

Fra GDPR europeo e FOIA italiano: nuovi regolamenti sulla protezione dei dati ed il diritto all'accesso

ANTONIO MONTEDURO

Senior Archivist, Central European Initiative – Executive Secretariat, via Genova 9, 34121 - I - Trieste
e-mail: monteduro@cei.int

Between European GDPR and Italian FOIA: New Regulations on Data Protection and Right to Access

ABSTRACT

The paper gives a brief account about the adoption of the new regulations on data protection and right to access introduced by the European Union and the Italian Republic. The texts of the two regulations are given, and a brief list about the present global situation is also given.

Fra GDPR europeo e FOIA italiano: nuovi regolamenti sulla protezione dei dati ed il diritto all'accesso

SINTESI

L'articolo dà brevemente conto dell'adozione dei nuovi regolamenti sulla protezione dei dati ed il diritto all'accesso introdotti dall'Unione Europea e dalla Repubblica Italiana. Vengono inoltre forniti i testi dei due decreti nonché un succinto elenco relativo alla situazione attualmente esistente a livello globale.

Med Evropsko BDPR in italijansko FOIA: Novi predpisi o varstvu osebnih podatkov in pravico do dostopa

IZVLEČEK

Prispevek podaja kratek povzetek o sprejetju novih predpisov o varstvu podatkov in pravico do dostopa, uvedenih s strani Evropske unije in Republike Italije. Predstavljeni sta besedili obeh uredb ter kratek povzetek globalnih razmer.

Esistono, nel mondo digitale, alcune specifiche difficoltà di gestione del dato conservato, legate, sostanzialmente, allo specifico informatico, ossia le difficoltà di conservazione di un elemento di per sé instabile e del cui supporto scrittorio sperimentiamo quotidianamente la rapida obsolescenza.

Chi di noi, infatti, è oggi in grado di leggere sul proprio pc, o peggio ancora sul proprio tablet, file risalenti solo ad una decina di anni fa, salvati (si pensava all'epoca) sui vecchi, cari, floppy disk, o conservati in un formato che i software contemporanei non sono più in grado di riprodurre? Certo, perdere la possibilità di leggere e condividere la scannerizzazione effettuata qualche anno fa di una pergamena trecentesca è senza dubbio un peccato; ma se, invece, ad essere diventato illeggibile è una parte del nostro percorso contributivo? Oppure alcune sezioni della nostra cartella clinica?

Un'altra delle problematiche più attuali e complesse legate alla conservazione del dato (e non solo digitale) è quella relativa al suo successivo utilizzo da parte dell'utenza.

Chi, e con quali modalità, ha il diritto di accedere ai dati, e di fruirne?

Il dibattito in proposito è stato da sempre molto sentito, sia da parte degli addetti ai lavori che da parte di coloro i quali quei dati debbono utilizzare per i motivi più svariati, siano essi di carattere giuridico, di ricerca, di interesse personale.

È questa una tematica che da sempre intesse di sé il mondo dell'archivistica, e che non a caso finisce poi con il coincidere con il concetto stesso di democrazia, della quale gli archivi sono strumento potente e quasi privilegiato.

Dare o non dare accesso ai dati, o darlo secondo modalità e tempistiche da studiare ed applicare quasi caso per caso, può risultare, anche, un indicatore abbastanza preciso del grado di partecipazione di una società civile alla vita del proprio paese, si pensi soltanto a come, nelle nazioni meno inclini ad una condivisione democratica del potere, il controllo dell'accesso ai dati possa voler dire indirizzare in un senso o nell'altro il consenso popolare, a seconda delle esigenze di coloro i quali di quelle nazioni sono a capo.

Non è quindi un caso che nel corso degli ultimi anni nuovi strumenti di gestione e di controllo dell'accessibilità ai dati siano stati elaborati all'interno del corpus legislativo dei vari paesi (in Appendice 3 un elenco di massima della situazione nelle varie nazioni).

Proprio nella prima metà di quest'anno, in particolare, sono stati emessi due strumenti legislativi che a queste problematiche si riferiscono: il primo, adottato nel mese di aprile prima dal Consiglio Europeo e poi dal Parlamento Europeo, è il Regolamento generale sulla protezione dei dati (General Data Protection Regulation – GDPR); l'altro, pubblicato in Gazzetta Ufficiale nel giugno scorso, è il decreto legislativo 97/2016 comunemente ormai noto come FOIA (Freedom of Information Act) italiano, decreto applicativo collegato alla più generale riforma della pubblica amministrazione.

Nel caso del GDPR europeo (che andrà a rimpiazzare l'ormai più che ventennale direttiva 95/46/EC in materia, adottata appunto nel 1995 dalla Commissione Europea) si tratta di uno strumento che ha come scopo principale quello di rafforzare ed unificare i diritti/doveri relativi alla protezione dei dati a livello individuale dei cittadini dell'Unione Europea. Obiettivo primario del legislatore è quello di ridare ai cittadini europei il controllo in prima persona sui propri dati personali, e di semplificare le procedure relative. Il nuovo GDPR, inoltre, rende anche gli enti extraeuropei soggetti alla legislazione europea in questo campo.

Per ciò che riguarda il FOIA italiano, pur essendo esso principalmente dedicato alla lotta alla corruzione ed alla riorganizzazione delle amministrazioni pubbliche (D.L.gs 25 maggio 2016, n. 97, "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190, e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche"), contiene nondimeno importanti novità riguardanti proprio l'accessibilità ai dati: una fra tutte, la non necessità di motivare la richiesta di accesso a dati in possesso delle pubbliche amministrazioni e la contestuale non possibilità di ricevere un rifiuto immotivato a tale richiesta.

Senza entrare nel dettaglio giurisprudenziale (si rimanda ad alcuni articoli in particolare dei testi legislativi in Appendice 1 e 2), va comunque sottolineato come la tendenza generale sia quella di una sempre maggior liberalizzazione dell'accessibilità pur nel pieno rispetto della privacy personale, a sempre maggior tutela della democraticità cui sopra si accennava.

APPENDICE 1 – General Data Protection Regulation

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,
deliberando secondo la procedura legislativa ordinaria,
considerando quanto segue:

- (1) La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
- (2) 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 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.
- (6) La decisione quadro 2008/977/GAI del Consiglio 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 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 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 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.
- (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; 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 e nella decisione 2007/533/GAI del Consiglio.
- (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, 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 arbitrarità.
- (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, decifrazione 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 di 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 i 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 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.
- (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.
- (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 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 o dell'articolo 23 della convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea. 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.
- (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.
- (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.
- (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.
- (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.
- (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.
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 provarlo.

... omissis...

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.

... omissis...

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.

... omissis...

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 pubblici 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.

... omissis...

Testo completo: <http://ec.europa.eu/justice/data-protection/>

Decreto legislativo 25 maggio 2016, n. 97

Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33, ai sensi dell'articolo 7 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche

(G.U. 8 giugno 2016, n. 132)

Capo I - Modifiche al decreto legislativo 14 marzo 2013, n. 33**Art. 1. Modifiche al titolo del decreto legislativo n. 33 del 2013**

1. Il titolo del decreto legislativo 14 marzo 2013, n. 33, è sostituito dal seguente: «Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni».

Art. 2. Modifiche all'articolo 1 del decreto legislativo n. 33 del 2013

1. All'articolo 1, comma 1, del decreto legislativo n. 33 del 2013, le parole «delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di», sono sostituite dalle seguenti: «dei dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di tutelare i diritti dei cittadini, promuovere la partecipazione degli interessati all'attività amministrativa».

Art. 3. Modifiche all'articolo 2 del decreto legislativo n. 33 del 2013 e inserimento dell'articolo 2-bis

1. Il comma 1 dell'articolo 2 del decreto legislativo 14 marzo 2013, n. 33, è sostituito dal seguente: «1. Le disposizioni del presente decreto disciplinano la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni e dagli altri soggetti di cui all'articolo 2-bis, garantita, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti, tramite l'accesso civico e tramite la pubblicazione di documenti, informazioni e dati concernenti l'organizzazione e l'attività delle pubbliche amministrazioni e le modalità per la loro realizzazione».

2. Dopo l'articolo 2 è inserito il seguente:

«Art. 2-bis. Ambito soggettivo di applicazione»

1. Ai fini del presente decreto, per “pubbliche amministrazioni” si intendono tutte le amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, ivi comprese le autorità portuali, nonché le autorità amministrative indipendenti di garanzia, vigilanza e regolazione.

