GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Arricchito con riferimenti ai Considerando

Aggiornato alle rettifiche pubblicate sulla Gazzetta Ufficiale dell'Unione europea 127 del 23 maggio 2018

NOTA PER LA LETTURA DEL TESTO

Per facilitare una fruizione più ampia e ragionata del testo, articoli e paragrafi del Regolamento riportano tra parentesi i rispettivi "Considerando", laddove esistenti, indicati con l'abbreviazione "C" e il numero corrispondente

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 27 aprile 2016

relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

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

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo (1),

visto il parere del Comitato delle regioni (2),

deliberando secondo la procedura legislativa ordinaria (3),

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 dati di carattere personale (“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. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

(3) La direttiva 95/46/CE del Parlamento europeo e del Consiglio (4) ha come obiettivo di armonizzare la tutela dei diritti e delle libertà fondamentali delle persone fisiche rispetto alle attività di trattamento dei dati e assicurare la libera circolazione dei dati personali tra Stati membri.

(4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di

proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

(5) L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro.

(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che le riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.

(7) Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che le riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche.

(8) Ove il presente regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono, nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone cui si applicano, integrare elementi del presente regolamento nel proprio diritto nazionale.

(9) Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE.

(10) Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento. In combinato disposto con la legislazione generale e orizzontale in materia di protezione dei dati che attua la direttiva 95/46/CE, gli Stati membri dispongono di varie leggi settoriali in settori che richiedono disposizioni più specifiche. Il presente regolamento prevede anche un margine di manovra degli Stati membri per precisarne le norme, anche con riguardo al trattamento di categorie particolari di dati personali («dati sensibili»). In tal senso, il presente regolamento non esclude che il diritto degli Stati membri stabilisca le condizioni per specifiche situazioni di trattamento, anche determinando con maggiore precisione le condizioni alle quali il trattamento di dati personali è lecito.

(11) Un'efficace protezione dei dati personali in tutta l'Unione presuppone il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali, nonché poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri.

(12) 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.

(13) Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un controllo coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri. Per il buon funzionamento del mercato interno è necessario che la libera circolazione dei dati personali all'interno dell'Unione non sia limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali. Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni. Inoltre, le istituzioni e gli organi dell'Unione e gli Stati membri e le loro autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese nell'applicare il presente regolamento. La nozione di micro, piccola e media impresa dovrebbe ispirarsi all'articolo 2 dell'allegato della raccomandazione 2003/361/CE della Commissione (5).

(14) È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro

dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto.

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

(16) Il presente regolamento non si applica a questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale. Il presente regolamento non si applica al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione.

(17) Il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio (6) 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 dal presente regolamento e applicati alla luce dello stesso. Per offrire un quadro di protezione dei dati solido e coerente nell'Unione, si dovrebbe procedere, successivamente all'adozione del presente regolamento, ai necessari adeguamenti del regolamento (CE) n. 45/2001, al fine di consentirne l'applicazione contemporaneamente al presente regolamento.

(18) Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

(19) La 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, e la libera circolazione di tali dati sono oggetto di uno specifico atto dell'Unione. Il presente regolamento non dovrebbe pertanto applicarsi ai trattamenti effettuati per tali finalità. I dati personali trattati dalle autorità pubbliche in forza del presente regolamento, quando utilizzati per tali finalità, dovrebbero invece essere disciplinati da un più specifico atto dell'Unione, segnatamente la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio (7). Gli Stati membri possono conferire alle autorità competenti ai sensi della direttiva (UE) 2016/680 altri compiti che non siano necessariamente svolti 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, affinché il trattamento di dati personali per tali

altre finalità, nella misura in cui ricada nell'ambito di applicazione del diritto dell'Unione, rientri nell'ambito di applicazione del presente regolamento.

