) Una persona fisica dovrebbe avere il diritto di accedere ai dati raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. È pertanto opportuno che ogni interessato abbia il diritto di conoscere e ottenere comunicazioni in relazione alla finalità del trattamento, al periodo per il quale i dati sono trattati e ai destinatari dei dati, anche quelli nei paesi terzi. Qualora tali comunicazioni comprendano informazioni sull'origine dei dati personali, le informazioni non dovrebbero rivelare l'identità delle persone fisiche, in particolare fonti riservate. Affinché tale diritto sia rispettato, è sufficiente che l'interessato sia in possesso di una sintesi completa di tali dati in forma intelligibile, cioè in una

forma che gli consenta di venire a conoscenza di tali dati e di verificare che siano esatti e trattati conformemente alla presente direttiva, in modo tale che possa esercitare i diritti conferitigli dalla presente direttiva. Detta sintesi potrebbe essere fornita in forma di copia dei dati personali oggetto del trattamento.

(44) Gli Stati membri dovrebbero poter adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato o a limitare, in tutto o in parte, l'accesso di questi ai suoi dati personali nella misura e per la durata in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata, per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, per proteggere la sicurezza pubblica o la sicurezza nazionale o per tutelare i diritti e le libertà altrui. È opportuno che il titolare del trattamento valuti, mediante un esame concreto e individuale di ciascun caso, se si debba applicare una limitazione parziale o totale del diritto di accesso.

(45) In linea di massima, qualsiasi rifiuto o limitazione di accesso dovrebbero essere comunicati per iscritto all'interessato e indicare i motivi di fatto o di diritto sui quali si basa la decisione.

(46) Qualsiasi limitazione dei diritti dell'interessato deve essere conforme alla Carta e alla CEDU, come interpretate nella giurisprudenza rispettivamente della Corte di giustizia e della Corte europea dei diritti dell'uomo, e rispettare in particolare la sostanza di tali diritti e libertà.

(47) Una persona fisica dovrebbe avere il diritto di ottenere la rettifica di dati personali inesatti che la riguardano, in particolare se relativi a fatti, e il diritto alla cancellazione quando il trattamento di tali dati viola la presente direttiva. Il diritto di rettifica, tuttavia, non dovrebbe avere effetti, ad esempio, sul contenuto di una prova testimoniale. Una persona fisica dovrebbe inoltre avere il diritto di ottenere la limitazione del trattamento qualora contesti l'esattezza dei dati personali e l'esattezza o l'inesattezza di tali dati non possa essere accertata o qualora i dati personali debbano essere conservati a fini probatori. In particolare, invece della cancellazione dei dati personali, ne dovrebbe essere limitato il trattamento se in un caso specifico vi sono motivi ragionevoli di ritenere che la cancellazione possa compromettere gli interessi legittimi dell'interessato. In tal caso, i dati limitati dovrebbero essere trattati solo per la finalità che ne ha impedito la cancellazione. Le modalità per limitare il trattamento dei dati personali potrebbero consistere, tra l'altro, nel trasferire i dati selezionati verso un altro sistema di trattamento, ad esempio a fini di archiviazione, o nel rendere i dati selezionati inaccessibili. Negli archivi automatizzati la limitazione del trattamento dovrebbe essere assicurata, in linea di massima, mediante dispositivi tecnici. Il sistema dovrebbe indicare che il trattamento dei dati personali è stato limitato in modo da renderne evidente la limitazione. Tali rettifiche o cancellazioni di dati personali o limitazioni del trattamento dovrebbero essere comunicate ai destinatari a cui tali dati sono stati comunicati e alle autorità competenti da cui i dati inesatti provengono. I titolari del trattamento dovrebbero inoltre astenersi dal diffondere ulteriormente tali dati.

(48) Nel caso in cui il titolare del trattamento neghi all'interessato il suo diritto di informazione, accesso, rettifica o cancellazione di dati personali o limitazione di trattamento, l'interessato dovrebbe avere il diritto di chiedere che l'autorità nazionale di controllo verifichi la liceità del trattamento. È opportuno che l'interessato sia informato di tale diritto. Qualora l'autorità di controllo intervenga per conto dell'interessato, essa dovrebbe quanto meno informarlo di aver eseguito tutti i riesami o le verifiche necessari. È inoltre opportuno che l'autorità di controllo informi l'interessato del diritto di proporre ricorso giurisdizionale.

(49) Se i dati personali sono trattati nel corso di un'indagine penale e di un procedimento giudiziario penale, gli Stati membri dovrebbero poter prevedere che i diritti di informazione, accesso, rettifica o cancellazione di dati personali e limitazione di trattamento siano esercitati conformemente alle norme nazionali sui procedimenti giudiziari.

(50) È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci e dovrebbe essere in grado di dimostrare che le attività di trattamento sono conformi alla presente direttiva. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Le misure adottate dal titolare del trattamento dovrebbero comprendere la definizione e la messa in atto di garanzie specifiche con riguardo al trattamento dei dati personali delle persone fisiche vulnerabili, come i minori.

(51) I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di

essere privati dei loro diritti e delle loro libertà o dell'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale; se sono trattati i dati genetici o biometrici per identificare in modo univoco una persona o se sono trattati i dati relativi alla salute o i dati relativi alla vita sessuale e all'orientamento sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi e la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; o se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

(52) La probabilità e la gravità del rischio dovrebbero essere determinate con riferimento alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se il trattamento di dati comporta un rischio elevato. Un rischio elevato è un particolare rischio di pregiudizio dei diritti e delle libertà degli interessati.

(53) La tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni della presente direttiva. L'attuazione di tali misure non dovrebbe dipendere unicamente da considerazioni economiche. Al fine di poter dimostrare la conformità con la presente direttiva, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che aderiscano in particolare ai principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita. Se il titolare del trattamento ha effettuato una valutazione d'impatto sulla protezione dei dati ai sensi della presente direttiva, è opportuno prenderne in considerazione i risultati in fase di sviluppo delle misure e delle procedure suddette. Le misure potrebbero consistere, tra l'altro, nell'utilizzo della pseudonimizzazione il più presto possibile. L'utilizzo della pseudonimizzazione ai fini della presente direttiva può essere strumentale per agevolare, in particolare, la libera circolazione dei dati personali all'interno dello spazio di libertà, sicurezza e giustizia.

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

(55) L'esecuzione dei trattamenti da parte di un responsabile dl trattamento dovrebbe essere disciplinata da un atto giuridico, comprensivo di un contratto che vincoli il responsabile del trattamento al titolare del trattamento e che in particolare preveda che il responsabile del trattamento debba agire soltanto su istruzione del titolare del trattamento. Il responsabile del trattamento dovrebbe tenere conto dei principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita.

(56) Per dimostrare che si conforma alla presente direttiva, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro di tutte le categorie di attività di trattamento effettuate sotto la sua responsabilità. Bisognerebbe obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere detti registri a sua disposizione, previa richiesta, affinché possano servire per monitorare detti trattamenti. Il titolare del trattamento o il responsabile del trattamento che tratta dati personali in sistemi di trattamento non automatizzati dovrebbe aver posto in essere metodi efficaci per dimostrare la liceità del trattamento, rendere possibile l'autocontrollo e assicurare l'integrità e la sicurezza dei dati, quali registrazioni o altre forme di documentazione.

(57) È opportuno registrare almeno le operazioni nei sistemi di trattamento automatizzato, quali raccolta, modifica, consultazione, comunicazione, inclusi trasferimenti, interconnessione e cancellazione. L'identificazione della persona fisica che ha consultato o comunicato i dati personali dovrebbe essere registrata e da tale identificazione dovrebbe essere possibile stabilire il motivo delle operazioni di trattamento. Le registrazioni dovrebbero essere usate ai soli fini della verifica della liceità del trattamento dei dati, dell'autocontrollo, per garantire l'integrità e la sicurezza dei dati e nell'ambito di procedimenti penali. L'autocontrollo dovrebbe altresì comprendere anche procedimenti disciplinari interni delle autorità competenti.

(58) Nei casi in cui le operazioni di trattamento possano comportare un rischio elevato per i diritti e le libertà degli interessati in considerazione della loro natura, ambito di applicazione e finalità, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati, che verta in particolare sulle misure, sulle garanzie e sui meccanismi previsti per assicurare la protezione dei dati personali e per comprovare la conformità con la presente direttiva. Le valutazioni d'impatto dovrebbero riguardare i sistemi e processi delle operazioni di trattamento pertinenti, non singoli casi.

(59) Al fine di garantire un'efficace tutela dei diritti e delle libertà dell'interessato, il titolare del trattamento o il responsabile del trattamento dovrebbe consultare l'autorità di controllo, in determinati casi, prima del trattamento.

(60) Per mantenere la sicurezza e prevenire trattamenti che violino la presente direttiva, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e dovrebbe attuare misure per limitare tali rischi, quali la cifratura. Tali misure dovrebbero assicurare un adeguato livello di sicurezza, inclusa la riservatezza, e tener conto dello stato dell'arte, dei costi di attuazione rispetto al rischio che presentano i trattamenti e della natura dei dati personali da proteggere. Nella valutazione dei rischi per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati, come la distruzione, la perdita, la modifica accidentali o illecite o la divulgazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque trattati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. Il titolare del trattamento e il responsabile del trattamento dovrebbero provvedere affinché il trattamento dei dati personali non sia eseguito da persone non autorizzate.

(61) Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

(62) Le persone fisiche dovrebbero essere informate senza ingiustificato ritardo in caso di violazione dei dati personali suscettibile di presentare un rischio elevato per i loro diritti e le loro libertà affinché possano prendere le precauzioni del caso. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e comprendere raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. La comunicazione agli interessati dovrebbe essere effettuata non appena ragionevolmente possibile, in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati sia tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni ripetute o analoghe dei dati potrebbe giustificare più tempo per la comunicazione. Qualora non fosse possibile evitare di compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, evitare di pregiudicare la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, proteggere la sicurezza pubblica o la sicurezza nazionale o tutelare i diritti e le libertà altrui ritardando o limitando la comunicazione di una violazione dei dati personali alla persona fisica interessata, detta comunicazione potrebbe, in casi eccezionali, essere omessa.

(63) Il titolare del trattamento dovrebbe designare una persona che lo assista nel controllo del rispetto a livello interno delle disposizioni adottate ai sensi della presente direttiva, tranne nel caso in cui uno Stato membro decida di esentare le autorità giurisdizionali e le altre autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali. Tale persona potrebbe essere un membro del personale in organico del titolare del trattamento che ha ricevuto una formazione specifica sulla normativa e la prassi in materia di protezione dei dati al fine di acquisire una conoscenza specialistica in questo settore. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base al trattamento di dati effettuato e alla protezione richiesta per i dati personali trattati dal titolare del trattamento. Il suo compito potrebbe essere svolto a tempo parziale o a tempo pieno. Un responsabile della protezione dei dati può essere designato congiuntamente da più titolari del trattamento, tenendo conto della loro struttura organizzativa e dimensione, per esempio in caso di risorse condivise in unità centrali. Tale persona può anche essere nominata per ricoprire diverse posizioni all'interno della struttura dei pertinenti titolari del trattamento. Detta persona dovrebbe aiutare il titolare del trattamento e i dipendenti che trattano dati personali informandoli e consigliandoli in merito al rispetto dei loro pertinenti obblighi in materia di protezione dei dati. Tali responsabili della protezione dei dati dovrebbero poter adempiere le funzioni e ai compiti loro incombenti in maniera indipendente conformemente al diritto dello Stato membro.