2. La medesima disciplina prevista per le pubbliche amministrazioni di cui al comma 1 si applica anche, in quanto compatibile:

- a) agli enti pubblici economici e agli ordini professionali;
- b) alle società in controllo pubblico come definite dal decreto legislativo emanato in attuazione dell'articolo 18 della legge 7 agosto 2015, n. 124. Sono escluse le società quotate come definite dallo stesso decreto legislativo emanato in attuazione dell'articolo 18 della legge 7 agosto 2015, n. 124;
- c) alle associazioni, alle fondazioni e agli enti di diritto privato comunque denominati, anche privi di personalità giuridica, con bilancio superiore a cinquecentomila euro, la cui attività sia finanziata in modo maggioritario per almeno due esercizi finanziari consecutivi nell'ultimo triennio da pubbliche amministrazioni e in cui la totalità dei titolari o dei componenti dell'organo d'amministrazione o di indirizzo sia designata da pubbliche amministrazioni.

3. La medesima disciplina prevista per le pubbliche amministrazioni di cui al comma 1 si applica, in quanto compatibile, limitatamente ai dati e ai documenti inerenti all'attività di pubblico interesse disciplinata dal diritto nazionale o dell'Unione europea, alle società in partecipazione pubblica come definite dal decreto legislativo emanato in attuazione dell'articolo 18 della legge 7 agosto 2015, n. 124, e alle associazioni, alle fondazioni e

agli enti di diritto privato, anche privi di personalità giuridica, con bilancio superiore a cinquecentomila euro, che esercitano funzioni amministrative, attività di produzione di beni e servizi a favore delle amministrazioni pubbliche o di gestione di servizi pubblici».

Art. 4. Modifiche all'articolo 3 del decreto legislativo n. 33 del 2013

1. All'articolo 3 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole «i dati oggetto» sono inserite le seguenti: «di accesso civico, ivi compresi quelli oggetto»;

b) dopo il comma 1 sono inseriti i seguenti:

«1-bis. L'Autorità nazionale anticorruzione, sentito il Garante per la protezione dei dati personali nel caso in cui siano coinvolti dati personali, con propria delibera adottata, previa consultazione pubblica, in conformità con i principi di proporzionalità e di semplificazione, e all'esclusivo fine di ridurre gli oneri gravanti sui soggetti di cui all'articolo 2-bis, può identificare i dati, le informazioni e i documenti oggetto di pubblicazione obbligatoria ai sensi della disciplina vigente per i quali la pubblicazione in forma integrale è sostituita con quella di informazioni riassuntive, elaborate per aggregazione. In questi casi, l'accesso ai dati e ai documenti nella loro integrità è disciplinato dall'articolo 5.

1-ter. L'Autorità nazionale anticorruzione può, con il Piano nazionale anticorruzione, nel rispetto delle disposizioni del presente decreto, precisare gli obblighi di pubblicazione e le relative modalità di attuazione, in relazione alla natura dei soggetti, alla loro dimensione organizzativa e alle attività svolte, prevedendo in particolare modalità semplificate per i comuni con popolazione inferiore a 15.000 abitanti, per gli ordini e collegi professionali».

Art. 5. Inserimento dell'articolo 4-bis e del capo I-bis

1. Dopo l'articolo 4 del decreto legislativo n. 33 del 2013 è inserito il seguente:

«Art. 4-bis. Trasparenza nell'utilizzo delle risorse pubbliche

1. L'Agenzia per l'Italia digitale, d'intesa con il Ministero dell'economia e delle finanze, al fine di promuovere l'accesso e migliorare la comprensione dei dati relativi all'utilizzo delle risorse pubbliche, gestisce il sito internet denominato "Soldi pubblici" che consente l'accesso ai dati dei pagamenti delle pubbliche amministrazioni e ne permette la consultazione in relazione alla tipologia di spesa sostenuta e alle amministrazioni che l'hanno effettuata, nonché all'ambito temporale di riferimento.

2. Ciascuna amministrazione pubblica sul proprio sito istituzionale, in una parte chiaramente identificabile della sezione "Amministrazione trasparente", i dati sui propri pagamenti e ne permette la consultazione in relazione alla tipologia di spesa sostenuta, all'ambito temporale di riferimento e ai beneficiari.

3. Per le spese in materia di personale si applica quanto previsto dagli articoli da 15 a 20.

4. Dalle disposizioni di cui ai commi 1 e 2 non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni interessate provvedono ai relativi adempimenti nell'ambito delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente».

2. Dopo l'articolo 4-bis del decreto legislativo n. 33 del 2013, come inserito dal comma 1, è inserito il seguente Capo: «CAPO I-BIS - DIRITTO DI ACCESSO A DATI E DOCUMENTI».

Art. 6. Modifiche all'articolo 5 del decreto legislativo n. 33 del 2013 e inserimento degli articoli 5-bis e 5-ter e del capo I-ter

1. L'articolo 5 del decreto legislativo n. 33 del 2013 è sostituito dal seguente:

«Art. 5. Accesso civico a dati e documenti

1. L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti,

informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione.

2. Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, chiunque ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del presente decreto, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis.

3. L'esercizio del diritto di cui ai commi 1 e 2 non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente. L'istanza di accesso civico identifica i dati, le informazioni o i documenti richiesti e non richiede motivazione. L'istanza può essere trasmessa per via telematica secondo le modalità previste dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ed è presentata alternativamente ad uno dei seguenti uffici:

- a) all'ufficio che detiene i dati, le informazioni o i documenti;
- b) all'Ufficio relazioni con il pubblico;
- c) ad altro ufficio indicato dall'amministrazione nella sezione "Amministrazione trasparente" del sito istituzionale;
- d) al responsabile della prevenzione della corruzione e della trasparenza, ove l'istanza abbia a oggetto dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del presente decreto.

4. Il rilascio di dati o documenti in formato elettronico o cartaceo è gratuito, salvo il rimborso del costo effettivamente sostenuto e documentato dall'amministrazione per la riproduzione su supporti materiali.

5. Fatti salvi i casi di pubblicazione obbligatoria, l'amministrazione cui è indirizzata la richiesta di accesso, se individua soggetti controinteressati, ai sensi dell'articolo 5-bis, comma 2, è tenuta a dare comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica per coloro che abbiano consentito tale forma di comunicazione. Entro dieci giorni dalla ricezione della comunicazione, i controinteressati possono presentare una motivata opposizione, anche per via telematica, alla richiesta di accesso. A decorrere dalla comunicazione ai controinteressati, il termine di cui al comma 6 è sospeso fino all'eventuale opposizione dei controinteressati. Decorso tale termine, la pubblica amministrazione provvede sulla richiesta, accertata la ricezione della comunicazione.

6. Il procedimento di accesso civico deve concludersi con provvedimento espresso e motivato nel termine di trenta giorni dalla presentazione dell'istanza con la comunicazione al richiedente e agli eventuali controinteressati. In caso di accoglimento, l'amministrazione provvede a trasmettere tempestivamente al richiedente i dati o i documenti richiesti, ovvero, nel caso in cui l'istanza riguardi dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del presente decreto, a pubblicare sul sito i dati, le informazioni o i documenti richiesti e a comunicare al richiedente l'avvenuta pubblicazione dello stesso, indicandogli il relativo collegamento ipertestuale. In caso di accoglimento della richiesta di accesso civico nonostante l'opposizione del controinteressato, salvi i casi di comprovata indifferibilità, l'amministrazione ne dà comunicazione al controinteressato e provvede a trasmettere al richiedente i dati o i documenti richiesti non prima di quindici giorni dalla ricezione della stessa comunicazione da parte del controinteressato. Il rifiuto, il differimento e la limitazione dell'accesso devono essere motivati con riferimento ai casi e ai limiti stabiliti dall'articolo 5-bis. Il responsabile della prevenzione della corruzione e della trasparenza può chiedere agli uffici della relativa amministrazione informazioni sull'esito delle istanze.

7. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato al comma 6, il richiedente può presentare richiesta di riesame al responsabile della prevenzione della corruzione e della trasparenza, di cui all'articolo 43, che decide con provvedimento motivato, entro il termine di venti giorni. Se l'accesso è stato negato o differito a tutela degli interessi di cui all'articolo 5-bis, comma 2, lettera a), il suddetto responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del responsabile è sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni. Avverso la decisione dell'amministrazione competente o, in caso di richiesta di riesame, avverso quella del responsabile della prevenzione della corruzione e della trasparenza, il richiedente può proporre ricorso al Tribunale amministrativo regionale ai sensi dell'articolo 116 del Codice del processo amministrativo di cui al decreto legislativo 2 luglio 2010, n. 104.

8. Qualora si tratti di atti delle amministrazioni delle regioni o degli enti locali, il richiedente può altresì presentare

ricorso al difensore civico competente per ambito territoriale, ove costituito. Qualora tale organo non sia stato istituito, la competenza è attribuita al difensore civico competente per l'ambito territoriale immediatamente superiore. Il ricorso va altresì notificato all'amministrazione interessata. Il difensore civico si pronuncia entro trenta giorni dalla presentazione del ricorso. Se il difensore civico ritiene illegittimo il diniego o il differimento, ne informa il richiedente e lo comunica all'amministrazione competente. Se questa non conferma il diniego o il differimento entro trenta giorni dal ricevimento della comunicazione del difensore civico, l'accesso è consentito. Qualora il richiedente l'accesso si sia rivolto al difensore civico, il termine di cui all'articolo 116 del Codice del processo amministrativo decorre dalla data di ricevimento, da parte del richiedente, dell'esito della sua istanza al difensore civico. Se l'accesso è stato negato o differito a tutela degli interessi di cui all'articolo 5-bis, comma 2, lettera a), il difensore civico provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per la pronuncia del difensore è sospeso, fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti dieci giorni.