Con riguardo al trattamento dei dati personali da parte di tali autorità competenti per finalità rientranti nell'ambito di applicazione del presente regolamento, gli Stati membri dovrebbero poter mantenere o introdurre disposizioni più specifiche per adattare l'applicazione delle disposizioni del presente regolamento. Tali disposizioni possono determinare con maggiore precisione requisiti specifici per il trattamento di dati personali da parte di dette autorità competenti per tali altre finalità, tenuto conto della struttura costituzionale, organizzativa e amministrativa dei rispettivi Stati membri. Quando il trattamento dei dati personali effettuato da organismi privati rientra nell'ambito di applicazione del presente regolamento, è opportuno che lo stesso preveda la facoltà per gli Stati membri, a determinate condizioni, di adottare disposizioni legislative intese a limitare determinati obblighi e diritti, qualora tale limitazione costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia di importanti interessi specifici, comprese la sicurezza pubblica e le attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica. Ciò riveste particolare importanza ad esempio nel quadro del riciclaggio o di attività di medicina legale.

(20) Sebbene il presente regolamento si applichi, tra l'altro, anche alle attività delle autorità giurisdizionali e di altre autorità giudiziarie, il diritto dell'Unione o degli Stati membri potrebbe specificare le operazioni e le procedure di trattamento relativamente al trattamento dei dati personali effettuato da autorità giurisdizionali e da altre autorità giudiziarie. Non è opportuno che rientri nella competenza delle autorità di controllo il trattamento di dati personali effettuato dalle autorità giurisdizionali nell'adempimento delle loro funzioni giurisdizionali, al fine di salvaguardare l'indipendenza della magistratura nell'adempimento dei suoi compiti giurisdizionali, compreso il processo decisionale. Si dovrebbe poter affidare il controllo su tali trattamenti di dati ad organismi specifici all'interno del sistema giudiziario dello Stato membro, che dovrebbero in particolare assicurare la conformità alle norme del presente regolamento, rafforzare la consapevolezza della magistratura con riguardo agli obblighi che alla stessa derivano dal presente regolamento ed esaminare i reclami in relazione a tali operazioni di trattamento dei dati.

(21) Il presente regolamento non pregiudica l'applicazione della direttiva 2000/31/CE del Parlamento europeo e del Consiglio (8), in particolare delle norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva. Detta direttiva mira a contribuire al buon funzionamento del mercato interno garantendo la libera circolazione dei servizi della società dell'informazione tra Stati membri.

(22) Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o responsabile del trattamento nel territorio dell'Unione dovrebbe essere conforme al presente regolamento, indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica.

(23) Onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al presente regolamento, è opportuno che questo disciplini il trattamento dei dati personali degli interessati che si trovano nell'Unione effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono connesse all'offerta

di beni o servizi a detti interessati indipendentemente dal fatto che vi sia un pagamento correlato. Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione.

(24) È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al monitoraggio del comportamento di detti interessati, nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.

(25) Laddove vige il diritto di uno Stato membro in virtù del diritto internazionale pubblico, ad esempio nella rappresentanza diplomatica o consolare di uno Stato membro, il presente regolamento dovrebbe applicarsi anche a un titolare del trattamento non stabilito nell'Unione.

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

(27) Il presente regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute.

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

(29) Al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale nell'ambito dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento in questione, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate nell'ambito dello stesso titolare del trattamento

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

(31) 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 degli Stati membri. 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.

(32) Il consenso dovrebbe essere prestato mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.

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

(34) È opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino 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.

(35) 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 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 (9); 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.