(64) Gli Stati membri dovrebbero garantire che un trasferimento verso un paese terzo o un'organizzazione internazionale avvenga unicamente se necessario ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, e che il titolare del trattamento nel paese terzo o presso l'organizzazione internazionale sia un'autorità

competente ai sensi della presente direttiva. Un trasferimento dovrebbe essere effettuato solo a opera delle autorità competenti che agiscono in qualità di titolari del trattamento, tranne nel caso in cui i responsabili del trattamento siano esplicitamente incaricati di effettuare un trasferimento a nome dei titolari del trattamento. Un tale trasferimento è ammesso se la Commissione ha deciso che il paese terzo o l'organizzazione internazionale in questione garantisce un livello di protezione adeguato, se sono state fornite adeguate garanzie o se si applicano deroghe in specifiche situazioni. È opportuno che qualora i dati personali siano trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di protezione delle persone fisiche previsto nell'Unione dalla presente direttiva non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento o responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale.

(65) Qualora i dati personali siano trasferiti da uno Stato membro a paesi terzi o a organizzazioni internazionali, tale trasferimento dovrebbe avvenire, in linea di principio, unicamente dopo che lo Stato membro presso cui sono stati ottenuti i dati ha autorizzato il trasferimento. Nell'interesse di una cooperazione efficace in materia di applicazione della legge occorre che, quando la minaccia alla sicurezza pubblica di uno Stato membro o di un paese terzo o agli interessi vitali di uno Stato membro è così immediata da rendere impossibile il tempestivo ottenimento dell'autorizzazione preliminare, l'autorità competente sia in grado di trasferire i pertinenti dati personali al paese terzo o all'organizzazione internazionale interessati senza autorizzazione preliminare. Gli Stati membri dovrebbero disporre che qualsiasi condizione specifica riguardante il trasferimento sia comunicata ai paesi terzi o alle organizzazioni internazionali. I trasferimenti successivi dei dati personali dovrebbero essere oggetto di un'autorizzazione preliminare da parte dell'autorità competente che ha effettuato il trasferimento originario. Nel decidere in merito alla richiesta di autorizzazione di un trasferimento successivo, l'autorità competente che ha effettuato il trasferimento originario dovrebbe tenere debitamente conto di tutti i fattori pertinenti, tra cui la gravità del reato, le condizioni specifiche alle quali sono soggetti e la finalità per la quale i dati sono stati originariamente trasferiti, la natura e le condizioni dell'esecuzione della sanzione penale e il livello di protezione dei dati personali nel paese terzo o nell'organizzazione internazionale verso i quali i dati personali sono successivamente trasferiti. L'autorità competente che ha effettuato il trasferimento originario dovrebbe inoltre poter subordinare il trasferimento successivo a condizioni specifiche. Tali condizioni specifiche possono essere descritte, per esempio, in codici di gestione.

(66) La Commissione dovrebbe poter decidere, con effetto nell'intera Unione, che taluni paesi terzi, un territorio o uno o più settori specifici all'interno di un paese terzo o un'organizzazione internazionale offrono un livello adeguato di protezione dei dati, garantendo in tal modo la certezza del diritto e l'uniformità in tutta l'Unione nei confronti dei paesi terzi o delle organizzazioni internazionali che si ritiene offrano tale livello di protezione. In tali casi, i trasferimenti di dati personali verso tali paesi dovrebbero poter avere luogo senza specifiche autorizzazioni, tranne nel caso in cui un altro Stato membro presso cui sono stati ottenuti i dati debba autorizzare il trasferimento.

(67) In linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo, è opportuno che la Commissione, nella sua valutazione di un paese terzo, di un territorio o di un settore specifico all'interno di un paese terzo, tenga conto del modo in cui un determinato paese terzo rispetti lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in materia di diritti dell'uomo, nonché la legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure l'ordine pubblico e il diritto penale. L'adozione di una decisione di adeguatezza nei confronti di un territorio o di un settore specifico all'interno di un paese terzo dovrebbe prendere in considerazione criteri chiari e obiettivi come specifiche attività di trattamento e l'ambito di applicazione delle norme giuridiche e degli atti legislativi applicabili in vigore nel paese terzo. Il paese terzo dovrebbe offrire garanzie atte ad assicurare un adeguato livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione, in particolare qualora i dati siano trattati in uno o più settori specifici. In particolare, il paese terzo dovrebbe assicurare un effettivo controllo indipendente della protezione dei dati e dovrebbe prevedere meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri e agli interessati dovrebbero essere riconosciuti diritti effettivi e azionabili e un mezzo di ricorso effettivo in sede amministrativa e giudiziaria.

(68) Al di là degli impegni internazionali che il paese terzo o l'organizzazione internazionale hanno assunto, la Commissione dovrebbe tenere altresì in considerazione gli obblighi derivanti dalla partecipazione del paese terzo o dell'organizzazione internazionale a sistemi multilaterali o regionali, soprattutto in relazione alla protezione dei dati personali, nonché all'attuazione di tali obblighi. In particolare, si dovrebbe tenere in considerazione l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone

rispetto al trattamento automatizzato di dati di carattere personale e relativo protocollo addizionale. La Commissione, nel valutare l'adeguatezza del livello di protezione nei paesi terzi o nelle organizzazioni internazionali, dovrebbe consultare il comitato europeo per la protezione dei dati istituito dal regolamento (UE) 2016/679 («comitato»). La Commissione dovrebbe altresì tenere conto delle eventuali decisioni di adeguatezza pertinenti adottate a norma dell'articolo 45 del regolamento (UE) 2016/679.

(69) È opportuno che la Commissione controlli il funzionamento delle decisioni sul livello di protezione in un paese terzo, in un territorio o settore specifico all'interno di un paese terzo o un'organizzazione internazionale. Nelle sue decisioni di adeguatezza, la Commissione dovrebbe prevedere un meccanismo di riesame periodico del loro funzionamento. Tale riesame periodico dovrebbe essere intrapreso in consultazione con il paese terzo o l'organizzazione internazionale in questione e tenere conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale.

(70) È opportuno che la Commissione sia altresì in grado di riconoscere che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo o un'organizzazione internazionale non garantisca più un livello adeguato di protezione dei dati. Di conseguenza, il trasferimento di dati personali verso tale paese terzo o organizzazione internazionale dovrebbe essere vietato, a meno che non siano soddisfatti i requisiti di cui alla presente direttiva con riguardo ai trasferimenti soggetti ad adeguate salvaguardie e alle deroghe per situazioni specifiche. È opportuno prevedere procedure di consultazione tra la Commissione e detti paesi terzi o organizzazioni internazionali. La Commissione dovrebbe informare tempestivamente il paese terzo o l'organizzazione internazionale dei motivi e avviare consultazioni con questi al fine di risolvere la situazione.

(71) I trasferimenti non effettuati sulla base di una decisione di adeguatezza dovrebbero essere autorizzati unicamente qualora siano offerte adeguate garanzie in uno strumento giuridicamente vincolante, atto ad assicurare la protezione dei dati personali, o qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento dei dati e, sulla base di tale valutazione, ritenga che esistano adeguate garanzie con riguardo alla protezione dei dati personali. Tali strumenti giuridicamente vincolanti potrebbero ad esempio consistere in accordi bilaterali giuridicamente vincolanti che sono stati conclusi dagli Stati membri e recepiti nel loro ordinamento giuridico e che potrebbero essere fatti valere dai loro interessati, così da garantire il rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati, compreso il diritto a un ricorso effettivo in sede amministrativa o giudiziaria. All'atto della valutazione di tutte le circostanze relative al trasferimento dei dati, il titolare del trattamento dovrebbe poter tener conto degli accordi di cooperazione conclusi tra Europol o Eurojust e i paesi terzi che consentono lo scambio di dati personali. Il titolare del trattamento dovrebbe potere inoltre tenere conto del fatto che il trasferimento di dati personali sarà soggetto a obblighi di riservatezza e al principio di specificità, così da garantire che i dati non siano trattati per finalità diverse da quella del trasferimento. Inoltre, il titolare del trattamento dovrebbe tener conto del fatto che i dati personali non saranno utilizzati per richiedere, emettere o eseguire la pena di morte o qualsiasi forma di trattamento crudele e disumano. Benché tali condizioni possano ritenersi garanzie adeguate che consentono il trasferimento dei dati, il titolare del trattamento dovrebbe poter richiedere garanzie supplementari.

(72) In mancanza di una decisione di adeguatezza o di garanzie adeguate, si può procedere a un trasferimento o a una categoria di trasferimenti soltanto in situazioni specifiche se necessario per salvaguardare un interesse vitale dell'interessato o di un'altra persona, o per salvaguardare i legittimi interessi dell'interessato, qualora lo preveda la legislazione dello Stato membro che trasferisce i dati personali; per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo; in un singolo caso per prevenire, indagare, accertare e perseguire reati o eseguire sanzioni penali, incluse la salvaguardia nei confronti e la prevenzione di minacce alla sicurezza pubblica; o in un singolo caso per accertare, esercitare o difendere un diritto in sede giudiziaria. Tali deroghe dovrebbero essere interpretate in modo restrittivo e non dovrebbero consentire trasferimenti frequenti, ingenti e strutturali di dati personali o trasferimenti su larga scala di dati, ma andrebbero invece limitate ai dati strettamente necessari. Tali trasferimenti dovrebbero essere documentati e, su richiesta, messi a disposizione dell'autorità di controllo per consentire il monitoraggio della loro liceità.