9. Nei casi di accoglimento della richiesta di accesso, il controinteressato può presentare richiesta di riesame ai sensi del comma 7 e presentare ricorso al difensore civico ai sensi del comma 8.

10. Nel caso in cui la richiesta di accesso civico riguardi dati, informazioni o documenti oggetto di pubblicazione obbligatoria ai sensi del presente decreto, il responsabile della prevenzione della corruzione e della trasparenza ha l'obbligo di effettuare la segnalazione di cui all'articolo 43, comma 5.

11. Restano fermi gli obblighi di pubblicazione previsti dal Capo II, nonché le diverse forme di accesso degli interessati previste dal Capo V della legge 7 agosto 1990, n. 241».

2. Dopo l'articolo 5 sono inseriti i seguenti:

«Art. 5-bis. Esclusioni e limiti all'accesso civico

1. L'accesso civico di cui all'articolo 5, comma 2, è rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno degli interessi pubblici inerenti a:

- a) la sicurezza pubblica e l'ordine pubblico;
- b) la sicurezza nazionale;
- c) la difesa e le questioni militari;
- d) le relazioni internazionali;
- e) la politica e la stabilità finanziaria ed economica dello Stato;
- f) la conduzione di indagini sui reati e il loro perseguimento;
- g) il regolare svolgimento di attività ispettive.

2. L'accesso di cui all'articolo 5, comma 2, è altresì rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla tutela di uno dei seguenti interessi privati:

- a) la protezione dei dati personali, in conformità con la disciplina legislativa in materia;
- b) la libertà e la segretezza della corrispondenza;
- c) gli interessi economici e commerciali di una persona fisica o giuridica, ivi compresi la proprietà intellettuale, il diritto d'autore e i segreti commerciali.

3. Il diritto di cui all'articolo 5, comma 2, è escluso nei casi di segreto di Stato e negli altri casi di divieti di accesso o divulgazione previsti dalla legge, ivi compresi i casi in cui l'accesso è subordinato dalla disciplina vigente al rispetto di specifiche condizioni, modalità o limiti, inclusi quelli di cui all'articolo 24, comma 1, della legge n. 241 del 1990.

4. Restano fermi gli obblighi di pubblicazione previsti dalla normativa vigente. Se i limiti di cui ai commi 1 e 2 riguardano soltanto alcuni dati o alcune parti del documento richiesto, deve essere consentito l'accesso agli altri dati o alle altre parti.

5. I limiti di cui ai commi 1 e 2 si applicano unicamente per il periodo nel quale la protezione è giustificata in relazione alla natura del dato. L'accesso civico non può essere negato ove, per la tutela degli interessi di cui ai commi 1 e 2, sia sufficiente fare ricorso al potere di differimento.

6. Ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui al presente articolo, l'Autorità nazionale anticorruzione, d'intesa con il Garante per la protezione dei dati personali e sentita la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, adotta linee guida recanti indicazioni

operative.

Art. 5-ter. Accesso per fini scientifici ai dati elementari raccolti per finalità statistiche

1. Gli enti e uffici del Sistema statistico nazionale ai sensi del decreto legislativo 6 settembre 1989, n. 322, di seguito Sistan, possono consentire l'accesso per fini scientifici ai dati elementari, privi di ogni riferimento che permetta l'identificazione diretta delle unità statistiche, raccolti nell'ambito di trattamenti statistici di cui i medesimi soggetti siano titolari, a condizione che:

a) l'accesso sia richiesto da ricercatori appartenenti a università, enti di ricerca e istituzioni pubbliche o private o loro strutture di ricerca, inseriti nell'elenco redatto dall'autorità statistica dell'Unione europea (Eurostat) o che risultino in possesso dei requisiti stabiliti ai sensi del comma 3, lettera a), a seguito di valutazione effettuata dal medesimo soggetto del Sistan che concede l'accesso e approvata dal Comitato di cui al medesimo comma 3;

b) sia sottoscritto, da parte di un soggetto abilitato a rappresentare l'ente richiedente, un impegno di riservatezza specificante le condizioni di utilizzo dei dati, gli obblighi dei ricercatori, i provvedimenti previsti in caso di violazione degli impegni assunti, nonché le misure adottate per tutelare la riservatezza dei dati;

c) sia presentata una proposta di ricerca e la stessa sia ritenuta adeguata, sulla base dei criteri di cui al comma 3, lettera b), dal medesimo soggetto del Sistan che concede l'accesso. Il progetto deve specificare lo scopo della ricerca, il motivo per il quale tale scopo non può essere conseguito senza l'utilizzo di dati elementari, i ricercatori che hanno accesso ai dati, i dati richiesti, i metodi di ricerca e i risultati che si intendono diffondere. Alla proposta di ricerca sono allegate dichiarazioni di riservatezza sottoscritte singolarmente dai ricercatori che avranno accesso ai dati. È fatto divieto di effettuare trattamenti diversi da quelli previsti nel progetto di ricerca, conservare i dati elementari oltre i termini di durata del progetto, comunicare i dati a terzi e diffonderli, pena l'applicazione della sanzione di cui all'articolo 162, comma 2-bis, del decreto legislativo 30 giugno 2003, n. 196.

2. I dati elementari di cui al comma 1, tenuto conto dei tipi di dati nonché dei rischi e delle conseguenze di una loro illecita divulgazione, sono messi a disposizione dei ricercatori sotto forma di file a cui sono stati applicati metodi di controllo al fine di non permettere l'identificazione dell'unità statistica. In caso di motivata richiesta, da cui emerga la necessità ai fini della ricerca e l'impossibilità di soluzioni alternative, sono messi a disposizione file a cui non sono stati applicati tali metodi, purché l'utilizzo di questi ultimi avvenga all'interno di laboratori costituiti dal titolare dei trattamenti statistici cui afferiscono i dati, accessibili anche da remoto tramite laboratori organizzati e gestiti da soggetto ritenuto idoneo e a condizione che il rilascio dei risultati delle elaborazioni sia autorizzato dal responsabile del laboratorio stesso, che i risultati della ricerca non permettano il collegamento con le unità statistiche, nel rispetto delle norme in materia di segreto statistico e di protezione dei dati personali, o nell'ambito di progetti congiunti finalizzati anche al perseguimento di compiti istituzionali del titolare del trattamento statistico cui afferiscono i dati, sulla base di appositi protocolli di ricerca sottoscritti dai ricercatori che partecipano al progetto, nei quali siano richiamate le norme in materia di segreto statistico e di protezione dei dati personali.

3. Sentito il Garante per la protezione dei dati personali, il Comitato di indirizzo e coordinamento dell'informazione statistica (Comstat), con atto da emanarsi ai sensi dell'articolo 3, comma 6, del decreto del Presidente della Repubblica 7 settembre 2010, n. 166, avvalendosi del supporto dell'Istat, adotta le linee guida per l'attuazione della disciplina di cui al presente articolo. In particolare, il Comstat stabilisce:

a) i criteri per il riconoscimento degli enti di cui al comma 1, lettera a), avuto riguardo agli scopi istituzionali perseguiti, all'attività svolta e all'organizzazione interna in relazione all'attività di ricerca, nonché alle misure adottate per garantire la sicurezza dei dati;

b) i criteri di ammissibilità dei progetti di ricerca avuto riguardo allo scopo della ricerca, alla necessità di disporre dei dati richiesti, ai risultati e benefici attesi e ai metodi impiegati per la loro analisi e diffusione;

c) le modalità di organizzazione e funzionamento dei laboratori fisici e virtuali di cui al comma 2;

d) i criteri per l'accreditamento dei gestori dei laboratori virtuali, avuto riguardo agli scopi istituzionali, all'adeguatezza della struttura organizzativa e alle misure adottate per la gestione e la sicurezza dei dati;

e) le conseguenze di eventuali violazioni degli impegni assunti dall'ente di ricerca e dai singoli ricercatori.

4. Nei siti istituzionali del Sistan e di ciascun soggetto del Sistan sono pubblicati gli elenchi degli enti di ricerca riconosciuti e dei file di dati elementari resi disponibili.

5. Il presente articolo si applica anche ai dati relativi a persone giuridiche, enti od associazioni».

3. Dopo l'articolo 5-ter, come inserito dal comma 2, è inserito il seguente Capo: «CAPO I-TER - PUBBLICAZIONE DEI DATI, DELLE INFORMAZIONI E DEI DOCUMENTI».