(36) Lo stabilimento principale di un titolare del trattamento nell'Unione dovrebbe essere il luogo in cui ha sede la sua amministrazione centrale nell'Unione, a meno che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione, nel qual caso tale altro stabilimento dovrebbe essere considerato lo stabilimento principale. Lo stabilimento principale di un titolare del trattamento nell'Unione dovrebbe essere determinato in base a criteri obiettivi e implicare l'effettivo e reale svolgimento di attività di gestione finalizzate alle principali decisioni sulle finalità e sui mezzi del trattamento nel quadro di un'organizzazione stabile. Tale criterio non dovrebbe dipendere dal fatto che i dati personali siano trattati in quella sede. La presenza o l'uso di mezzi tecnici e tecnologie di trattamento di dati personali o di attività di trattamento non costituiscono di per sé lo stabilimento principale né sono quindi criteri determinanti della sua esistenza. Per quanto riguarda il responsabile del trattamento, per «stabilimento principale» dovrebbe intendersi il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se non dispone di un'amministrazione centrale nell'Unione, il luogo in cui sono condotte le principali attività di trattamento nell'Unione. In caso di coinvolgimento sia del titolare del trattamento sia del responsabile del trattamento, l'autorità di controllo competente capofila dovrebbe continuare a essere l'autorità di controllo dello Stato membro in cui il titolare del trattamento ha lo stabilimento principale, ma l'autorità di controllo del responsabile del trattamento dovrebbe essere considerata autorità di controllo interessata e tale autorità di controllo dovrebbe partecipare alla procedura di cooperazione prevista dal presente regolamento. In ogni caso, le autorità di controllo dello Stato membro o degli Stati membri in cui il responsabile del trattamento ha uno o più stabilimenti non dovrebbero essere considerate autorità di controllo interessate quando il progetto di decisione riguarda soltanto il titolare del trattamento. Se il trattamento è effettuato da un gruppo imprenditoriale, lo stabilimento principale dell'impresa

controllante dovrebbe essere considerato lo stabilimento principale del gruppo di imprese, tranne nei casi in cui le finalità e i mezzi del trattamento sono stabiliti da un'altra impresa.

(37) Un gruppo imprenditoriale dovrebbe costituirsi di un'impresa controllante e delle sue controllate, là dove l'impresa controllante dovrebbe essere quella che può esercitare un'influenza dominante sulle controllate in forza, ad esempio, della proprietà, della partecipazione finanziaria o delle norme societarie o del potere di fare applicare le norme in materia di protezione dei dati personali. Un'impresa che controlla il trattamento dei dati personali in imprese a essa collegate dovrebbe essere considerata, unitamente a tali imprese, quale «gruppo imprenditoriale».

(38) I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. Il consenso del titolare della responsabilità genitoriale non dovrebbe essere necessario nel quadro dei servizi di prevenzione o di consulenza forniti direttamente a un minore.

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

(40) Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri, come indicato nel presente regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della

necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso.

(41) Qualora il presente regolamento faccia riferimento 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 base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea (la «Corte di giustizia») e della Corte europea dei diritti dell'uomo.

(42) Per i trattamenti basati sul consenso dell'interessato, il titolare del trattamento dovrebbe essere in grado di dimostrare che l'interessato ha acconsentito al trattamento. In particolare, nel contesto di una dichiarazione scritta relativa a un'altra questione dovrebbero esistere garanzie che assicurino che l'interessato sia consapevole del fatto di prestare un consenso e della misura in cui ciò avviene. In conformità della direttiva 93/13/CEE del Consiglio (10) è opportuno prevedere una dichiarazione di consenso predisposta dal titolare del trattamento in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive. Ai fini di un consenso informato, l'interessato dovrebbe essere posto a conoscenza almeno dell'identità del titolare del trattamento e delle finalità del trattamento cui sono destinati i dati personali. Il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.

(43) Per assicurare la libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

(44) Il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.

(45) È opportuno che il trattamento effettuato in conformità a un obbligo legale al quale il titolare del trattamento è soggetto o necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri sia basato sul diritto dell'Unione o di uno Stato membro. Il presente regolamento non impone che vi sia un atto legislativo specifico per ogni singolo trattamento. Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo giuridico cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento. Inoltre, tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali,

prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto. Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale.

(46) Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

(47) I legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati personali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento. Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto.

(48) I titolari del trattamento facenti parte di un gruppo imprenditoriale o di enti collegati a un organismo centrale possono avere un interesse legittimo a trasmettere dati personali all'interno del gruppo imprenditoriale a fini amministrativi interni, compreso il trattamento di dati personali dei clienti o dei dipendenti. Sono fatti salvi i principi generali per il trasferimento di dati personali, all'interno di un gruppo imprenditoriale, verso un'impresa situata in un paese terzo.