(73) Le autorità competenti degli Stati membri applicano accordi internazionali bilaterali o multilaterali vigenti, conclusi con paesi terzi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, ai fini dello scambio di informazioni pertinenti affinché possano eseguire i compiti assegnati loro dalla legge. In linea di principio, ciò avviene tramite o almeno con la cooperazione delle autorità competenti nei paesi terzi interessati ai fini della presente direttiva, talvolta persino in mancanza di un accordo internazionale bilaterale o multilaterale. Tuttavia, in singoli casi specifici, le normali procedure che richiedono di contattare tale autorità nel paese terzo possono risultare inefficaci o inadatte, in particolare in quanto il trasferimento non potrebbe essere effettuato tempestivamente, o in quanto detta autorità nel paese terzo non rispetta lo stato di diritto o le norme e gli standard internazionali in materia di diritti dell'uomo, cosicché le autorità competenti degli Stati membri potrebbero decidere di trasferire i dati personali direttamente ai destinatari stabiliti in detti paesi terzi. Ciò potrebbe verificarsi qualora vi sia urgente necessità di trasferire dati personali per salvare la vita di una persona che rischia di essere vittima di un reato o al fine di evitare l'imminente commissione di un reato, anche

terroristico. Anche se detto trasferimento tra autorità competenti e destinatari stabiliti in paesi terzi dovrebbe prodursi unicamente in singoli casi specifici, la presente direttiva dovrebbe stabilire le condizioni per regolamentare tali casi. Dette disposizioni non dovrebbero essere considerate alla stregua di deroghe ad accordi internazionali bilaterali o multilaterali vigenti nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia. Tali norme dovrebbero applicarsi in aggiunta alle altre disposizioni della presente direttiva, in particolare quelle sulla liceità del trattamento e quelle del capo V.

(74) Con il trasferimento transfrontaliero di dati personali potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati per tutelarsi da usi o divulgazioni illeciti 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 essere ostacolati da poteri insufficienti per prevenire e correggere e da ordinamenti 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.

(75) La designazione negli Stati membri di autorità di controllo che possano agire in totale indipendenza è un elemento essenziale della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali. Spetterebbe alle autorità di controllo sorvegliare l'applicazione delle disposizioni adottate a norma della presente direttiva e contribuire alla loro coerente applicazione in tutta l'Unione, così da tutelare le persone fisiche con riguardo al trattamento dei loro dati personali. A tal fine, le autorità di controllo dovrebbero cooperare tra loro e con la Commissione.

(76) Gli Stati membri possono prevedere che l'autorità di controllo già istituita ai sensi del regolamento (UE) 2016/679 possa assolvere anche i compiti che devono essere adempiuti dalle autorità di controllo nazionali da istituirsi a norma della presente direttiva.

(77) È opportuno che gli Stati membri abbiano la facoltà di istituire più di una autorità di controllo, al fine di rispecchiare la loro struttura costituzionale, organizzativa e amministrativa. Ciascuna autorità di controllo dovrebbe disporre delle risorse umane e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei propri compiti, compresi i compiti di assistenza reciproca e cooperazione con altre autorità di controllo in tutta l'Unione. Ciascuna autorità di controllo dovrebbe disporre di un bilancio annuale, separato e pubblico, che può far parte del bilancio generale statale o nazionale.

(78) Le autorità di controllo dovrebbero essere soggette a meccanismi di controllo o monitoraggio indipendenti con riguardo alle loro spese finanziarie, purché tale controllo finanziario non pregiudichi la loro indipendenza.

(79) Le condizioni generali applicabili al membro o ai membri dell'autorità di controllo dovrebbero essere stabilite nel diritto dello Stato membro e dovrebbero in particolare prevedere che i membri siano nominati dal parlamento o dal governo o dal capo di Stato dello Stato membro, sulla base di una proposta del governo o di un membro del governo, o del parlamento o di una sua camera, o da un organismo indipendente incaricato ai sensi del diritto dello Stato membro della nomina attraverso una procedura trasparente. Al fine di assicurare l'indipendenza dell'autorità di controllo, è opportuno che il membro o i membri di tale autorità agiscano con integrità, si astengano da qualunque azione incompatibile con le loro funzioni e, per tutta la durata del mandato, non esercitino alcuna altra attività professionale incompatibile, remunerata o meno. Al fine di assicurare l'indipendenza dell'autorità di controllo, è opportuno che il personale sia scelto dall'autorità di controllo anche con l'eventuale intervento di un organismo indipendente incaricato ai sensi del diritto dello Stato membro.

(80) Sebbene la presente direttiva si applichi anche alle attività delle autorità giurisdizionali nazionali e di altre autorità giudiziarie, non è opportuno che rientri nella competenza delle autorità di controllo il trattamento di dati personali effettuato dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali, al fine di salvaguardare l'indipendenza dei giudici nell'adempimento dei loro compiti giurisdizionali. Tale esenzione dovrebbe essere limitata all'attività giurisdizionale e non applicarsi ad altre attività a cui i giudici potrebbero partecipare in forza del diritto dello Stato membro. Gli Stati membri dovrebbero inoltre poter disporre che nella competenza delle autorità di controllo non rientri il trattamento di dati personali effettuato da altre autorità giudiziarie indipendenti nell'esercizio delle loro funzioni giurisdizionali, ad esempio le procure. In ogni caso, il rispetto delle norme della presente direttiva da parte di autorità giurisdizionali e altre autorità giudiziarie indipendenti è sempre soggetto a un controllo indipendente conformemente all'articolo 8, paragrafo 3, della Carta.

(81) È opportuno che ciascuna autorità di controllo tratti i reclami proposti da qualsiasi interessato e svolga le relative indagini o li trasmetta alla competente autorità di controllo. A seguito di reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nella fattispecie. È opportuno che l'autorità di controllo informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato dovrebbe ricevere informazioni interlocutorie.

(82) Al fine di garantire un monitoraggio efficace, affidabile e coerente del rispetto e dell'applicazione della presente direttiva in tutta l'Unione, conformemente al TFUE come interpretato Corte di giustizia, le autorità di controllo dovrebbero avere in ciascuno Stato membro gli stessi compiti e poteri effettivi, fra cui poteri di indagine, correttivi e consultivi, che costituiscono mezzi necessari per eseguire i loro compiti. I loro poteri, tuttavia, non dovrebbero interferire con le norme specifiche per i procedimenti penali, compresi l'indagine e il perseguimento di reati, o con l'indipendenza della magistratura. Fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale ai sensi del diritto dello Stato membro, le autorità di controllo dovrebbero inoltre avere la facoltà di agire in sede giudiziale o stragiudiziale in caso di violazione della presente direttiva. È opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e dal diritto dello Stato membro, in modo imparziale ed equo ed entro un termine ragionevole. In particolare, ogni misura dovrebbe essere appropriata, necessaria e proporzionata al fine di assicurare la conformità alla presente direttiva, tenuto conto delle circostanze di ciascun singolo caso, rispettare il diritto di ogni persona di essere ascoltata prima che sia adottato nei suoi confronti un provvedimento individuale che le rechi pregiudizio ed evitare costi superflui ed eccessivi disagi per la persona interessata. I poteri di indagine per quanto riguarda l'accesso ai locali dovrebbero essere esercitati nel rispetto dei requisiti specifici previsti dal diritto dello Stato membro, quale l'obbligo di ottenere un'autorizzazione giudiziaria preliminare. L'adozione di una decisione giuridicamente vincolante dovrebbe essere soggetta a controllo giurisdizionale nello Stato membro dell'autorità di controllo che ha adottato la decisione.

(83) Le autorità di controllo dovrebbero prestarsi assistenza reciproca nell'adempimento dei loro compiti, in modo da garantire la coerente applicazione e attuazione delle disposizioni adottate a norma della presente direttiva.

(84) Il comitato dovrebbe contribuire all'applicazione uniforme della presente direttiva in tutta l'Unione, in particolare fornendo consulenza alla Commissione e promuovendo la cooperazione delle autorità di controllo in tutta l'Unione.

(85) Ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo e a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode ai sensi delle disposizioni adottate a norma della presente direttiva o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato. Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico. È opportuno che l'autorità di controllo competente informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato dovrebbe ricevere informazioni interlocutorie. Per agevolare la proposizione di reclami, ogni autorità di controllo dovrebbe adottare misure quali la messa a disposizione di un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.

(86) Ogni persona fisica o giuridica dovrebbe avere diritto a un ricorso giurisdizionale effettivo dinanzi alle competenti autorità giurisdizionali nazionali avverso una decisione dell'autorità di controllo che produce effetti giuridici nei confronti di tale persona. Tale decisione riguarda in particolare l'esercizio di poteri di indagine, correttivi e autorizzativi da parte dell'autorità di controllo o l'archiviazione o il rigetto dei reclami. Tuttavia, tale diritto non comprende altre misure delle autorità di controllo che non sono giuridicamente vincolanti, come pareri o consulenza forniti dall'autorità di controllo. Le azioni nei confronti di un'autorità di controllo dovrebbero essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita e dovrebbero essere effettuate conformemente al diritto dello Stato membro in questione. Tali autorità giurisdizionali dovrebbero esercitare i loro pieni poteri giurisdizionali, ivi compreso quello di esaminare tutte le questioni di fatto e di diritto che abbiano rilevanza per la controversia dinanzi a esse pendente.

(87) Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma della presente direttiva, dovrebbe avere il diritto di dare mandato a un organismo che intenda tutelare i diritti e gli interessi degli interessati in

relazione alla protezione dei loro dati personali e sia istituito conformemente al diritto di uno Stato membro, per proporre reclamo per suo conto a un'autorità di controllo o esercitare il diritto a un ricorso giurisdizionale. Il diritto di rappresentanza degli interessati non dovrebbe pregiudicare il diritto processuale dello Stato membro, che può prescrivere l'obbligo per gli interessati di essere rappresentati da un avvocato dinanzi alle autorità giurisdizionali nazionali, come definito nella direttiva 77/249/CEE del Consiglio ([1]).

(88) Il titolare del trattamento o qualsiasi altra autorità competente ai sensi del diritto dello Stato membro dovrebbe risarcire la persona interessata per i danni cagionati da un trattamento che violi le disposizioni adottate a norma della presente direttiva. Il concetto di danno dovrebbe essere interpretato estensivamente alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi della presente direttiva. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o dello Stato membro. Quando si fa riferimento a un trattamento illecito o che violi le disposizioni adottate a norma della presente direttiva, esso comprende anche il trattamento che viola atti di esecuzione adottati ai sensi della presente direttiva. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito.

(89) Dovrebbe essere punibile chiunque, persona fisica o giuridica, di diritto pubblico o di diritto privato, violi la presente direttiva. Gli Stati membri dovrebbero garantire sanzioni effettive, proporzionate e dissuasive e dovrebbero adottare tutte le misure necessarie per la loro applicazione.

(90) Al fine di garantire condizioni uniformi di esecuzione della presente direttiva, dovrebbero essere attribuite alla Commissione competenze di esecuzione riguardanti l'adeguato livello di protezione offerto da un paese terzo, da un territorio o da un settore specifico all'interno di un paese terzo o da un'organizzazione internazionale e il formato e le procedure per l'assistenza reciproca e le modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio ([2]).

(91) È opportuno applicare la procedura d'esame per l'adozione di atti di esecuzione sull'adeguato livello di protezione offerto da un paese terzo, da un territorio o da un settore specifico all'interno di un paese terzo o da un'organizzazione internazionale e sul formato e le procedure per l'assistenza reciproca e sulle modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato in considerazione della portata generale di tali atti.

(92) È opportuno che la Commissione adotti atti di esecuzione immediatamente applicabili quando, in casi debitamente giustificati relativi a un paese terzo, a un territorio o a un settore specifico all'interno di un paese terzo, o a un'organizzazione internazionale che non garantisce più un livello di protezione adeguato, ciò sia reso necessario da imperativi motivi di urgenza.