Art. 7. Inserimento dell'articolo 7-bis

1. Dopo l'articolo 7 è inserito il seguente:

«Art. 7-bis. Riutilizzo dei dati pubblicati

1. Gli obblighi di pubblicazione dei dati personali diversi dai dati sensibili e dai dati giudiziari, di cui all'articolo 4, comma 1, lettere d) ed e), del decreto legislativo 30 giugno 2003, n. 196, comportano la possibilità di una diffusione dei dati medesimi attraverso siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web ed il loro riutilizzo ai sensi dell'articolo 7 nel rispetto dei principi sul trattamento dei dati personali.

2. La pubblicazione nei siti istituzionali, in attuazione del presente decreto, di dati relativi a titolari di organi di indirizzo politico e di uffici o incarichi di diretta collaborazione, nonché a dirigenti titolari degli organi amministrativi è finalizzata alla realizzazione della trasparenza pubblica, che integra una finalità di rilevante interesse pubblico nel rispetto della disciplina in materia di protezione dei dati personali.

3. Le pubbliche amministrazioni possono disporre la pubblicazione nel proprio sito istituzionale di dati, informazioni e documenti che non hanno l'obbligo di pubblicare ai sensi del presente decreto o sulla base di specifica previsione di legge o regolamento, nel rispetto dei limiti indicati dall'articolo 5-bis, procedendo alla indicazione in forma anonima dei dati personali eventualmente presenti.

4. Nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

5. Le notizie concernenti lo svolgimento delle prestazioni di chiunque sia addetto a una funzione pubblica e la relativa valutazione sono rese accessibili dall'amministrazione di appartenenza. Non sono invece ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione dal lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il predetto dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di cui all'articolo 4, comma 1, lettera d), del decreto legislativo n. 196 del 2003.

6. Restano fermi i limiti all'accesso e alla diffusione delle informazioni di cui all'articolo 24, commi 1 e 6, della legge 7 agosto 1990, n. 241, e successive modifiche, di tutti i dati di cui all'articolo 9 del decreto legislativo 6 settembre 1989, n. 322, di quelli previsti dalla normativa europea in materia di tutela del segreto statistico e di quelli che siano espressamente qualificati come riservati dalla normativa nazionale ed europea in materia statistica, nonché quelli relativi alla diffusione dei dati idonei a rivelare lo stato di salute e la vita sessuale.

7. La Commissione di cui all'articolo 27 della legge 7 agosto 1990, n. 241, continua ad operare anche oltre la scadenza del mandato prevista dalla disciplina vigente, senza oneri a carico del bilancio dello Stato.
8. Sono esclusi dall'ambito di applicazione del presente decreto i servizi di aggregazione, estrazione e trasmissione massiva degli atti memorizzati in banche dati rese disponibili sul web».

Art. 8. Modifiche all'articolo 8 del decreto legislativo n. 33 del 2013

1. All'articolo 8 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

a) al comma 3 sono aggiunte, in fine, le seguenti parole: «Decorsi detti termini, i relativi dati e documenti sono accessibili ai sensi dell'articolo 5»;

b) dopo il comma 3 è inserito il seguente: «3-bis. L'Autorità nazionale anticorruzione, sulla base di una valutazione del rischio corruttivo, delle esigenze di semplificazione e delle richieste di accesso, determina, anche su proposta del Garante per la protezione dei dati personali, i casi in cui la durata della pubblicazione del dato e del documento può essere inferiore a 5 anni».

Art. 9. Modifiche all'articolo 9 del decreto legislativo n. 33 del 2013 e inserimento dell'articolo 9-bis

1. All'articolo 9 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

a) al comma 1, dopo il primo periodo è inserito il seguente: «Al fine di evitare eventuali duplicazioni, la suddetta

pubblicazione può essere sostituita da un collegamento ipertestuale alla sezione del sito in cui sono presenti i relativi dati, informazioni o documenti, assicurando la qualità delle informazioni di cui all'articolo 6»;
b) il comma 2 è abrogato.

2. Dopo l'articolo 9 è inserito il seguente:

«Art. 9-bis. Pubblicazione delle banche dati

1. Le pubbliche amministrazioni titolari delle banche dati di cui all'Allegato B pubblicano i dati, contenuti nelle medesime banche dati, corrispondenti agli obblighi di pubblicazione di cui al presente decreto, indicati nel medesimo, con i requisiti di cui all'articolo 6, ove compatibili con le modalità di raccolta ed elaborazione dei dati.

2. Nei casi di cui al comma 1, nei limiti dei dati effettivamente contenuti nelle banche dati di cui al medesimo comma, i soggetti di cui all'articolo 2-bis adempiono agli obblighi di pubblicazione previsti dal presente decreto, indicati nell'Allegato B, mediante la comunicazione dei dati, delle informazioni o dei documenti dagli stessi detenuti all'amministrazione titolare della corrispondente banca dati e con la pubblicazione sul proprio sito istituzionale, nella sezione "Amministrazione trasparente", del collegamento ipertestuale, rispettivamente, alla banca dati contenente i relativi dati, informazioni o documenti, ferma restando la possibilità per le amministrazioni di continuare a pubblicare sul proprio sito i predetti dati purché identici a quelli comunicati alla banca dati.

3. Nel caso in cui sia stata omessa la pubblicazione, nelle banche dati, dei dati oggetto di comunicazione ai sensi del comma 2 ed effettivamente comunicati, la richiesta di accesso civico di cui all'articolo 5 è presentata al responsabile della prevenzione della corruzione e della trasparenza dell'amministrazione titolare della banca dati.

4. Qualora l'omessa pubblicazione dei dati da parte delle pubbliche amministrazioni di cui al comma 1 sia imputabile ai soggetti di cui al comma 2, la richiesta di accesso civico di cui all'articolo 5 è presentata al responsabile della prevenzione della corruzione e della trasparenza dell'amministrazione tenuta alla comunicazione».

Art. 10. Modifiche all'articolo 10 del decreto legislativo n. 33 del 2013

1. All'articolo 10 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) la rubrica è sostituita dalla seguente: «Coordinamento con il Piano triennale per la prevenzione della corruzione»;
- b) il comma 1 è sostituito dal seguente: «1. Ogni amministrazione indica, in un'apposita sezione del Piano triennale per la prevenzione della corruzione di cui all'articolo 1, comma 5, della legge n. 190 del 2012, i responsabili della trasmissione e della pubblicazione dei documenti, delle informazioni e dei dati ai sensi del presente decreto»;
- c) il comma 2 è abrogato;
- d) il comma 3 è sostituito dal seguente: «3. La promozione di maggiori livelli di trasparenza costituisce un obiettivo strategico di ogni amministrazione, che deve tradursi nella definizione di obiettivi organizzativi e individuali.»;
- e) il comma 7 è abrogato;
- f) al comma 8, la lettera a) è sostituita dalla seguente: «a) il Piano triennale per la prevenzione della corruzione;» e la lettera d) è soppressa.

Art. 11. Modifiche all'articolo 12 del decreto legislativo n. 33 del 2013

1. All'articolo 12 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

a) al comma 1:

1) dopo le parole «e ogni atto» sono inserite le seguenti: «, previsto dalla legge o comunque adottato,»;

2) dopo le parole «i codici di condotta» sono inserite le seguenti: «, le misure integrative di prevenzione della corruzione individuate ai sensi dell'articolo 1, comma 2-bis, della legge n. 190 del 2012, i documenti di programmazione strategico-gestionale e gli atti degli organismi indipendenti di valutazione».

Art. 12. Modifiche all'articolo 13 del decreto legislativo n. 33 del 2013

1. All'articolo 13, comma 1, lettera b), del decreto legislativo n. 33 del 2013, le parole: «e le risorse a disposizione» sono soppresse.

Art. 13. Modifiche all'articolo 14 del decreto legislativo n. 33 del 2013

1. All'articolo 14 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) la rubrica dell'articolo 14 è sostituita dalla seguente: «Obblighi di pubblicazione concernenti i titolari di incarichi politici, di amministrazione, di direzione o di governo e i titolari di incarichi dirigenziali»;
- b) al comma 1, le parole «di carattere elettivo o comunque esercizio di poteri di indirizzo politico» sono sostituite dalle seguenti: «anche se non di carattere elettivo» e le parole «le pubbliche amministrazioni pubblicano con riferimento a tutti i propri componenti,» sono sostituite dalle seguenti: «lo Stato, le regioni e gli enti locali pubblicano»;
- c) dopo il comma 1 sono inseriti i seguenti: «1-bis. Le pubbliche amministrazioni pubblicano i dati di cui al comma 1 per i titolari di incarichi o cariche di amministrazione, di direzione o di governo comunque denominati, salvo che siano attribuiti a titolo gratuito, e per i titolari di incarichi dirigenziali, a qualsiasi titolo conferiti, ivi inclusi quelli conferiti discrezionalmente dall'organo di indirizzo politico senza procedure pubbliche di selezione.