(49) Costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano

la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERT), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza. Ciò potrebbe, ad esempio, includere misure atte a impedire l'accesso non autorizzato a reti di comunicazioni elettroniche e la diffusione di codici maligni, e a porre termine agli attacchi da «blocco di servizio» e ai danni ai sistemi informatici e di comunicazione elettronica.

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

Ove l'interessato abbia prestato il suo consenso o il trattamento si basi sul diritto dell'Unione o degli Stati membri che costituisce una misura necessaria e proporzionata in una società democratica per salvaguardare, in particolare, importanti obiettivi di interesse pubblico generale, il titolare del trattamento dovrebbe poter sottoporre i dati personali a ulteriore trattamento a prescindere dalla compatibilità delle finalità. In ogni caso, dovrebbe essere garantita l'applicazione dei principi stabiliti dal presente regolamento, in particolare l'obbligo di informare l'interessato di tali altre finalità e dei suoi diritti, compreso il diritto di opporsi. L'indicazione da parte del titolare del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati personali pertinenti a un'autorità competente in singoli casi o in più casi riguardanti lo stesso reato o la stessa minaccia alla sicurezza pubblica dovrebbero essere considerate nell'interesse legittimo perseguito dal titolare del trattamento. Tuttavia, tale trasmissione nell'interesse legittimo del titolare del trattamento o l'ulteriore trattamento dei dati personali dovrebbero essere vietati se il trattamento non è compatibile con un obbligo vincolante di segretezza, di natura giuridica, professionale o di altro genere.

(51) Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali. Tra tali dati personali dovrebbero essere compresi anche i dati personali che rivelano l'origine razziale o etnica, essendo inteso che l'utilizzo dei termini «origine razziale» nel presente regolamento non implica l'accettazione da parte dell'Unione di teorie che tentano di dimostrare l'esistenza di razze umane

distinte. Il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica. Tali dati personali non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito nei casi specifici di cui al presente regolamento, tenendo conto del fatto che il diritto degli Stati membri può stabilire disposizioni specifiche sulla protezione dei dati per adeguare l'applicazione delle norme del presente regolamento ai fini della conformità a un obbligo legale o dell'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Oltre ai requisiti specifici per tale trattamento, dovrebbero applicarsi i principi generali e altre norme del presente regolamento, in particolare per quanto riguarda le condizioni per il trattamento lecito. È opportuno prevedere espressamente deroghe al divieto generale di trattare tali categorie particolari di dati personali, tra l'altro se l'interessato esprime un consenso esplicito o in relazione a esigenze specifiche, in particolare se il trattamento è eseguito nel corso di legittime attività di talune associazioni o fondazioni il cui scopo sia permettere l'esercizio delle libertà fondamentali.

(52) La deroga al divieto di trattare categorie particolari di dati personali dovrebbe essere consentita anche quando è prevista dal diritto dell'Unione o degli Stati membri, fatte salve adeguate garanzie, per proteggere i dati personali e altri diritti fondamentali, laddove ciò avvenga nell'interesse pubblico, in particolare il trattamento dei dati personali nel settore del diritto del lavoro e della protezione sociale, comprese le pensioni, e per finalità di sicurezza sanitaria, controllo e allerta, la prevenzione o il controllo di malattie trasmissibili e altre minacce gravi alla salute. Tale deroga può avere luogo per finalità inerenti alla salute, compresa la sanità pubblica e la gestione dei servizi di assistenza sanitaria, soprattutto al fine di assicurare la qualità e l'economicità delle procedure per soddisfare le richieste di prestazioni e servizi nell'ambito del regime di assicurazione sanitaria, o a fini di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici. La deroga dovrebbe anche consentire di trattare tali dati personali se necessario per accertare, esercitare o difendere un diritto, che sia in sede giudiziale, amministrativa o stragiudiziale.