(93) Poiché gli obiettivi della presente direttiva, vale a dire tutelare i diritti 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 ma piuttosto, a motivo della portata e degli effetti dell'azione in questione, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 TUE. La presente direttiva si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(94) È opportuno che rimangano impregiudicate le disposizioni specifiche di atti dell'Unione nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia adottati prima della data di adozione della presente direttiva e che disciplinano il trattamento dei dati personali tra Stati membri e l'accesso delle

([1]) Direttiva 77/249/CEE del Consiglio, del 22 marzo 1977, intesa a facilitare l'esercizio effettivo della libera prestazione di servizi da parte degli avvocati (GU L 78 del 26.3.1977, pag. 17).

([2]) Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13).

autorità nazionali designate ai sistemi di informazione istituiti ai sensi dei trattati, quali, ad esempio, le disposizioni specifiche relative alla protezione dei dati personali applicate ai sensi della decisione 2008/615/GAI del Consiglio ([1]) o dell'articolo 23 della convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea ([2]). Poiché l'articolo 8 della Carta e l'articolo 16 TFUE richiedono che il diritto fondamentale alla protezione dei dati personali sia assicurato in maniera coerente in tutta l'Unione, è opportuno 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. Se del caso, la Commissione dovrebbe presentare proposte intese ad assicurare norme giuridiche coerenti riguardo al trattamento dei dati personali.

(95) Per garantire una sistematica e coerente protezione dei dati personali nell'Unione, dovrebbero rimanere in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali che siano stati conclusi dagli Stati membri anteriormente alla data di entrata in vigore della presente direttiva e che siano conformi al pertinente diritto dell'Unione applicabile anteriormente a tale data.

(96) Agli Stati membri dovrebbe essere concesso un periodo di non più di due anni dalla data di entrata in vigore della presente direttiva per recepirla. Il trattamento già in corso a tale data dovrebbe essere reso conforme alla presente direttiva entro un periodo di due anni dall'entrata in vigore della presente direttiva. Tuttavia, qualora tale trattamento sia conforme al diritto dell'Unione applicabile anteriormente alla data di entrata in vigore della presente direttiva, i requisiti della presente direttiva relativi alla consultazione preventiva dell'autorità di controllo non dovrebbero applicarsi ai trattamenti già in corso alla data suddetta, dato che tali requisiti, per loro stessa natura, devono essere soddisfatti prima del trattamento. Qualora gli Stati membri si avvalgano del periodo di attuazione più lungo che si conclude sette anni dopo la data di entrata in vigore della presente direttiva per conformarsi agli obblighi di registrazione per i sistemi di trattamento automatizzato istituiti prima della data suddetta, il titolare del trattamento o il responsabile del trattamento dovrebbe aver posto in essere metodi efficaci per dimostrare la liceità del trattamento dei dati, rendere possibile l'autocontrollo e assicurare l'integrità e la sicurezza dei dati, quali registrazioni e altre forme di documentazione.

(97) 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 2011/93/UE del Parlamento europeo e del Consiglio ([3]).

(98) La decisione quadro 2008/977/GAI dovrebbe pertanto essere abrogata.

(99) A norma dell'articolo 6 *bis* del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al TUE e al TFUE, il Regno Unito e l'Irlanda non sono vincolati da norme stabilite nella presente direttiva che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE laddove il Regno Unito e l'Irlanda non siano vincolati da norme 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 TFUE.

(100) A norma degli articoli 2 e 2 *bis* del protocollo n. 22 sulla posizione della Danimarca, allegato al TUE e al TFUE, la Danimarca non è vincolata da norme stabilite nella presente direttiva che riguardano il trattamento dei dati personali da parte degli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione della parte terza, titolo V, capi 4 o 5, TFUE né è soggetta alla loro applicazione. Dato che la presente direttiva si basa sull'acquis di Schengen in applicazione della parte terza, titolo V, TFUE, la Danimarca decide, ai sensi dell'articolo 4 di tale protocollo, entro sei mesi dall'adozione della presente direttiva, se intende recepirla nel proprio diritto interno.

(101) 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 ([4]).

([1]) Decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera (GU L 210 del 6.8.2008, pag. 1).

([2]) Atto del Consiglio, del 29 maggio 2000, che stabilisce, conformemente all'articolo 34 del trattato sull'Unione europea, la convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea (GU C 197 del 12.7.2000, pag. 1).

([3]) Direttiva 2011/93/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).

([4]) GU L 176 del 10.7.1999, pag. 36.

(102) 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 ([1]).

(103) Per quanto riguarda il Liechtenstein, la presente direttiva costituisce uno sviluppo delle disposizioni dell'acquis di Schengen ai sensi del protocollo 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 ([2]).

(104) La presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta, sanciti dal TFUE, 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.

(105) Conformemente alla dichiarazione politica comune del 28 settembre 2011 degli Stati membri e della Commissione sui documenti esplicativi, gli Stati membri si sono impegnati ad accompagnare, in casi giustificati, la notifica delle loro misure di recepimento con uno o più documenti che chiariscano il rapporto tra gli elementi costitutivi di una direttiva e le parti corrispondenti delle misure nazionali di recepimento. Per quanto riguarda la presente direttiva, il legislatore ritiene che la trasmissione di tali documenti sia giustificata.

(106) Conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001, il garante europeo della protezione dei dati è stato consultato e ha espresso un parere il 7 marzo 2012 ([3]).

(107) La presente direttiva non dovrebbe pregiudicare la facoltà degli Stati membri di dare attuazione all'esercizio dei diritti dell'interessato in materia di informazione, accesso, rettifica o cancellazione di dati personali e limitazione del trattamento nel corso di un procedimento penale e, alle eventuali limitazioni di tali diritti, nelle norme nazionali di procedura penale,

HANNO ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

Disposizioni generali

Articolo 1

Oggetto e obiettivi

1. La presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

2. Ai sensi 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, qualora tale scambio sia richiesto dal diritto dell'Unione o da quello dello Stato membro, non sia limitato né vietato per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

([1]) GU L 53 del 27.2.2008, pag. 52.
([2]) GU L 160 del 18.6.2011, pag. 21.
([3]) GU C 192 del 30.6.2012, pag. 7.

3. La presente direttiva non pregiudica la facoltà degli Stati membri di prevedere garanzie più elevate di quelle in essa stabilite per la tutela dei diritti e delle libertà dell'interessato con riguardo al trattamento dei dati personali da parte delle autorità competenti.

Articolo 2

Ambito di 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. La presente direttiva non si applica ai trattamenti di dati personali:

a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione;

b) effettuati da istituzioni, organi, uffici e agenzie dell'Unione.

Articolo 3

Definizioni

Ai fini della presente direttiva si intende per:

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

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

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

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

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

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «autorità competente»:

   a) qualsiasi autorità pubblica competente in materia di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; o

   b) qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica;

8) «titolare del trattamento»: l'autorità competente che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o dello Stato membro, il titolare del trattamento o i criteri specifici applicabili alla sua nomina possono essere previsti dal diritto dell'Unione o dello Stato membro;

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

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

11) «violazione dei dati personali»: la violazione della sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

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

13) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

14) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

15) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 41;

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

CAPO II

Principi

Articolo 4

Principi applicabili al trattamento di dati personali

1. Gli Stati membri dispongono che i dati personali siano:

a) trattati in modo lecito e corretto;

b) raccolti per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità;

c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati;

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

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 in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

2. Il trattamento da parte dello stesso o di un altro titolare del trattamento per una qualsiasi delle finalità di cui all'articolo 1, paragrafo 1, diversa da quella per cui sono raccolti i dati personali, è consentito nella misura in cui:

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

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

3. Il trattamento da parte dello stesso o di un altro titolare del trattamento può comprendere l'archiviazione nel pubblico interesse, l'utilizzo scientifico, storico o statistico per le finalità di cui all'articolo 1, paragrafo 1, fatte salve le garanzie adeguate per i diritti e le libertà degli interessati.

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

Articolo 5

Termini per conservazione ed esame

Gli Stati membri dispongono che siano fissati adeguati termini per la cancellazione dei dati personali o per un esame periodico della necessità della conservazione dei dati personali. Misure procedurali garantiscono che tali termini siano rispettati.

Articolo 6

Distinzione tra diverse categorie di interessati

Gli Stati membri dispongono che il titolare del trattamento, se del caso e nella misura del possibile, operi una chiara distinzione tra i dati personali delle 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, e

d) altre parti rispetto a un 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).

Articolo 7

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

1. Gli Stati membri dispongono che i dati personali fondati su fatti siano differenziati, nella misura del possibile, da quelli fondati su valutazioni personali.

2. Gli Stati membri dispongono che le autorità competenti adottino tutte le misure ragionevoli per garantire che i dati personali inesatti, incompleti o non più aggiornati non siano trasmessi o resi disponibili. A tal fine, ciascuna autorità competente verifica, per quanto possibile, la qualità dei dati personali prima che questi siano trasmessi o resi disponibili. Per quanto possibile, tutte le trasmissioni di dati personali sono corredate delle informazioni necessarie che consentono all'autorità competente ricevente di valutare il grado di esattezza, completezza e affidabilità dei dati personali, e la misura in cui essi sono aggiornati.

3. Qualora risulti che sono stati trasmessi dati personali inesatti o che sono stati trasmessi dati personali illecitamente, il destinatario deve esserne informato quanto prima. In tal caso, i dati personali devono essere rettificati o cancellati o il trattamento deve essere limitato a norma dell'articolo 16.

Articolo 8

Liceità del trattamento

1. Gli Stati membri dispongono che il trattamento sia lecito solo se e nella misura in cui è necessario per l'esecuzione di un compito di un'autorità competente, per le finalità di cui all'articolo 1, paragrafo 1, e si basa sul diritto dell'Unione o dello Stato membro.

2. Il diritto dello Stato membro che disciplina il trattamento nell'ambito di applicazione della presente direttiva specifica quanto meno gli obiettivi del trattamento, i dati personali da trattare e le finalità del trattamento.

Articolo 9

Condizioni di trattamento specifiche

1. I dati personali raccolti dalle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1, non possono essere trattati per finalità diverse da quelle di cui all'articolo 1, paragrafo 1, a meno che tale trattamento non sia autorizzato dal diritto dell'Unione o dello Stato membro. Qualora i dati personali siano trattati per tali finalità diverse, si applica il regolamento (UE) 2016/679, a meno che il trattamento non sia effettuato nell'ambito di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione.

2. Qualora il diritto dello Stato membro affidi alle autorità competenti l'esecuzione di compiti diversi da quelli eseguiti per le finalità di cui all'articolo 1, paragrafo 1, il regolamento (UE) 2016/679 si applica al trattamento per tali finalità, comprese quelle di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per finalità statistiche, a meno che il trattamento non sia effettuato nel contesto di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione.