1-ter. Ciascun dirigente comunica all'amministrazione presso la quale presta servizio gli emolumenti complessivi percepiti a carico della finanza pubblica, anche in relazione a quanto previsto dall'articolo 13, comma 1, del decreto-legge 24 aprile 2014, n. 66, convertito, con modificazioni, dalla legge 23 giugno 2014, n. 89. L'amministrazione pubblica sul proprio sito istituzionale l'ammontare complessivo dei suddetti emolumenti per ciascun dirigente.

1-quater. Negli atti di conferimento di incarichi dirigenziali e nei relativi contratti sono riportati gli obiettivi di trasparenza, finalizzati a rendere i dati pubblicati di immediata comprensione e consultazione per il cittadino, con particolare riferimento ai dati di bilancio sulle spese e ai costi del personale, da indicare sia in modo aggregato che analitico. Il mancato raggiungimento dei suddetti obiettivi determina responsabilità dirigenziale ai sensi dell'articolo 21 del decreto legislativo 30 marzo 2001, n. 165. Del mancato raggiungimento dei suddetti obiettivi si tiene conto ai fini del conferimento di successivi incarichi.

1-quinquies. Gli obblighi di pubblicazione di cui al comma 1 si applicano anche ai titolari di posizioni organizzative a cui sono affidate deleghe ai sensi dell'articolo 17, comma 1-bis, del decreto legislativo n. 165 del 2001, nonché nei casi di cui all'articolo 4-bis, comma 2, del decreto-legge 19 giugno 2015, n. 78 e in ogni altro caso in cui sono svolte funzioni dirigenziali. Per gli altri titolari di posizioni organizzative è pubblicato il solo curriculum vitae»;

d) il comma 2 è sostituito dal seguente: «Le pubbliche amministrazioni pubblicano i dati di cui ai commi 1 e 1-bis entro tre mesi dalla elezione, dalla nomina o dal conferimento dell'incarico e per i tre anni successivi dalla cessazione del mandato o dell'incarico dei soggetti, salve le informazioni concernenti la situazione patrimoniale e, ove consentita, la dichiarazione del coniuge non separato e dei parenti entro il secondo grado, che vengono pubblicate fino alla cessazione dell'incarico o del mandato. Decorsi detti termini, i relativi dati e documenti sono accessibili ai sensi dell'articolo 5».

Art. 14. Modifiche all'articolo 15 del decreto legislativo n. 33 del 2013 e inserimento degli articoli 15-bis e 15-ter

1. All'articolo 15 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) la rubrica dell'articolo è sostituita dalla seguente: «Obblighi di pubblicazione concernenti i titolari di incarichi di collaborazione o consulenza»;
- b) al comma 1:
 - 1) all'alinea, le parole «Fermi restando gli obblighi» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis e fermi restando gli obblighi» e le parole «amministrativi di vertice e di incarichi dirigenziali, a qualsiasi titolo conferiti, nonché» sono soppresse;
 - 2) alla lettera d), le parole: «di lavoro,» sono soppresse;
- c) al comma 2, le parole «dirigenziali a soggetti estranei alla pubblica amministrazione,» sono soppresse;

d) il comma 5 è abrogato.

2. Dopo l'articolo 15 sono inseriti i seguenti:

«Art. 15-bis. Obblighi di pubblicazione concernenti incarichi conferiti nelle società controllate

1. Fermo restando quanto previsto dall'articolo 9-bis, le società a controllo pubblico, nonché le società in regime di amministrazione straordinaria, ad esclusione delle società emittenti strumenti finanziari quotati nei mercati regolamentati e loro controllate, pubblicano, entro trenta giorni dal conferimento di incarichi di collaborazione, di consulenza o di incarichi professionali, inclusi quelli arbitrali, e per i due anni successivi alla loro cessazione, le seguenti informazioni:

a) gli estremi dell'atto di conferimento dell'incarico, l'oggetto della prestazione, la ragione dell'incarico e la durata;

b) il curriculum vitae;

c) i compensi, comunque denominati, relativi al rapporto di consulenza o di collaborazione, nonché agli incarichi professionali, inclusi quelli arbitrali;

d) il tipo di procedura seguita per la selezione del contraente e il numero di partecipanti alla procedura.

2. La pubblicazione delle informazioni di cui al comma 1, relativamente ad incarichi per i quali è previsto un compenso, è condizione di efficacia per il pagamento stesso. In caso di omessa o parziale pubblicazione, il soggetto responsabile della pubblicazione ed il soggetto che ha effettuato il pagamento sono soggetti ad una sanzione pari alla somma corrisposta.

Art. 15-ter. Obblighi di pubblicazione concernenti gli amministratori e gli esperti nominati da organi giurisdizionali o amministrativi

1. L'albo di cui all'articolo 1 del decreto legislativo 4 febbraio 2010, n. 14, è tenuto con modalità informatiche ed è inserito in un'area pubblica dedicata del sito istituzionale del Ministero della giustizia. Nell'albo sono indicati, per ciascun iscritto, gli incarichi ricevuti, con precisazione dell'autorità che lo ha conferito e della relativa data di attribuzione e di cessazione, nonché gli acconti e il compenso finale liquidati. I dati di cui al periodo precedente sono inseriti nell'albo, a cura della cancelleria, entro quindici giorni dalla pronuncia del provvedimento. Il regolamento di cui all'articolo 10 del suddetto decreto legislativo n. 14 del 2010 stabilisce gli ulteriori dati che devono essere contenuti nell'albo.

2. L'Agenzia nazionale per l'amministrazione e la destinazione dei beni sequestrati e confiscati alla criminalità organizzata, di cui all'articolo 110 del decreto legislativo 6 settembre 2011, n. 159, pubblica sul proprio sito istituzionale gli incarichi conferiti ai tecnici e agli altri soggetti qualificati di cui all'articolo 38, comma 3, dello stesso decreto legislativo n. 159 del 2011, nonché i compensi a ciascuno di essi liquidati.

3. Nel registro di cui all'articolo 28, quarto comma, del regio decreto 16 marzo 1942, n. 267, vengono altresì annotati i provvedimenti di liquidazione degli acconti e del compenso finale in favore di ciascuno dei soggetti di cui al medesimo articolo 28, quelli di chiusura del fallimento e di omologazione del concordato e quelli che attestano l'esecuzione del concordato, nonché l'ammontare dell'attivo e del passivo delle procedure chiuse.

4. Le prefetture pubblicano i provvedimenti di nomina e di quantificazione dei compensi degli amministratori e degli esperti nominati ai sensi dell'articolo 32 del decreto-legge 24 giugno 2014, n. 90».

Art. 15. Modifiche all'articolo 16 del decreto legislativo n. 33 del 2013

1. All'articolo 16 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

a) al comma 1, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni»;

b) al comma 2, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni»;

c) dopo il comma 3, è inserito il seguente: «3-bis. Il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri assicura adeguate forme di pubblicità dei processi di mobilità dei dipendenti delle pubbliche amministrazioni, anche attraverso la pubblicazione di dati identificativi dei soggetti interessati».

Art. 16. Modifiche all'articolo 17 del decreto legislativo n. 33 del 2013

1. All'articolo 17 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) al comma 1, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni» e le parole «con la indicazione delle diverse tipologie di rapporto, della distribuzione di questo personale tra le diverse qualifiche e aree professionali,» e «La pubblicazione comprende l'elenco dei titolari dei contratti a tempo determinato.» sono soppresse;
- b) al comma 2, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni» e le parole «articolato per aree professionali,» sono soppresse.

Art. 17. Modifiche all'articolo 18 del decreto legislativo n. 33 del 2013

1. Al comma 1, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni».

Art. 18. Modifiche all'articolo 19 del decreto legislativo n. 33 del 2013

1. All'articolo 19 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:
- a) al comma 1, dopo le parole «presso l'amministrazione» sono inserite le seguenti: «, nonché i criteri di valutazione della Commissione e le tracce delle prove scritte»;
- b) al comma 2, le parole «, nonché quello dei bandi espletati nel corso dell'ultimo triennio, accompagnato dall'indicazione, per ciascuno di essi, del numero dei dipendenti assunti e delle spese effettuate» sono soppresse.

Art. 19. Modifiche all'articolo 20 del decreto legislativo n. 33 del 2013

1. All'articolo 20 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:
- a) il comma 2 è sostituito dal seguente: «Le pubbliche amministrazioni pubblicano i criteri definiti nei sistemi di misurazione e valutazione della performance per l'assegnazione del trattamento accessorio e i dati relativi alla sua distribuzione, in forma aggregata, al fine di dare conto del livello di selettività utilizzato nella distribuzione dei premi e degli incentivi, nonché i dati relativi al grado di differenziazione nell'utilizzo della premialità sia per i dirigenti sia per i dipendenti.»;
- b) il comma 3 è abrogato.