(53) Le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società, in particolare nel contesto della gestione dei servizi e sistemi di assistenza sanitaria o sociale, compreso il trattamento di tali dati da parte della dirigenza e delle autorità sanitarie nazionali centrali a fini di controllo della qualità, informazione sulla gestione e supervisione nazionale e locale generale del sistema di assistenza sanitaria o sociale, nonché per garantire la continuità dell'assistenza sanitaria o sociale e dell'assistenza sanitaria transfrontaliera o per finalità di sicurezza sanitaria, controllo e allerta o a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale che deve perseguire un obiettivo di interesse pubblico, nonché per studi svolti nel pubblico interesse nell'ambito della sanità pubblica. Pertanto il presente regolamento dovrebbe prevedere condizioni armonizzate per il trattamento di categorie particolari di dati personali relativi alla salute in relazione a esigenze specifiche, in particolare qualora il trattamento di tali dati sia svolto da persone vincolate dal segreto professionale per talune finalità connesse alla salute. Il diritto dell'Unione o degli Stati membri dovrebbe prevedere misure specifiche e appropriate a protezione dei diritti fondamentali e dei dati personali delle persone fisiche. Gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre ulteriori condizioni, fra cui limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute, senza tuttavia ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi.

(54) Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. Tale trattamento dovrebbe essere soggetto a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche. In tale contesto, la nozione di «sanità pubblica» dovrebbe essere interpretata secondo la definizione del regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio (11): tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. Il trattamento dei dati relativi alla salute effettuato per motivi di interesse pubblico non dovrebbe comportare il trattamento dei dati personali per altre finalità da parte di terzi, quali datori di lavoro, compagnie di assicurazione e istituti di credito.

(55) Inoltre, è effettuato per motivi di interesse pubblico il trattamento di dati personali a cura di autorità pubbliche allo scopo di realizzare fini, previsti dal diritto costituzionale o dal diritto internazionale pubblico, di associazioni religiose ufficialmente riconosciute.

(56) Se, nel corso di attività elettorali, il funzionamento del sistema democratico presuppone, in uno Stato membro, che i partiti politici raccolgano dati personali sulle opinioni politiche delle persone, può esserne consentito il trattamento di tali dati per motivi di interesse pubblico, purché siano predisposte garanzie adeguate.

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

(58) Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.

(59) È opportuno prevedere modalità volte ad agevolare l'esercizio, da parte dell'interessato, dei diritti di cui al presente regolamento, compresi i meccanismi per richiedere e, se del caso, ottenere gratuitamente, in particolare l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione. Il titolare del trattamento dovrebbe predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi

elettronici. Il titolare del trattamento dovrebbe essere tenuto a rispondere alle richieste dell'interessato senza ingiustificato ritardo e al più tardi entro un mese e a motivare la sua eventuale intenzione di non accogliere tali richieste.

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

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

(62) Per contro, non è necessario imporre l'obbligo di fornire l'informazione se l'interessato dispone già dell'informazione, se la registrazione o la comunicazione dei dati personali sono previste per legge o se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato. Quest'ultima eventualità potrebbe verificarsi, ad esempio, nei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi si può tener conto del numero di interessati, dell'antichità dei dati e di eventuali garanzie adeguate in essere.

(63) Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non

dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce.

(64) Il titolare del trattamento dovrebbe adottare tutte le misure ragionevoli per verificare l'identità di un interessato che chieda l'accesso, in particolare nel contesto di servizi online e di identificativi online. Il titolare del trattamento non dovrebbe conservare dati personali al solo scopo di poter rispondere a potenziali richieste.

(65) Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che lo riguardano e il «diritto all'oblio» se la conservazione di tali dati violi il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia revocato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.

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

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

(68) Per rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un

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

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

(70) Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato dovrebbe avere il diritto, in qualsiasi momento e gratuitamente, di opporsi a tale trattamento, con riguardo sia a quello iniziale che a quello ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto dovrebbe essere esplicitamente portato all'attenzione dell'interessato e presentato chiaramente e separatamente da qualsiasi altra informazione.