3. Gli Stati membri dispongono che, nei casi in cui il diritto dell'Unione o dello Stato membro applicabile all'autorità competente che trasmette i dati preveda condizioni specifiche per il trattamento, l'autorità competente che trasmette i dati informi il destinatario di tali dati personali di tali condizioni e dell'obbligo di rispettarle.

4. Gli Stati membri dispongono che l'autorità competente che trasmette i dati non applichi a destinatari di altri Stati membri o a agenzie, uffici e organi istituiti a norma del titolo V, capi 4 e 5, TFUE condizioni ai sensi del paragrafo 3 diverse da quelle applicabili a trasmissioni di dati analoghe all'interno dello Stato membro dell'autorità competente che trasmette i dati.

Articolo 10

Trattamento di categorie particolari di dati personali

Il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, e il trattamento di dati genetici, di dati biometrici intesi a identificare in modo univoco una persona fisica o di dati relativi alla salute o di dati relativi alla vita sessuale della persona fisica o all'orientamento sessuale è autorizzato solo se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto:

a) se autorizzato dal diritto dell'Unione o dello Stato membro;

b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o

c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato.

Articolo 11

Processo decisionale automatizzato relativo alle persone fisiche

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

2. Le decisioni di cui al paragrafo 1 del presente articolo non si basano sulle categorie particolari di dati personali di cui all'articolo 10, a meno che non siano in vigore misure adeguate a salvaguardia dei diritti, delle libertà e dei legittimi interessi dell'interessato.

3. La profilazione che porta alla discriminazione di persone fisiche sulla base di categorie particolari di dati personali di cui all'articolo 10 è vietata, conformemente al diritto dell'Unione.

CAPO III

Diritti dell'interessato

Articolo 12

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

1. Gli Stati membri dispongono che il titolare del trattamento adotti misure ragionevoli per fornire all'interessato tutte le informazioni di cui all'articolo 13 e faccia le comunicazioni con riferimento agli articoli 11, da 14 a 18 e 31, relative al trattamento, in forma concisa, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro. Le informazioni sono fornite con qualsiasi mezzo adeguato, anche per via elettronica. Come regola generale il titolare del trattamento fornisce le informazioni nella stessa forma della richiesta.

2. Gli Stati membri dispongono che il titolare del trattamento faciliti l'esercizio dei diritti di cui agli articoli 11 e da 14 a 18 da parte dell'interessato.

3. Gli Stati membri dispongono che il titolare del trattamento informi senza ingiustificato ritardo l'interessato per iscritto del seguito alla sua richiesta.

4. Gli Stati membri dispongono che le informazioni fornite ai sensi dell'articolo 13 ed eventuali comunicazioni effettuate o azioni intraprese ai sensi degli articoli 11, da 14 a 18 e 31 siano gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta, oppure

b) rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

5. Qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta una richiesta di cui agli articoli 14 o 16, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

Articolo 13

Informazioni da rendere disponibili o da fornire all'interessato

1. Gli Stati membri dispongono che il titolare del trattamento metta a disposizione dell'interessato almeno le seguenti informazioni:

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

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

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

d) il diritto di proporre reclamo a un'autorità di controllo e i dati di contatto di detta autorità;

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

2. In aggiunta alle informazioni di cui al paragrafo 1,gli Stati membri dispongono per legge che il titolare del trattamento fornisca all'interessato, in casi specifici, le seguenti ulteriori informazioni per consentire l'esercizio dei diritti dell'interessato:

a) la base giuridica per il trattamento;

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

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

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

3. Gli Stati membri possono adottare misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato ai sensi del paragrafo 2 nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:

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

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

c) proteggere la sicurezza pubblica;

d) proteggere la sicurezza nazionale;

e) proteggere i diritti e le libertà altrui.

4. Gli Stati membri possono adottare misure legislative al fine di determinare le categorie di trattamenti cui può applicarsi, in tutto o in parte, una delle lettere del paragrafo 3.

Articolo 14

Diritto di accesso dell'interessato

Fatto salvo l'articolo 15, gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità e la base giuridica del trattamento;

b) le categorie di dati personali trattati;

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

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

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

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.

Articolo 15

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 e per il tempo in cui tale limitazione totale o parziale costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:

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

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

c) proteggere la sicurezza pubblica;

d) proteggere la sicurezza nazionale;

e) proteggere i diritti e le libertà altrui.

2. Gli Stati membri possono adottare misure legislative al fine di determinare le categorie di trattamenti cui possono applicarsi, in tutto o in parte, le lettere da a) a e) del paragrafo 1.

3. Nei casi di cui ai paragrafi 1 e 2, gli Stati membri dispongono che il titolare del trattamento informi l'interessato, senza ingiustificato ritardo e per iscritto, di ogni rifiuto o limitazione dell'accesso e dei motivi del rifiuto o della limitazione. Detta comunicazione può essere omessa qualora il suo rilascio rischi di compromettere una delle finalità di cui al paragrafo 1. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato della possibilità di proporre reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale.

4. Gli Stati membri dispongono che il titolare del trattamento documenti i motivi di fatto o di diritto su cui si basa la decisione. Tali informazioni sono rese disponibili alle autorità di controllo.

Articolo 16

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

1. Gli Stati membri dispongono che l'interessato abbia il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, gli Stati membri dispongono che l'interessato abbia il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

2. Gli Stati membri impongono al titolare del trattamento di cancellare i dati personali senza ingiustificato ritardo e stabiliscono il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione di dati personali che lo riguardano senza ingiustificato ritardo qualora il trattamento violi le disposizioni adottate a norma degli articoli 4, 8 o 10 o qualora i dati personali debbano essere cancellati per conformarsi a un obbligo legale al quale è soggetto il titolare del trattamento.

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

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

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

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

4. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato per iscritto di ogni rifiuto di rettifica o cancellazione dei dati personali o limitazione del trattamento e dei motivi del rifiuto. Gli Stati membri possono adottare misure legislative volte a limitare, in tutto o in parte, l'obbligo di fornire tali informazioni nella misura in cui tale limitazione costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata per:

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

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

c) proteggere la sicurezza pubblica;

d) proteggere la sicurezza nazionale;

e) proteggere i diritti e le libertà altrui.

Gli Stati membri dispongono che il titolare del trattamento informi l'interessato delle possibilità di proporre reclamo dinanzi a un'autorità di controllo o di proporre ricorso giurisdizionale.

5. Gli Stati membri dispongono che il titolare del trattamento comunichi le rettifiche dei dati personali inesatti all'autorità competente da cui i dati personali inesatti provengono.

6. Gli Stati membri dispongono che, qualora i dati personali siano stati rettificati o cancellati o il trattamento sia stato limitato a norma dei paragrafi 1, 2 e 3, il titolare del trattamento ne informi i destinatari e che i destinatari rettifichino o cancellino i dati personali o limitino il trattamento dei dati personali sotto la propria responsabilità.

Articolo 17

Esercizio dei diritti dell'interessato e verifica da parte dell'autorità di controllo

1. Nei casi di cui all'articolo 13, paragrafo 3, all'articolo 15, paragrafo 3, e all'articolo 16, paragrafo 4, gli Stati membri adottano misure che dispongano che i diritti dell'interessato possano essere esercitati anche tramite l'autorità di controllo competente.

2. Gli Stati membri dispongono che il titolare del trattamento informi l'interessato della possibilità di esercitare i suoi diritti tramite l'autorità di controllo ai sensi del paragrafo 1.

3. Qualora sia esercitato il diritto di cui al paragrafo 1, l'autorità di controllo informa l'interessato, perlomeno, di aver eseguito tutte le verifiche necessarie o un riesame. L'autorità di controllo informa inoltre l'interessato del diritto di quest'ultimo di proporre ricorso giurisdizionale.

Articolo 18

Diritti dell'interessato nel corso di indagini e procedimenti penali

Gli Stati membri possono disporre che i diritti di cui agli articoli 13, 14 e 16 siano esercitati conformemente al diritto dello Stato membro qualora i dati personali figurino in una decisione giudiziaria, in un casellario o in un fascicolo giudiziario oggetto di trattamento nel corso di un'indagine e di un procedimento penale.

CAPO IV

Titolare del trattamento e responsabile del trattamento

Sezione 1

Obblighi generali

Articolo 19

Obblighi del titolare del trattamento

1. Gli Stati membri dispongono che il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato ai sensi della presente direttiva. Tali misure sono riesaminate e aggiornate qualora necessario.

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

Articolo 20

Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

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

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

Articolo 21

Contitolari del trattamento

1. Gli Stati membri dispongono che, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi siano contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza della presente direttiva, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui all'articolo 13, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo designa il punto di contatto per gli interessati. Gli Stati membri possono designare quale dei contitolari del trattamento possa fungere da punto di contatto unico ai fini dell'esercizio da parte degli interessati dei loro diritti.

2. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, gli Stati membri possono disporre che l'interessato possa esercitare i propri diritti a norma delle disposizioni adottate ai sensi della presente direttiva nei confronti di e contro ciascun titolare del trattamento.

Articolo 22

Responsabile del trattamento

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

2. Gli Stati membri dispongono che il responsabile del trattamento non ricorra a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di obiettare a tali modifiche.

3. Gli Stati membri dispongono che l'esecuzione dei trattamenti da parte di un responsabile del trattamento sia disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o dello Stato membro, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Tale contratto o altro atto giuridico deve prevedere in particolare che il responsabile del trattamento:

a) agisca soltanto su istruzione del titolare del trattamento;

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

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

d) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi di trattamento di dati e cancelli le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati personali;

e) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare la conformità con il presente articolo;

f) soddisfi le condizioni di cui ai paragrafi 2 e 3 per ricorrere a un altro responsabile del trattamento.

4. Il contratto o l'altro atto giuridico di cui al paragrafo 3 è stipulato per iscritto, anche in formato elettronico.

5. Se un responsabile del trattamento determina, in violazione della presente direttiva, le finalità e i mezzi del trattamento, è considerato un titolare del trattamento relativamente al trattamento in questione.

Articolo 23

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

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

Articolo 24

Registri delle attività di trattamento

1. Gli Stati membri dispongono che i titolari del trattamento tengano un registro di tutte le categorie di attività di trattamento sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, se del caso, di ogni contitolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

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

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

e) se del caso, il ricorso alla profilazione;

f) se del caso, le categorie di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;

g) un'indicazione della base giuridica del trattamento, compresi i trasferimenti, al quale sono destinati i dati personali;

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

i) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 29, paragrafo 1.

2. Gli Stati membri dispongono che tutti i responsabili del trattamento tengano un registro di tutte le categorie di attività di trattamento svolte per conto di un titolare del trattamento, contenente:

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

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

c) se del caso, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale ove esplicitamente istruito in tal senso dal titolare del trattamento, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 29, paragrafo 1.

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

Su richiesta, il titolare del trattamento e il responsabile del trattamento mettono tali registri a disposizione dell'autorità di controllo.