Art. 20. Modifiche all'articolo 21 del decreto legislativo n. 33 del 2013

1. All'articolo 21 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:
- a) al comma 1, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni»;
- b) al comma 2, dopo le parole «Fermo restando quanto previsto» sono inserite le seguenti: «dall'articolo 9-bis e».

Art. 21. Modifiche all'articolo 22 del decreto legislativo n. 33 del 2013

1. All'articolo 22 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:
- a) al comma 1:
- 1) all'alinea, le parole «Ciascuna amministrazione» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, ciascuna amministrazione»;
- 2) alla lettera a) le parole «e finanziati dall'Amministrazione medesima ovvero» sono sostituite dalle seguenti: «o finanziati dall'amministrazione medesima nonché di quelli»;
- 3) dopo la lettera d) è inserita la seguente: «d-bis) i provvedimenti in materia di costituzione di società a partecipazione pubblica, acquisto di partecipazioni in società già costituite, gestione delle partecipazioni pubbliche, alienazione di partecipazioni sociali, quotazione di società a controllo pubblico in mercati regolamentati e razionalizzazione periodica delle partecipazioni pubbliche, previsti dal decreto legislativo adottato ai sensi dell'articolo 18 della legge 7 agosto 2015, n. 124.»;
- b) al comma 2, le parole «Per ciascuno degli enti» sono sostituite dalle seguenti: «Fermo restando quanto previsto

dall'articolo 9-bis, per ciascuno degli enti»;

c) al comma 3, le parole «degli enti» sono sostituite dalle seguenti: «dei soggetti» e le parole «, nei quali sono pubblicati i dati relativi ai componenti degli organi di indirizzo e ai soggetti titolari di incarico, in applicazione degli articoli 14 e 15» sono soppresse;

d) al comma 4, dopo le parole «dell'amministrazione interessata» sono inserite le seguenti: «ad esclusione dei pagamenti che le amministrazioni sono tenute ad erogare a fronte di obbligazioni contrattuali per prestazioni svolte in loro favore da parte di uno degli enti e società indicati nelle categorie di cui al comma 1, lettere da a) a c)»;

e) il comma 6 è sostituito dal seguente: «6. Le disposizioni di cui al presente articolo non trovano applicazione nei confronti delle società, partecipate da amministrazioni pubbliche, con azioni quotate in mercati regolamentati italiani o di altri paesi dell'Unione europea, e loro controllate.».

Art. 22. Modifiche all'articolo 23 del decreto legislativo n. 33 del 2013

1. All'articolo 23 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

a) al comma 1,

1) la lettera a) è soppressa;

2) alla lettera b), le parole «12 aprile 2006, n. 163» sono sostituite dalle seguenti: «18 aprile 2016, n. 50, fermo restando quanto previsto dall'articolo 9-bis»;

3) la lettera c) è soppressa;

4) alla lettera d) sono aggiunte, in fine, le seguenti parole: «, ai sensi degli articoli 11 e 15 della legge 7 agosto 1990, n. 241»;

b) il comma 2 è abrogato.

Art. 23. Modifiche all'articolo 26 del decreto legislativo n. 33 del 2013

1. Al comma 3 dell'articolo 26 del decreto legislativo n. 33 del 2013 le parole «; la sua eventuale omissione o incompletezza è rilevata d'ufficio dagli organi dirigenziali, sotto la propria responsabilità amministrativa, patrimoniale e contabile per l'indebita concessione o attribuzione del beneficio economico» sono soppresse.

Art. 24. Modifiche all'articolo 28 del decreto legislativo n. 33 del 2013

1. Al comma 1 dell'articolo 28 del decreto legislativo n. 33 del 2013, le parole «Le regioni, le province» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le regioni, le province».

Art. 25. Modifiche all'articolo 29 del decreto legislativo n. 33 del 2013

1. Al comma 1 dell'articolo 29 del decreto legislativo n. 33 del 2013, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni».

Art. 26. Modifiche all'articolo 30 del decreto legislativo n. 33 del 2013

1. Al comma 1 dell'articolo 30 del decreto legislativo n. 33 del 2013, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni» e dopo le parole «immobili posseduti» sono inserite le seguenti: «e di quelli detenuti».

Art. 27. Modifiche all'articolo 31 del decreto legislativo n. 33 del 2013

1. Il comma 1 dell'articolo 31 del decreto legislativo n. 33 del 2013 è sostituito dal seguente: «1. Le pubbliche amministrazioni pubblicano gli atti degli organismi indipendenti di valutazione o nuclei di valutazione, procedendo all'indicazione in forma anonima dei dati personali eventualmente presenti. Pubblicano, inoltre, la relazione degli organi di revisione amministrativa e contabile al bilancio di previsione o budget, alle relative variazioni e al conto consuntivo o bilancio di esercizio nonché tutti i rilievi ancorché non recepiti della Corte dei conti riguardanti l'organizzazione e l'attività delle amministrazioni stesse e dei loro uffici».

Art. 28. Modifiche all'articolo 32 del decreto legislativo n. 33 del 2013

1. All'articolo 32 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole «Le pubbliche amministrazioni» sono inserite le seguenti: «e i gestori di pubblici servizi»;

b) al comma 2:

1) dopo le parole «Le pubbliche amministrazioni» sono inserite le seguenti: «e i gestori di pubblici servizi,»;

2) alla lettera a), le parole «, evidenziando quelli effettivamente sostenuti e quelli imputati al personale per ogni servizio erogato» sono soppresse;

3) la lettera b) è abrogata.

Art. 29. Modifiche all'articolo 33 del decreto legislativo n. 33 del 2013

1. Al comma 1 dell'articolo 33 del decreto legislativo n. 33 del 2013, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni», dopo le parole «**beni, servizi,**» sono inserite le seguenti: «prestazioni professionali» e dopo le parole «dei pagamenti» sono inserite le seguenti: «, nonché l'ammontare complessivo dei debiti e il numero delle imprese creditrici».

Art. 30. Modifiche all'articolo 35 del decreto legislativo n. 33 del 2013

1. All'articolo 35 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

a) Al comma 1, lettera c) le parole «il nome del responsabile» sono sostituite dalle seguenti: «l'ufficio»;

b) la lettera n) del comma 1 è soppressa;

c) le lettere b) e c) del comma 3 sono soppresse.

Art. 31. Modifiche all'articolo 37 del decreto legislativo n. 33 del 2013

1. L'articolo 37 del decreto legislativo n. 33 del 2013 è sostituito dal seguente:

«Art. 37. Obblighi di pubblicazione concernenti i contratti pubblici di lavori, servizi e forniture

1. Fermo restando quanto previsto dall'articolo 9-bis e fermi restando gli obblighi di pubblicità legale, le pubbliche amministrazioni e le stazioni appaltanti pubblicano:

a) i dati previsti dall'articolo 1, comma 32, della legge 6 novembre 2012, n. 190;

b) gli atti e le informazioni oggetto di pubblicazione ai sensi del decreto legislativo 18 aprile 2016, n. 50.

2. Ai sensi dell'articolo 9-bis, gli obblighi di pubblicazione di cui alla lettera a) si intendono assolti, attraverso l'invio dei medesimi dati alla banca dati delle amministrazioni pubbliche ai sensi dell'articolo 2 del decreto legislativo 29 dicembre 2011, n. 229, limitatamente alla parte lavori».

Art. 32. Modifiche all'articolo 38 del decreto legislativo n. 33 del 2013

1. All'articolo 38 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) al comma 1, le parole «Le pubbliche amministrazioni» sono sostituite dalle seguenti: «Fermo restando quanto previsto dall'articolo 9-bis, le pubbliche amministrazioni» e le parole da: «tempestivamente» a «ex ante;» sono soppresse;
- b) il comma 2 è sostituito dal seguente: «2. Fermi restando gli obblighi di pubblicazione di cui all'articolo 21 del decreto legislativo 18 aprile 2016, n. 50, le pubbliche amministrazioni pubblicano tempestivamente gli atti di programmazione delle opere pubbliche, nonché le informazioni relative ai tempi, ai costi unitari e agli indicatori di realizzazione delle opere pubbliche in corso o completate. Le informazioni sono pubblicate sulla base di uno schema tipo redatto dal Ministero dell'economia e delle finanze d'intesa con l'Autorità nazionale anticorruzione, che ne curano altresì la raccolta e la pubblicazione nei propri siti web istituzionali al fine di consentirne una agevole comparazione»;
- c) dopo il comma 2 è aggiunto il seguente: «2-bis. Per i Ministeri, gli atti di programmazione di cui al comma 2 sono quelli indicati dall'articolo 2 del decreto legislativo 29 dicembre 2011, n. 228.».