(71) L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni

sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione. Tale misura non dovrebbe riguardare un minore.

Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti.. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni.

(72) La profilazione è soggetta alle norme del presente regolamento che disciplinano il trattamento dei dati personali, quali i fondamenti giuridici del trattamento o i principi di protezione dei dati. Il comitato europeo per la protezione dei dati istituito dal presente regolamento («comitato») dovrebbe poter emanare orientamenti in tale contesto.

(73) Il diritto dell'Unione o degli Stati membri può imporre limitazioni a specifici principi e ai diritti di informazione, accesso, rettifica e cancellazione di dati, al diritto alla portabilità dei dati, al diritto di opporsi, alle decisioni basate sulla profilazione, nonché alla comunicazione di una violazione di dati personali all'interessato e ad alcuni obblighi connessi in capo ai titolari del trattamento, ove ciò sia necessario e proporzionato in una società democratica per la salvaguardia della sicurezza pubblica, ivi comprese la tutela della vita umana, in particolare in risposta a catastrofi di origine naturale o umana, le attività di prevenzione, indagine e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, o di violazioni della deontologia professionale, per la tutela di altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, tra cui un interesse economico o finanziario rilevante dell'Unione o di uno Stato membro, per la tenuta di registri pubblici per ragioni di interesse pubblico generale, per l'ulteriore trattamento di dati personali archiviati al fine di fornire informazioni specifiche connesse al comportamento politico sotto precedenti regimi statali totalitari o per la tutela dell'interessato o dei diritti e delle libertà altrui, compresi la protezione sociale, la sanità pubblica e gli scopi umanitari. Tali limitazioni dovrebbero essere conformi alla Carta e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

(74) È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a

mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

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

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

(77) Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio.

(78) La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita..Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che

trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici..

(79) La protezione 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 controllo e alle misure delle autorità di controllo, esigono una chiara ripartizione delle responsabilità ai sensi del presente regolamento, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento o quando l'operazione di trattamento viene eseguita per conto del titolare del trattamento.

(80) Quando un titolare del trattamento o un responsabile del trattamento non stabilito nell'Unione tratta dati personali di interessati che si trovano nell'Unione e le sue attività di trattamento sono connesse all'offerta di beni o alla prestazione di servizi a tali interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, o al controllo del loro comportamento, nella misura in cui tale comportamento ha luogo all'interno dell'Unione, è opportuno che tale titolare del trattamento o responsabile del trattamento designi un rappresentante, tranne se il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati personali o il trattamento di dati personali relativi alle condanne penali e ai reati, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento, o se il titolare del trattamento è un'autorità pubblica o un organismo pubblico. Il rappresentante dovrebbe agire per conto del titolare del trattamento o del responsabile del trattamento e può essere interpellato da qualsiasi autorità di controllo. Il rappresentante dovrebbe essere esplicitamente designato mediante mandato scritto del titolare del trattamento o del responsabile del trattamento ad agire per conto di questi ultimi con riguardo agli obblighi che a questi derivano dal presente regolamento. La designazione di tale rappresentante non incide sulla responsabilità generale del titolare del trattamento o del responsabile del trattamento ai sensi del presente regolamento. Tale rappresentante dovrebbe svolgere i suoi compiti nel rispetto del mandato conferitogli dal titolare del trattamento o dal responsabile del trattamento, anche per quanto riguarda la cooperazione con le autorità di controllo competenti per qualsiasi misura adottata al fine di garantire il rispetto del presente regolamento. Il rappresentante designato dovrebbe essere oggetto di misure attuative in caso di inadempienza da parte del titolare del trattamento o del responsabile del trattamento.