Articolo 25

Registrazione

1. Gli Stati membri dispongono che siano registrati in sistemi di trattamento automatizzato almeno i seguenti trattamenti: raccolta, modifica, consultazione, comunicazione, inclusi i trasferimenti, interconnessione e cancellazione. Le registrazioni delle consultazioni e delle comunicazioni consentono di stabilire la motivazione, la data e l'ora di tali operazioni e, nella misura del possibile, di identificare la persona che ha consultato o comunicato i dati personali, nonché di stabilire l'identità dei destinatari di tali dati personali.

2. Le registrazioni sono usate ai soli fini della verifica della liceità del trattamento, dell'autocontrollo, per garantire l'integrità e la sicurezza dei dati personali e nell'ambito di procedimenti penali.

3. Su richiesta, il titolare del trattamento e il responsabile del trattamento mettono le registrazioni a disposizione dell'autorità di controllo.

Articolo 26

Cooperazione con l'autorità di controllo

Gli Stati membri dispongono che il titolare del trattamento e il responsabile del trattamento cooperino, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

Articolo 27

Valutazione d'impatto sulla protezione dei dati

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

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

Articolo 28

Consultazione preventiva dell'autorità di controllo

1. Gli Stati membri dispongono che il titolare del trattamento o il responsabile del trattamento consulti l'autorità di controllo prima del trattamento di dati personali che figureranno in un nuovo archivio di prossima creazione se:

a) una valutazione d'impatto sulla protezione dei dati di cui all'articolo 27 indica che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio; oppure

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

2. Gli Stati membri dispongono che l'autorità di controllo sia consultata durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su tale atto legislativo relativamente al trattamento.

3. Gli Stati membri dispongono che l'autorità di controllo possa stabilire un elenco di trattamenti soggetti a consultazione preventiva ai sensi del paragrafo 1.

4. Gli Stati membri dispongono che il titolare del trattamento trasmetta all'autorità di controllo la valutazione d'impatto sulla protezione dei dati di cui all'articolo 27 e, su richiesta, ogni altra informazione, al fine di consentire all'autorità di controllo di effettuare una valutazione della conformità del trattamento, in particolare dei rischi per la protezione dei dati personali dell'interessato e delle relative garanzie.

5. Gli Stati membri dispongono che, se ritiene che il trattamento previsto di cui al paragrafo 1 del presente articolo violi le disposizioni adottate a norma della presente direttiva, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisca, entro un termine di sei settimane dal ricevimento della richiesta di consultazione, un parere per iscritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e possa avvalersi dei poteri di cui all'articolo 47. Tale periodo può essere prorogato di un mese, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione.

Sezione 2

Sicurezza dei dati personali

Articolo 29

Sicurezza del trattamento

1. Gli Stati membri dispongono che il titolare del trattamento e il responsabile del trattamento, tenuto conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, mettano in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, in particolare riguardo al trattamento di categorie particolari di dati personali di cui all'articolo 10.

2. Ciascuno Stato membro dispone che per il trattamento automatizzato il titolare del trattamento o il responsabile 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 («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 personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

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

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

f) garantire la possibilità di verificare e accertare gli organismi ai quali 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, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali 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 conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Articolo 30

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

1. Gli Stati membri dispongono che, in caso di violazione dei dati personali, il titolare del trattamento notifichi la violazione all'autorità di controllo senza ingiustificato ritardo, ove possibile entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

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

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

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

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

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

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

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

5. Gli Stati membri dispongono che il titolare del trattamento documenti qualsiasi violazione dei dati personali di cui al paragrafo 1, comprese le circostanze in cui si è verificata la violazione dei dati personali, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

6. Gli Stati membri dispongono che, se la violazione dei dati personali riguarda dati personali che sono stati trasmessi dal o al titolare del trattamento di un altro Stato membro, le informazioni di cui al paragrafo 3 siano comunicate al titolare del trattamento di tale Stato membro senza ingiustificato ritardo.

Articolo 31

Comunicazione di una violazione dei dati personali all'interessato

1. Gli Stati membri dispongono che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunichi la violazione all'interessato senza ingiustificato ritardo.

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 30, paragrafo 3, lettere b), c) e d).

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

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

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

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

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

5. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo può essere ritardata, limitata od omessa alle condizioni e per i motivi di cui all'articolo 13, paragrafo 3.

Sezione 3

Responsabile della protezione dei dati

Articolo 32

Designazione del responsabile della protezione dei dati

1. Gli Stati membri dispongono che il titolare del trattamento designi un responsabile della protezione dei dati. Gli Stati membri possono esentare le autorità giurisdizionali e le altre autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali da tale obbligo.

2. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 34.

3. Può essere designato un unico responsabile della protezione dei dati per più autorità competenti, tenuto conto della loro struttura organizzativa e dimensione.

4. Gli Stati membri dispongono che il titolare del trattamento pubblichi i dati di contatto del responsabile della protezione dei dati e le comunichi all'autorità di controllo.

Articolo 33

Posizione del responsabile della protezione dei dati

1. Gli Stati membri dispongono che il titolare del trattamento si assicuri che il responsabile della protezione dei dati sia coinvolto adeguatamente e tempestivamente in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare del trattamento sostiene il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 34 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Articolo 34

Compiti del responsabile della protezione dei dati

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

a) informare e consigliare il titolare del trattamento e i dipendenti che effettuano il trattamento in merito ai loro obblighi derivanti dalla presente direttiva nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza della presente direttiva, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 27;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 28, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

CAPO V

Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

Articolo 35

Principi generali per il trasferimento di dati personali

1. Gli Stati membri dispongono che qualunque trasferimento, a cura delle autorità competenti, di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi verso un altro paese terzo o un'altra organizzazione internazionale, abbia luogo, fatta salva la conformità alle disposizioni nazionali adottate a norma delle altre disposizioni della presente direttiva, soltanto se sono soddisfatte le condizioni di cui al presente capo, vale a dire:

a) il trasferimento è necessario per le finalità di cui all'articolo 1, paragrafo 1;

b) i dati personali sono trasferiti al titolare del trattamento in un paese terzo o un'organizzazione internazionale che sia un'autorità competente per le finalità di cui all'articolo 1, paragrafo 1;

c) qualora i dati personali siano trasmessi o resi disponibili da un altro Stato membro, tale Stato membro ha fornito la propria autorizzazione preliminare al trasferimento conformemente al proprio diritto nazionale;

d) la Commissione ha adottato una decisione di adeguatezza, a norma dell'articolo 36, oppure, in mancanza di detta decisione, sono state fornite o esistono garanzie adeguate ai sensi dell'articolo 37, oppure, in mancanza di una decisione di adeguatezza ai sensi dell'articolo 36 e di garanzie adeguate ai sensi dell'articolo 37, si applicano deroghe per situazioni specifiche a norma dell'articolo 38; e

e) in caso di trasferimento successivo a un altro paese terzo o a un'altra organizzazione internazionale, l'autorità competente che ha effettuato il trasferimento originario o un'altra autorità competente dello stesso Stato membro autorizza il trasferimento successivo, dopo aver tenuto debitamente conto di tutti i fattori pertinenti, tra cui la gravità del reato, la finalità per la quale i dati personali sono stati originariamente trasferiti e il livello di protezione dei dati personali nel paese terzo o nell'organizzazione internazionale verso i quali i dati personali sono successivamente trasferiti.

2. Gli Stati membri dispongono che i trasferimenti senza l'autorizzazione preventiva di un altro Stato membro conformemente al paragrafo 1, lettera c), siano consentiti soltanto se il trasferimento di dati personali è necessario per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo o agli interessi vitali di uno Stato membro e l'autorizzazione preliminare non può essere ottenuta tempestivamente. L'autorità competente a rilasciare l'autorizzazione preliminare è informata senza indugio.

3. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche assicurato dalla presente direttiva non sia pregiudicato.

Articolo 36

Trasferimento sulla base di una decisione di adeguatezza

1. Gli Stati membri dispongono che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale sia ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

2. Nel valutare l'adeguatezza del livello di protezione la Commissione prende in considerazione in particolare i seguenti elementi:

a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), come anche l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le regole professionali e le misure di sicurezza, comprese le regole per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza, nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono trasferiti;

b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri esecutivi, per assistere e consigliare gli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e

c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.

3. La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante un atto di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, se del caso, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 58, paragrafo 2.

4. La Commissione controlla su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate a norma del paragrafo 3.

5. Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 del presente articolo mediante atti di esecuzione senza effetto retroattivo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 58, paragrafo 2.

Per imperativi motivi di urgenza debitamente giustificati, la Commissione adotta atti di esecuzione immediatamente applicabili secondo la procedura di cui all'articolo 58, paragrafo 3.

6. La Commissione avvia consultazioni con il paese terzo o l'organizzazione internazionale per porre rimedio alla situazione che ha motivato la decisione di cui al paragrafo 5.

7. Gli Stati membri dispongono che una decisione ai sensi del paragrafo 5 lasci impregiudicato il trasferimento di dati personali verso il paese terzo, il territorio o uno o più settori specifici all'interno del paese terzo, o verso l'organizzazione internazionale in questione, a norma degli articoli 37 e 38.

8. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* e sul suo sito web l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è più garantito un livello di protezione adeguato.

Articolo 37

Trasferimenti soggetti a garanzie adeguate

1. In mancanza di una decisione ai sensi dell'articolo 36, paragrafo 3, gli Stati membri dispongono che sia ammesso un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale se:

a) sono fornite garanzie adeguate per la protezione dei dati personali in uno strumento giuridicamente vincolante; oppure

b) il titolare 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. Il titolare del trattamento informa l'autorità di controllo in merito alle categorie di trasferimenti di cui al paragrafo 1, lettera b).

3. Qualora sia basato sul paragrafo 1, lettera b), un tale trasferimento deve essere documentato e, su richiesta, la documentazione deve essere messa a disposizione dell'autorità di controllo con l'indicazione della data e dell'ora del trasferimento, delle informazioni sull'autorità competente ricevente, della motivazione del trasferimento e dei dati personali trasferiti.

Articolo 38

Deroghe in specifiche situazioni

1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 36 o di garanzie adeguate ai sensi dell'articolo 37, gli Stati membri provvedono affinché un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale possano aver luogo soltanto a condizione che il trasferimento sia necessario:

a) per tutelare un interesse vitale dell'interessato o di un'altra persona;

b) per salvaguardare i legittimi interessi dell'interessato qualora lo preveda il diritto dello Stato membro che trasferisce i dati personali;

c) per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un paese terzo;

d) nei singoli casi, per le finalità di cui all'articolo 1, paragrafo 1; oppure

e) nel singolo caso, per accertare, esercitare o difendere un diritto in sede giudiziaria in relazione alle finalità di cui all'articolo 1, paragrafo 1.

2. I dati personali non sono trasferiti se l'autorità competente che opera il trasferimento determina che i diritti e le libertà fondamentali dell'interessato prevalgono sull'interesse pubblico al trasferimento di cui al paragrafo 1, lettere d) ed e).