Art. 33. Modifiche all'articolo 41 del decreto legislativo n. 33 del 2013

1. All'articolo 41 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) dopo il comma 1 è inserito il seguente: «1-bis. Le amministrazioni di cui al comma 1 pubblicano altresì, nei loro siti istituzionali, i dati relativi a tutte le spese e a tutti i pagamenti effettuati, distinti per tipologia di lavoro, bene o servizio, e ne permettono la consultazione, in forma sintetica e aggregata, in relazione alla tipologia di spesa sostenuta, all'ambito temporale di riferimento e ai beneficiari.»;
- b) al comma 3, le parole «, fatta eccezione per i responsabili di strutture semplici,» sono soppresse;
- c) al comma 6, dopo le parole «Liste di attesa,» sono inserite le seguenti: «i criteri di formazione delle liste di attesa,».

Art. 34. Modifiche all'articolo 43 del decreto legislativo n. 33 del 2013

1. All'articolo 43 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) al comma 1, le parole «Programma triennale per la trasparenza e l'integrità» sono sostituite dalle seguenti: «Piano triennale per la prevenzione della corruzione»;
- b) il comma 2 è abrogato;
- c) il comma 4 è sostituito dal seguente: «4. I dirigenti responsabili dell'amministrazione e il responsabile per la trasparenza controllano e assicurano la regolare attuazione dell'accesso civico sulla base di quanto stabilito dal presente decreto.».

Art. 35. Modifiche all'articolo 44 del decreto legislativo n. 33 del 2013

1. Al comma 1 dell'articolo 44 del decreto legislativo n. 33 del 2013 le parole «Programma triennale per la trasparenza e l'integrità di cui all'articolo 10» sono sostituite dalle seguenti: «Piano triennale per la prevenzione della corruzione».

Art. 36. Modifiche all'articolo 45 del decreto legislativo n. 33 del 2013

1. All'articolo 45 del decreto legislativo n. 33 del 2013, sono apportate le seguenti modificazioni:

- a) le parole «la CIVIT, anche in qualità di Autorità nazionale anticorruzione,» e le parole «la CIVIT», ovunque ricorrano, sono sostituite dalle seguenti: «L'autorità nazionale anticorruzione»;
- b) al comma 1, le parole «l'adozione di atti o provvedimenti richiesti dalla normativa vigente, ovvero la rimozione di comportamenti o atti contrastanti con i piani e le regole sulla trasparenza.» sono sostituite dalle seguenti: «di procedere, entro un termine non superiore a trenta giorni, alla pubblicazione di dati, documenti e informazioni ai sensi del presente decreto, all'adozione di atti o provvedimenti richiesti dalla normativa vigente ovvero alla rimozione di comportamenti o atti contrastanti con i piani e le regole sulla trasparenza.»;
- c) al comma 4, il primo periodo è sostituito dai seguenti periodi: «Il mancato rispetto dell'obbligo di pubblicazione di cui al comma 1 costituisce illecito disciplinare. L'Autorità nazionale anticorruzione segnala l'illecito all'ufficio di cui all'articolo 55-bis, comma 4, del decreto legislativo 30 marzo 2001, n. 165, dell'amministrazione interessata ai fini dell'attivazione del procedimento disciplinare a carico del responsabile della pubblicazione o del dirigente tenuto alla trasmissione delle informazioni.».

Art. 37. Modifiche all'articolo 46 del decreto legislativo n. 33 del 2013

1. All'articolo 46 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) la rubrica è sostituita dalla seguente: «Responsabilità derivante dalla violazione delle disposizioni in materia di obblighi di pubblicazione e di accesso civico»;
- b) al comma 1, le parole «o la mancata predisposizione del Programma triennale per la trasparenza e l'integrità» sono sostituite dalla seguente: «e il rifiuto, il differimento e la limitazione dell'accesso civico, al di fuori delle ipotesi previste dall'articolo 5-bis,».

Art. 38. Modifiche all'articolo 47 del decreto legislativo n. 33 del 2013

1. All'articolo 47 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) la rubrica è sostituita dalla seguente: «Sanzioni per la violazione degli obblighi di trasparenza per casi specifici»;
- b) dopo il comma 1 è inserito il seguente: «1-bis. La sanzione di cui al comma 1 si applica anche nei confronti del dirigente che non effettua la comunicazione ai sensi dell'articolo 14, comma 1-ter, relativa agli emolumenti complessivi percepiti a carico della finanza pubblica, nonché nei confronti del responsabile della mancata pubblicazione dei dati di cui al medesimo articolo. La stessa sanzione si applica nei confronti del responsabile della mancata pubblicazione dei dati di cui all'articolo 4-bis, comma 2.»;
- c) il comma 3 dell'articolo 47 è sostituito dal seguente: «3. Le sanzioni di cui al comma 1 sono irrogate dall'Autorità nazionale anticorruzione. L'Autorità nazionale anticorruzione disciplina con proprio regolamento, nel rispetto delle norme previste dalla legge 24 novembre 1981, n. 689, il procedimento per l'irrogazione delle sanzioni.».

Art. 39. Modifiche all'articolo 48 del decreto legislativo n. 33 del 2013

1. All'articolo 48 del decreto legislativo n. 33 del 2013 sono apportate le seguenti modificazioni:

- a) al comma 1 le parole «Il Dipartimento della funzione pubblica» sono sostituite dalle seguenti: «L'Autorità nazionale anticorruzione»;
- b) al comma 3 le parole «con decreti del Presidente del Consiglio dei ministri» sono sostituite dalle seguenti: «dall'Autorità nazionale anticorruzione»;
- c) al comma 4 le parole «I decreti» sono sostituite dalle seguenti: «Gli standard, i modelli e gli schemi»;
- d) al comma 5 le parole «Le amministrazioni di cui all'articolo 11,» sono sostituite dalle seguenti: «I soggetti di cui all'articolo 2-bis,».

Art. 40. Modifiche all'articolo 52 del decreto legislativo n. 33 del 2013

1. All'articolo 52 del decreto legislativo n. 33 del 2013, dopo il comma 4 è inserito il seguente: «4-bis) All'articolo 1, comma 1, del decreto legislativo 29 dicembre 2011, n. 229, le parole da «e i soggetti» fino a «attività istituzionale» sono sostituite dalle seguenti: «nonché gli ulteriori soggetti di cui all'articolo 2-bis del decreto legislativo 14 marzo 2013, n. 33, che realizzano opere pubbliche».

Capo II - Modifiche alla legge 6 novembre 2012, n. 190**Art. 41. Modifiche all'articolo 1 della legge n. 190 del 2012**

1. All'articolo 1 della legge n. 190 del 2012 sono apportate le seguenti modificazioni:

- a) la lettera b) del comma 2 è sostituita dalla seguente: «b) adotta il Piano nazionale anticorruzione ai sensi del

comma 2-bis;»;

b) dopo il comma 2 è inserito il seguente: «2-bis. Il Piano nazionale anticorruzione è adottato sentiti il Comitato interministeriale di cui al comma 4 e la Conferenza unificata di cui all'articolo 8, comma 1, del decreto legislativo 28 agosto 1997, n. 281. Il Piano ha durata triennale ed è aggiornato annualmente. Esso costituisce atto di indirizzo per le pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ai fini dell'adozione dei propri piani triennali di prevenzione della corruzione, e per gli altri soggetti di cui all'articolo 2-bis, comma 2, del decreto legislativo 14 marzo 2013, n. 33, ai fini dell'adozione di misure di prevenzione della corruzione integrative di quelle adottate ai sensi del decreto legislativo 8 giugno 2001, n. 231, anche per assicurare l'attuazione dei compiti di cui al comma 4, lettera a). Esso, inoltre, anche in relazione alla dimensione e ai diversi settori di attività degli enti, individua i principali rischi di corruzione e i relativi rimedi e contiene l'indicazione di obiettivi, tempi e modalità di adozione e attuazione delle misure di contrasto alla corruzione.»;

c) il comma 3 è sostituito dal seguente: «3. Per l'esercizio delle funzioni di cui al comma 2, lettera f), l'Autorità nazionale anticorruzione esercita poteri ispettivi mediante richiesta di notizie, informazioni, atti e documenti alle pubbliche amministrazioni, e ordina l'adozione di atti o provvedimenti richiesti dai piani di cui ai commi 4 e 5 e dalle regole sulla trasparenza dell'attività amministrativa previste dalle disposizioni vigenti, ovvero la rimozione di comportamenti o atti contrastanti con i piani e le regole sulla trasparenza citati.»;

d) la lettera c) del comma 4 è soppressa;

e) il comma 6, è sostituito dal seguente: «6. I comuni con popolazione inferiore a 15.000 abitanti possono aggregarsi per definire in comune, tramite accordi ai sensi dell'articolo 15 della legge 7 agosto 1990, n. 241, il piano triennale per la prevenzione della corruzione, secondo le indicazioni contenute nel Piano nazionale anticorruzione di cui al comma 2-bis. Ai fini della predisposizione del piano triennale per la prevenzione della corruzione, il prefetto, su richiesta, fornisce il necessario supporto tecnico e informativo agli enti locali, anche al fine di assicurare che i piani siano formulati e adottati nel rispetto delle linee guida contenute nel Piano nazionale approvato dalla Commissione.»;