(81) Per garantire che siano rispettate le prescrizioni del presente regolamento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento il titolare del trattamento dovrebbe ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del presente regolamento, anche per la sicurezza del trattamento. L'applicazione da parte del responsabile del trattamento di un codice di condotta approvato o di un meccanismo di certificazione approvato può essere utilizzata come elemento per dimostrare il rispetto degli obblighi da parte del titolare del trattamento. L'esecuzione dei trattamenti da parte di un responsabile del trattamento dovrebbe

essere disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincoli il responsabile del trattamento al titolare del trattamento, in cui siano stipulati la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, tenendo conto dei compiti e responsabilità specifici del responsabile del trattamento nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato. Il titolare del trattamento e il responsabile del trattamento possono scegliere di usare un contratto individuale o clausole contrattuali tipo che sono adottate direttamente dalla Commissione oppure da un'autorità di controllo in conformità del meccanismo di coerenza e successivamente dalla Commissione. Dopo il completamento del trattamento per conto del titolare del trattamento, il responsabile del trattamento dovrebbe, a scelta del titolare del trattamento, restituire o cancellare i dati personali salvo che il diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento prescriva la conservazione dei dati personali.

(82) Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per controllare detti trattamenti.

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

(84) Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio. L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento. Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che il titolare del trattamento non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'autorità di controllo.

(85) 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.

(86) Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

(87) È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

(88) Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

(89) La direttiva 95/46/CE ha introdotto un obbligo generale di notificare alle autorità di controllo il trattamento dei dati personali. Mentre tale obbligo comporta oneri amministrativi e finanziari, non ha sempre contribuito a migliorare la protezione dei dati personali. È pertanto opportuno abolire tali obblighi generali e indiscriminati di notifica e sostituirli con meccanismi e procedure efficaci che si concentrino piuttosto su quei tipi di trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per loro natura, ambito di applicazione, contesto e finalità. Tali tipi di trattamenti includono, in particolare, quelli che comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione

d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale.

(90) In tali casi, è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio. La valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento.

(91) Ciò dovrebbe applicarsi in particolare ai trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. È opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza. Una valutazione d'impatto sulla protezione dei dati è altresì richiesta per la sorveglianza di zone accessibili al pubblico su larga scala, in particolare se effettuata mediante dispositivi optoelettronici, o per altri trattamenti che l'autorità di controllo competente ritiene possano presentare un rischio elevato per i diritti e le libertà degli interessati, specialmente perché impediscono a questi ultimi di esercitare un diritto o di avvalersi di un servizio o di un contratto, oppure perché sono effettuati sistematicamente su larga scala. Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato. In tali casi non dovrebbe essere obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati.

(92) Vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata.

(93) In vista dell'adozione della legge degli Stati membri che disciplina i compiti dell'autorità pubblica o dell'organismo pubblico e lo specifico trattamento o insieme di trattamenti, gli Stati membri possono ritenere necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

(94) Se dalla valutazione d'impatto sulla protezione dei dati risulta che il trattamento, in mancanza delle garanzie, delle misure di sicurezza e dei meccanismi per attenuare il rischio, presenterebbe un rischio elevato per i diritti e le libertà delle persone fisiche e il titolare del trattamento è del

parere che il rischio non possa essere ragionevolmente attenuato in termini di tecnologie disponibili e costi di attuazione, è opportuno consultare l'autorità di controllo prima dell'inizio delle attività di trattamento. Tale rischio elevato potrebbe scaturire da certi tipi di trattamento e dall'estensione e frequenza del trattamento, da cui potrebbe derivare altresì un danno o un'interferenza con i diritti e le libertà della persona fisica. L'autorità di controllo che riceve una richiesta di consultazione dovrebbe darvi seguito entro un termine determinato. Tuttavia, la mancanza di reazione dell'autorità di controllo entro tale termine dovrebbe far salvo ogni intervento della stessa nell'ambito dei suoi compiti e poteri previsti dal presente regolamento, compreso il potere di vietare i trattamenti. Nell'ambito di tale processo di consultazione, può essere presentato all'autorità di controllo il risultato di una valutazione d'impatto sulla protezione dei dati effettuata riguardo al trattamento in questione, in particolare le misure previste per attenuare il rischio per i diritti e le libertà delle persone fisiche.