3. Qualora sia basato sul paragrafo 1, un tale trasferimento deve essere documentato e, su richiesta, la documentazione deve essere messa a disposizione dell'autorità di controllo con l'indicazione della data e dell'ora del trasferimento, delle informazioni sull'autorità competente ricevente, della motivazione del trasferimento e dei dati personali trasferiti.

Articolo 39

Trasferimenti di dati personali a destinatari stabiliti in paesi terzi

1. In deroga all'articolo 35, paragrafo 1, lettera b), e fatti salvi eventuali accordi internazionali di cui al paragrafo 2 del presente articolo, il diritto dell'Unione o dello Stato membro può disporre che le autorità competenti di cui all'articolo 3, punto 7), lettera a), possano, in casi singoli e specifici, trasferire dati personali direttamente a destinatari stabiliti in paesi terzi soltanto se le altre disposizioni della presente direttiva sono rispettate e se sono soddisfatte tutte le seguenti condizioni:

a) il trasferimento è strettamente necessario per l'assolvimento di un compito dell'autorità competente che opera il trasferimento ai sensi del diritto dell'Unione o dello Stato membro per le finalità di cui all'articolo 1, paragrafo 1;

b) l'autorità competente che opera il trasferimento determina che i diritti e le libertà fondamentali dell'interessato non prevalgono sull'interesse pubblico che rende necessario il trasferimento nel caso in questione;

c) l'autorità competente che opera il trasferimento ritiene che il trasferimento a un'autorità competente per le finalità di cui all'articolo 1, paragrafo 1, nel paese terzo sia inefficace o inadatto, in particolare in quanto il trasferimento non può essere effettuato tempestivamente;

d) l'autorità competente ai fini di cui all'articolo 1, paragrafo 1, nel paese terzo è informata senza ingiustificato ritardo, a meno che ciò sia inefficace o inadatto;

e) l'autorità competente che opera il trasferimento informa il destinatario della finalità specifica o delle finalità specifiche per le quali i dati personali devono essere trattati da quest'ultimo soltanto a condizione che tale trattamento sia necessario.

2. Per accordo internazionale di cui al paragrafo 1 si intende qualsiasi accordo internazionale bilaterale o multilaterale in vigore tra gli Stati membri e paesi terzi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia.

3. L'autorità competente del trasferimento informa l'autorità di controllo in merito ai trasferimenti a norma del presente articolo.

4. Qualora sia basato sul paragrafo 1, un tale trasferimento è documentato.

Articolo 40

Cooperazione internazionale per la protezione dei dati personali

In relazione ai paesi terzi e alle organizzazioni internazionali, la Commissione e gli Stati membri adottano misure appropriate per:

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

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

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

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

CAPO VI

Autorità di controllo indipendenti

Sezione 1

Indipendenza

Articolo 41

Autorità di controllo

1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione della presente direttiva al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione («autorità di controllo»).

2. Ogni autorità di controllo contribuisce alla coerente applicazione della presente direttiva in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, a norma del capo VII.

3. Gli Stati membri possono disporre che un'autorità di controllo istituita ai sensi del regolamento (UE) 2016/679 sia l'autorità di controllo di cui alla presente direttiva e assolva i compiti dell'autorità di controllo da istituirsi ai sensi del paragrafo 1 del presente articolo.

4. Qualora in uno Stato membro siano istituite più autorità di controllo, tale Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato di cui all'articolo 51.

Articolo 42

Indipendenza

1. Ogni Stato membro dispone che ciascuna autorità di controllo agisca in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri previsti dalla presente direttiva.

2. Gli Stati membri dispongono che, nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dalla presente direttiva, il membro o i membri delle rispettive autorità di controllo non subiscano pressioni esterne, né dirette, né indirette, e non sollecitino né accettino istruzioni da alcuno.

3. I membri delle autorità di controllo degli Stati membri si astengono da qualunque azione incompatibile con le loro funzioni e per tutta la durata del mandato non possono esercitare alcuna altra attività incompatibile, remunerata o meno.

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

5. Ogni Stato membro provvede affinché ciascuna autorità di controllo selezioni e disponga di personale proprio, soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo in questione.

6. Ogni Stato membro garantisce che ciascuna autorità di controllo sia soggetta a un controllo finanziario che non ne pregiudichi l'indipendenza e disponga di bilanci annuali, separati e pubblici, che possono far parte del bilancio generale statale o nazionale.

Articolo 43

Condizioni generali per i membri dell'autorità di controllo

1. Gli Stati membri dispongono che ciascun membro delle rispettive autorità di controllo sia nominato attraverso una procedura trasparente:

— dal rispettivo parlamento;

— dal rispettivo governo;

— dal rispettivo capo di Stato; o

— da un organismo indipendente incaricato della nomina ai sensi del diritto dello Stato membro.

2. Ogni membro possiede le qualifiche, l'esperienza e le competenze, in particolare nel settore della protezione dei dati personali, richieste per l'esercizio delle sue funzioni e dei suoi poteri.

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

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

Articolo 44

Norme sull'istituzione dell'autorità di controllo

1. Ogni Stato membro prevede con legge tutte le condizioni seguenti:

a) l'istituzione di ciascuna autorità di controllo;

b) le qualifiche e le condizioni di idoneità richieste per essere nominato membro di ciascuna autorità di controllo;

c) le norme e le procedure per la nomina del membro o dei membri di ciascuna autorità di controllo;

d) la durata del mandato del membro o dei membri di ciascuna autorità di controllo non inferiore a quattro anni, salvo per le prime nomine dopo il 6 maggio 2016, alcune delle quali possono avere una durata inferiore qualora ciò sia necessario per tutelare l'indipendenza dell'autorità di controllo mediante una procedura di nomina scaglionata;

e) l'eventuale rinnovabilità e, in caso positivo, il numero di rinnovi del mandato del membro o dei membri di ciascuna autorità di controllo;

f) le condizioni che disciplinano gli obblighi del membro o dei membri e del personale di ciascuna autorità di controllo, i divieti relativi ad attività, professioni e benefici incompatibili con tali obblighi durante e dopo il mandato e le regole che disciplinano la cessazione del rapporto di lavoro.

2. Il membro o i membri e il personale di ogni autorità di controllo sono tenuti, in virtù del diritto dell'Unione o degli Stati membri, al segreto professionale in merito alle informazioni riservate cui hanno avuto accesso nell'esecuzione dei loro compiti o nell'esercizio dei loro poteri, sia durante che dopo il mandato. Per tutta la durata del loro mandato, tale obbligo del segreto professionale si applica in particolare alle segnalazioni da parte di persone fisiche di violazioni della presente direttiva.

Sezione 2

Competenza, compiti e poteri

Articolo 45

Competenza

1. Ogni Stato membro dispone che ciascuna autorità di controllo sia competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti, ai sensi della presente direttiva nel territorio del rispettivo Stato membro.

2. Ogni Stato membro dispone che ciascuna autorità di controllo non sia preposta a controllare i trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali. Gli Stati membri possono disporre che le rispettive autorità di controllo non siano competenti per il controllo dei trattamenti effettuati da altre autorità giurisdizionali indipendenti nell'esercizio delle loro funzioni giurisdizionali.

Articolo 46

Compiti

1. Ogni Stato membro dispone che sul proprio territorio ciascuna autorità di controllo:

a) sorvegli e assicuri l'applicazione delle disposizioni adottate a norma della presente direttiva e delle relative misure di esecuzione;

b) promuova la sensibilizzazione e favorisca la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento;

c) fornisca consulenza, a norma del diritto dello Stato membro, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;

d) promuova la consapevolezza dei titolari del trattamento e dei responsabili del trattamento degli obblighi imposti loro dalla presente direttiva;

e) su richiesta, fornisca informazioni all'interessato in merito all'esercizio dei propri diritti derivanti dalla presente direttiva e, se del caso, cooperi a tal fine con le autorità di controllo di altri Stati membri;

f) tratti i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 55, e svolga le indagini opportune sull'oggetto del reclamo e informi il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;

g) verifichi la liceità del trattamento ai sensi dell'articolo 17 e informi l'interessato entro un termine ragionevole dell'esito della verifica ai sensi del paragrafo 3 di tale articolo, o dei motivi per cui non è stata effettuata;

h) collabori, anche tramite scambi di informazioni, con le altre autorità di controllo e presti assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente della presente direttiva;

i) svolga indagini sull'applicazione della presente direttiva, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;

j) 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;

k) fornisca consulenza in merito ai trattamenti di cui all'articolo 28; e

l) contribuisca alle attività del comitato.

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

3. Ogni autorità di controllo svolge i propri compiti senza spese né per l'interessato né per il titolare della protezione dei dati.

4. Qualora una richiesta sia manifestamente infondata o eccessiva, in particolare in quanto ripetitiva, l'autorità di controllo può addebitare un contributo spese ragionevole basato sui propri costi amministrativi o può rifiutare di soddisfare la richiesta. Incombe all'autorità di controllo dimostrare che la richiesta è manifestamente infondata o eccessiva.

Articolo 47

Poteri

1. Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia poteri d'indagine effettivi. Tali poteri comprendono almeno il potere di ottenere, dal titolare del trattamento e dal responsabile del trattamento, l'accesso a tutti i dati personali oggetto del trattamento e a tutte le informazioni necessarie per l'adempimento dei suoi compiti.

2. Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia poteri correttivi effettivi, come ad esempio:

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

b) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni adottate a norma della presente direttiva, se del caso, in una determinata maniera ed entro un determinato termine, ordinando in particolare la rettifica o la cancellazione di dati personali o la limitazione del trattamento ai sensi dell'articolo 16;

c) imporre un limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento.

3. Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia poteri consultivi effettivi per fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 28, e per formulare, di propria iniziativa o su richiesta, pareri destinati al proprio parlamento nazionale e al proprio governo dello Stato membro, oppure, conformemente al proprio diritto nazionale, ad altri istituzioni e organismi nonché al pubblico su questioni riguardanti la protezione dei dati personali.

4. L'esercizio da parte di un'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie adeguate, inclusi il ricorso giurisdizionale effettivo e il giusto processo, previste dal diritto dell'Unione e dello Stato membro conformemente alla Carta.

5. Ogni Stato membro dispone per legge che ciascuna autorità di controllo abbia il potere di sottoporre all'attenzione di autorità giudiziarie violazioni delle disposizioni adottate a norma della presente direttiva e, se del caso, di intentare un'azione o di agire in sede giudiziale, per far rispettare le disposizioni adottate a norma della presente direttiva.

Articolo 48

Segnalazione di violazioni

Gli Stati membri dispongono che le autorità competenti pongano in essere meccanismi efficaci per incoraggiare la segnalazione riservata di violazioni della presente direttiva.