f) il comma 7 è sostituito dal seguente: «7. L'organo di indirizzo individua, di norma tra i dirigenti di ruolo in servizio, il Responsabile della prevenzione della corruzione e della trasparenza, disponendo le eventuali modifiche organizzative necessarie per assicurare funzioni e poteri idonei per lo svolgimento dell'incarico con piena autonomia ed effettività. Negli enti locali, il Responsabile della prevenzione della corruzione e della trasparenza è individuato, di norma, nel segretario o nel dirigente apicale, salva diversa e motivata determinazione. Nelle unioni di comuni, può essere nominato un unico responsabile della prevenzione della corruzione e della trasparenza. Il Responsabile della prevenzione della corruzione e della trasparenza segnala all'organo di indirizzo e all'organismo indipendente di valutazione le disfunzioni inerenti all'attuazione delle misure in materia di prevenzione della corruzione e di trasparenza e indica agli uffici competenti all'esercizio dell'azione disciplinare i nominativi dei dipendenti che non hanno attuato correttamente le misure in materia di prevenzione della corruzione e di trasparenza. Eventuali misure discriminatorie, dirette o indirette, nei confronti del Responsabile della prevenzione della corruzione e della trasparenza per motivi collegati, direttamente o indirettamente, allo svolgimento delle sue funzioni devono essere segnalate all'Autorità nazionale anticorruzione, che può chiedere informazioni all'organo di indirizzo e intervenire nelle forme di cui al comma 3, articolo 15, decreto legislativo 8 aprile 2013, n. 39.»;

g) il comma 8 è sostituito dal seguente: «8. L'organo di indirizzo definisce gli obiettivi strategici in materia di prevenzione della corruzione e trasparenza, che costituiscono contenuto necessario dei documenti di programmazione strategico-gestionale e del Piano triennale per la prevenzione della corruzione. L'organo di indirizzo adotta il Piano triennale per la prevenzione della corruzione su proposta del Responsabile della prevenzione della corruzione e della trasparenza entro il 31 gennaio di ogni anno e ne cura la trasmissione all'Autorità nazionale anticorruzione. Negli enti locali il piano è approvato dalla giunta. L'attività di elaborazione del piano non può essere affidata a soggetti estranei all'amministrazione. Il responsabile della prevenzione della corruzione e della trasparenza, entro lo stesso termine, definisce procedure appropriate per selezionare e formare, ai sensi del comma 10, i dipendenti destinati ad operare in settori particolarmente esposti alla corruzione. Le attività a rischio di corruzione devono essere svolte, ove possibile, dal personale di cui al comma 11.»;

h) dopo il comma 8 è inserito il seguente: «8-bis. L'Organismo indipendente di valutazione verifica, anche ai fini della validazione della Relazione sulla performance, che i piani triennali per la prevenzione della corruzione siano coerenti con gli obiettivi stabiliti nei documenti di programmazione strategico-gestionale e che nella misurazione e valutazione delle performance si tenga conto degli obiettivi connessi all'anticorruzione e alla trasparenza. Esso verifica i contenuti della Relazione di cui al comma 14 in rapporto agli obiettivi inerenti alla prevenzione della corruzione e alla trasparenza. A tal fine, l'Organismo medesimo può chiedere al Responsabile della prevenzione della corruzione e della trasparenza le informazioni e i documenti necessari per lo svolgimento

del controllo e può effettuare audizioni di dipendenti. L'Organismo medesimo riferisce all'Autorità nazionale anticorruzione sullo stato di attuazione delle misure di prevenzione della corruzione e di trasparenza.»;

i) alla lettera a) del comma 9, dopo le parole «di cui al comma 16,» sono inserite le seguenti: «anche ulteriori rispetto a quelle indicate nel Piano nazionale anticorruzione,» e dopo le parole «rischio di corruzione,» sono inserite le seguenti: «e le relative misure di contrasto,»;

j) alla lettera d) del comma 9, le parole «monitorare il» sono sostituite dalle seguenti: «definire le modalità di monitoraggio del»;

k) alla lettera e) del comma 9, le parole «monitorare i» sono sostituite dalle seguenti: «definire le modalità di monitoraggio dei»;

l) il comma 14 è sostituito dal seguente: «14. In caso di ripetute violazioni delle misure di prevenzione previste dal Piano, il responsabile individuato ai sensi del comma 7 del presente articolo risponde ai sensi dell'articolo 21 del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, nonché, per omesso controllo, sul piano disciplinare, salvo che provi di avere comunicato agli uffici le misure da adottare e le relative modalità e di avere vigilato sull'osservanza del Piano. La violazione, da parte dei dipendenti dell'amministrazione, delle misure di prevenzione previste dal Piano costituisce illecito disciplinare. Entro il 15 dicembre di ogni anno, il dirigente individuato ai sensi del comma 7 del presente articolo trasmette all'organismo indipendente di valutazione e all'organo di indirizzo dell'amministrazione una relazione recante i risultati dell'attività svolta e la pubblica nel sito web dell'amministrazione. Nei casi in cui l'organo di indirizzo lo richieda o qualora il dirigente responsabile lo ritenga opportuno, quest'ultimo riferisce sull'attività.».

Capo III - Disposizioni finali e transitorie

Art. 42. Disposizioni transitorie

1. I soggetti di cui all'articolo 2-bis del decreto legislativo n. 33 del 2013 si adeguano alle modifiche allo stesso decreto legislativo, introdotte dal presente decreto, e assicurano l'effettivo esercizio del diritto di cui all'articolo 5, comma 2, del decreto legislativo n. 33 del 2013, come modificato dall'articolo 6 del presente decreto, entro sei mesi dalla data di entrata in vigore del presente decreto.

2. Gli obblighi di pubblicazione di cui all'articolo 9-bis del decreto legislativo n. 33 del 2013, introdotto dall'articolo 9, comma 2, del presente decreto, acquistano efficacia decorso un anno dalla data di entrata in vigore del presente decreto. Ai fini dell'applicazione del predetto articolo, le pubbliche amministrazioni e gli altri soggetti di cui all'articolo 2-bis del predetto decreto legislativo n. 33 del 2013, entro un anno dalla data di entrata in vigore del presente decreto, verificano la completezza e la correttezza dei dati già comunicati alle pubbliche amministrazioni titolari delle banche dati di cui all'Allegato B del decreto legislativo n. 33 del 2013, e, ove necessario, trasmettono alle predette amministrazioni i dati mancanti o aggiornati. A decorrere dalla medesima data, nelle more dell'adozione del decreto legislativo di attuazione dell'articolo 17, comma 1, lettera u), della legge 7 agosto 2015, n. 124, i soggetti di cui al citato articolo 9-bis possono adempiere in forma associata agli obblighi di comunicazione e di pubblicazione con le modalità di cui al medesimo articolo 9-bis, comma 2, del decreto legislativo n. 33 del 2013.

3. Le forme di pubblicità di cui all'articolo 16, comma 3-bis, del decreto legislativo n. 33 del 2013, inserito dall'articolo 15 del presente decreto, sono dovute anche per i processi di mobilità di cui all'articolo 1, commi da 421 a 428 della legge 23 dicembre 2014, n. 190.

Art. 43. Abrogazioni

1. Al decreto legislativo n. 33 del 2013 sono abrogati:

- a) l'articolo 4;
- b) l'articolo 11;
- c) l'articolo 24;
- d) l'articolo 25;
- e) l'articolo 34;
- f) l'articolo 39, comma 1, lettera b);
- g) l'articolo 42, comma 1, lettera d).

1. Al decreto del Presidente della Repubblica 7 aprile 2000, n. 118, l'articolo 1 è abrogato.

2. Alla legge 27 dicembre 2013, n. 147, la lettera f), del comma 611, è soppressa.
3. Alla legge 28 dicembre 2015, n. 208, i commi 675 e 676 dell'articolo 1 sono abrogati.
4. I richiami effettuati all'articolo 11 del decreto legislativo n. 33 del 2013, ovunque ricorrano, si intendono riferiti all'articolo 2-bis del medesimo decreto, introdotto dall'articolo 3 del presente decreto.

Art. 44. Clausola di invarianza finanziaria

1. Dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri per la finanza pubblica. Le amministrazioni interessate provvedono agli adempimenti di cui al presente decreto con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.

La presente legge, munita del sigillo dello Stato, sarà inserita nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarla e di farla osservare come legge dello Stato.

APPENDICE 3 – SITUAZIONE MONDIALE NEL CAMPO DELL'ACCESSIBILITÀ AI DATI (cfr, Wiki)

Cfr: <https://www.dlapiperdataprotection.com/>

Typology: 1.25 Other

Submitting date: 01.02.2016

Acceptance date: 20.02.2016