Articolo 49

Relazioni di attività

Ogni autorità di controllo elabora una relazione annuale sulla propria attività, in cui può figurare un elenco delle tipologie di violazioni notificate e di sanzioni imposte. Tali relazioni sono trasmesse al parlamento nazionale, al governo e alle altre autorità designate dal diritto dello Stato membro. Esse sono messe a disposizione del pubblico, della Commissione e del comitato.

CAPO VII

Cooperazione

Articolo 50

Assistenza reciproca

1. Ogni Stato membro dispone che le rispettive autorità di controllo si scambino le informazioni utili e si prestino assistenza reciproca al fine di attuare e applicare la presente direttiva in maniera coerente, e mettano in atto misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di effettuare consultazioni, ispezioni e indagini.

2. Ogni Stato membro dispone che ciascuna autorità di controllo adotti tutte le misure opportune necessarie per dare seguito a una richiesta di un'altra autorità di controllo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta. Tali misure possono consistere, in particolare, nella trasmissione di informazioni utili sullo svolgimento di un'indagine.

3. Le richieste di assistenza contengono tutte le informazioni necessarie, compresi lo scopo e i motivi della richiesta. Le informazioni scambiate sono utilizzate ai soli fini per cui sono state richieste.

4. L'autorità di controllo cui è presentata la richiesta non deve rifiutare di darvi seguito, salvo che:

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

b) l'intervento richiesto violerebbe la presente direttiva o il diritto dell'Unione o dello Stato membro cui è soggetta l'autorità di controllo che riceve la richiesta.

5. L'autorità di controllo che riceve la richiesta informa l'autorità di controllo richiedente dell'esito o, se del caso, dei progressi delle misure adottate per rispondere alla richiesta. L'autorità di controllo che riceve la richiesta fornisce le motivazioni del rifiuto di darvi seguito ai sensi del paragrafo 4.

6. Di norma, le autorità di controllo che ricevono le richieste forniscono, con mezzi elettronici, usando un modulo standard, le informazioni richieste da altre autorità di controllo.

7. Le autorità di controllo che ricevono le richieste non addebitano un contributo spese per le misure da loro adottate a seguito di una richiesta di assistenza reciproca. Le autorità di controllo possono concordare di concedersi gli indennizzi per spese specifiche risultanti dalla prestazione di assistenza reciproca in circostanze eccezionali.

8. La Commissione può, mediante atti di esecuzione, specificare il formato e le procedure per l'assistenza reciproca di cui al presente articolo e le modalità per lo scambio di informazioni con mezzi elettronici tra autorità di controllo e tra le autorità di controllo e il comitato. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 58, paragrafo 2.

Articolo 51

Compiti del comitato

1. Il comitato istituito dal regolamento (UE) 2016/679 adempie tutti i seguenti compiti in relazione ai trattamenti rientranti nell'ambito 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, su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione della presente direttiva e pubblica linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente della presente direttiva;

c) elabora linee guida per le autorità di controllo concernenti l'applicazione delle misure di cui all'articolo 47, paragrafi 1 e 3;

d) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera b) del presente comma, per accertare la violazione di dati personali e determinare l'ingiustificato ritardo di cui all'articolo 30, paragrafi 1 e 2, e le circostanze particolari in cui il titolare del trattamento o il responsabile del trattamento è tenuto a notificare la violazione dei dati personali;

e) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera b) del presente comma relative alle circostanze in cui una violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche di cui all'articolo 31, paragrafo 1;

f) valuta l'applicazione pratica delle linee guida, raccomandazioni e migliori prassi di cui alle lettere b) e c);

g) trasmette alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo o in un'organizzazione internazionale, come pure per valutare se tale paese terzo, territorio, settore specifico o organizzazione internazionale non garantiscano più un livello adeguato di protezione;

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

i) 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 con organizzazioni internazionali;

j) promuove lo scambio di conoscenze e documentazione sul diritto e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo.

Con riguardo alla lettera g), primo comma, la Commissione fornisce al comitato tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, con il territorio o il settore specifico all'interno di tale paese terzo o con l'organizzazione internazionale.

2. Qualora chieda consulenza al comitato, la Commissione può indicare un termine, tenuto conto dell'urgenza della questione.

3. Il comitato trasmette pareri, linee guida, raccomandazioni e migliori prassi alla Commissione e al comitato di cui all'articolo 58, paragrafo 1, e li pubblica.

4. La Commissione informa il comitato del seguito dato ai suoi pareri, linee guida, raccomandazioni e migliori prassi.

CAPO VIII

Ricorsi, responsabilità e sanzioni

Articolo 52

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 dati personali che lo riguardano violi le disposizioni adottate a norma della presente direttiva abbia il diritto di proporre reclamo a un'unica autorità di controllo.

2. Gli Stati membri dispongono che l'autorità di controllo a cui è stato proposto il reclamo lo trasmetta senza ingiustificato ritardo all'autorità di controllo competente qualora il reclamo non sia proposto a quest'ultima ai sensi dell'articolo 45, paragrafo 1,. L'interessato è informato della trasmissione.

3. Gli Stati membri dispongono che l'autorità di controllo a cui sia stato proposto il reclamo fornisca ulteriore assistenza su richiesta dell'interessato.

4. L'autorità di controllo competente informa l'interessato dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 53.

Articolo 53

Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, gli Stati membri prevedono il diritto di una persona fisica o giuridica a un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda.

2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi dell'articolo 45, paragrafo 1, non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 52.

3. Gli Stati membri dispongono che le azioni nei confronti dell'autorità di controllo siano promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

Articolo 54

Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento

Gli Stati membri dispongono che, fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 52, l'interessato abbia il diritto a un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode ai sensi delle disposizioni adottate a norma della presente direttiva siano stati violati a seguito del trattamento dei propri dati personali in violazione di tali disposizioni.

Articolo 55

Rappresentanza degli interessati

Gli Stati membri dispongono che, conformemente al diritto processuale dello Stato membro, l'interessato abbia il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto dello Stato membro, abbiano obiettivi statutari che siano di pubblico interesse e siano attivi nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 52, 53 e 54.

Articolo 56

Diritto al risarcimento

Gli Stati membri dispongono che chiunque subisca un danno materiale o immateriale cagionato da un trattamento illecito o da qualsiasi altro atto che violi le disposizioni adottate a norma della presente direttiva abbia il diritto di ottenere il risarcimento del danno dal titolare del trattamento o da altra autorità competente in base al diritto dello Stato membro.

Articolo 57

Sanzioni

Gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazione delle disposizioni adottate a norma della presente direttiva e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive.

CAPO IX

Atti di esecuzione

Articolo 58

Procedura di comitato

1. La Commissione è assistita dal comitato istituito dall'articolo 93 del regolamento (UE) 2016/679. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

3. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 8 del regolamento (UE) n. 182/2011 in combinato disposto con il suo articolo 5.

CAPO X

Disposizioni finali

Articolo 59

Abrogazione della decisione quadro 2008/977/GAI

1. La decisione quadro 2008/977/GAI è abrogata a decorrere dal 6 maggio 2018.

2. I riferimenti alla decisione abrogata di cui al paragrafo 1 si intendono fatti alla presente direttiva.

Articolo 60

Atti giuridici dell'Unione già in vigore

Rimangono impregiudicate le disposizioni specifiche per la protezione dei dati personali contenute in atti giuridici dell'Unione che sono entrati in vigore il o anteriormente al 6 maggio 2016 nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia, che disciplinano il trattamento tra Stati membri e l'accesso delle autorità nazionali designate ai sistemi d'informazione istituiti ai sensi dei trattati, nell'ambito di applicazione della presente direttiva.

Articolo 61

Rapporto con gli accordi internazionali precedentemente conclusi nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia

Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali relativi al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali che sono stati conclusi dagli Stati membri anteriormente al 6 maggio 2016 e che sono conformi al diritto dell'Unione applicabile anteriormente a tale data.

Articolo 62

Relazioni della Commissione

1. Entro il 6 maggio 2022 e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame della presente direttiva. Tale relazione è pubblicata.

2. Nel contesto delle valutazioni e dei riesami di cui al paragrafo 1 la Commissione esamina, in particolare, l'applicazione e il funzionamento del capo V sul trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, con particolare riguardo alle decisioni adottate ai sensi dell'articolo 36, paragrafo 3, e dell'articolo 39.

3. Ai fini dei paragrafi 1 e 2 la Commissione può richiedere informazioni agli Stati membri e alle autorità di controllo.

4. Nello svolgere le valutazioni e i riesami di cui ai paragrafi 1 e 2, la Commissione tiene conto delle posizioni e delle conclusioni del Parlamento europeo, del Consiglio, nonché di altri organismi o fonti pertinenti.

5. Se del caso, la Commissione presenta opportune proposte di modifica della presente direttiva tenuto conto, in particolare, degli sviluppi delle tecnologie dell'informazione e dei progressi della società dell'informazione.

6. Entro il 6 maggio 2019, la Commissione riesamina gli altri atti giuridici adottati dall'Unione che disciplinano il trattamento da parte delle autorità competenti per le finalità di cui all'articolo 1, paragrafo 1, in particolare quelli di cui all'articolo 60, 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.

Articolo 63

Recepimento

1. Gli Stati membri adottano e pubblicano, entro il 6 maggio 2018, le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva. Essi comunicano immediatamente alla Commissione il testo di tali disposizioni. Essi applicano tali disposizioni a decorrere dal 6 maggio 2018.

Le disposizioni adottate dagli Stati membri contengono un riferimento alla presente direttiva o sono corredate di tale riferimento all'atto della pubblicazione ufficiale. Le modalità del riferimento sono stabilite dagli Stati membri.

2. In deroga al paragrafo 1, uno Stato membro può disporre che, in via eccezionale, qualora ciò comporti sforzi sproporzionati, i sistemi di trattamento automatizzato istituiti anteriormente al 6 maggio 2016 siano resi conformi all'articolo 25, paragrafo 1, entro il 6 maggio 2023.

3. In deroga ai paragrafi 1 e 2 del presente articolo, uno Stato membro può, in circostanze eccezionali, rendere un sistema di trattamento automatizzato di cui al paragrafo 2 del presente articolo conforme all'articolo 25, paragrafo 1, entro un termine specificato dopo il termine di cui al paragrafo 2 del presente articolo, qualora ciò causi altrimenti gravi difficoltà per il funzionamento di tale particolare sistema di trattamento automatizzato. Lo Stato membro in questione comunica alla Commissione i motivi di tali gravi difficoltà e i motivi del termine specificato entro il quale rende tale particolare sistema di trattamento automatizzato conforme all'articolo 25, paragrafo 1. Il termine specificato non supera in ogni caso il 6 maggio 2026.

4. Gli Stati membri comunicano alla Commissione il testo delle disposizioni fondamentali di diritto interno che adottano nel settore disciplinato dalla presente direttiva.

Articolo 64

Entrata in vigore

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

Articolo 65

Destinatari

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, il 27 aprile 2016

Per il Parlamento europeo	*Per il Consiglio*
Il presidente	*Il presidente*
M. SCHULZ	J.A. HENNIS-PLASSCHAERT