(95) Il responsabile del trattamento, se necessario e su richiesta, dovrebbe assistere il titolare del trattamento nel garantire il rispetto degli obblighi derivanti dallo svolgimento di una valutazione d'impatto sulla protezione dei dati e dalla previa consultazione dell'autorità di controllo.

(96) L'autorità di controllo dovrebbe essere altresì consultata durante l'elaborazione di una misura legislativa o regolamentare che prevede il trattamento di dati personali al fine di garantire che il trattamento previsto rispetti il presente regolamento e, in particolare, che si attenui il rischio per l'interessato.

(97) Per i trattamenti effettuati da un'autorità pubblica, eccettuate le autorità giurisdizionali o autorità giudiziarie indipendenti quando esercitano le loro funzioni giurisdizionali, o per i trattamenti effettuati nel settore privato da un titolare del trattamento le cui attività principali consistono in trattamenti che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala, o ove le attività principali del titolare del trattamento o del responsabile del trattamento consistano nel trattamento su larga scala di categorie particolari di dati personali e di dati relativi alle condanne penali e ai reati, il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. Nel settore privato le attività principali del titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria. Il livello necessario di conoscenza specialistica dovrebbe essere determinato in particolare in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento. Tali responsabili della protezione dei dati, dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente.

(98) Le associazioni o altre organizzazioni rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento dovrebbero essere incoraggiate a elaborare codici di condotta, nei limiti del presente regolamento, in modo da facilitarne l'effettiva applicazione, tenendo conto delle caratteristiche specifiche dei trattamenti effettuati in alcuni settori e delle esigenze specifiche delle microimprese e delle piccole e medie imprese. In particolare, tali codici di condotta potrebbero calibrare gli obblighi dei titolari del trattamento e dei responsabili del trattamento, tenuto conto del potenziale rischio del trattamento per i diritti e le libertà delle persone fisiche.

(99) Nell'elaborare un codice di condotta, o nel modificare o prorogare tale codice, le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento dovrebbero consultare le parti interessate pertinenti, compresi, quando possibile, gli interessati, e tener conto delle osservazioni ricevute e delle opinioni espresse in riscontro a tali consultazioni.

(100) Al fine di migliorare la trasparenza e il rispetto del presente regolamento dovrebbe essere incoraggiata l'istituzione di meccanismi di certificazione e sigilli nonché marchi di protezione dei dati che consentano agli interessati di valutare rapidamente il livello di protezione dei dati dei relativi prodotti e servizi.

(101) I flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. È opportuno però che, quando i dati personali sono trasferiti dall'Unione a titolari del trattamento e responsabili del trattamento o altri destinatari in paesi terzi o a organizzazioni internazionali, il livello di tutela delle persone fisiche assicurato nell'Unione dal presente regolamento non sia compromesso, anche nei casi di trasferimenti successivi dei dati personali dal paese terzo o dall'organizzazione internazionale verso titolari del trattamento e responsabili del trattamento nello stesso o in un altro paese terzo o presso un'altra organizzazione internazionale. In ogni caso, i trasferimenti verso paesi terzi e organizzazioni internazionali potrebbero essere effettuati soltanto nel pieno rispetto del presente regolamento. Il trasferimento potrebbe aver luogo soltanto se, fatte salve le altre disposizioni del presente regolamento, il titolare del trattamento o il responsabile del trattamento rispetta le condizioni stabilite dalle disposizioni del presente regolamento in relazione al trasferimento di dati personali verso paesi terzi o organizzazioni internazionali.

(102) Il presente regolamento lascia impregiudicate le disposizioni degli accordi internazionali conclusi tra l'Unione e i paesi terzi che disciplinano il trasferimento di dati personali, comprese adeguate garanzie per gli interessati. Gli Stati membri possono concludere accordi internazionali che implicano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, purché tali accordi non incidano sul presente regolamento o su qualsiasi altra disposizione del diritto dell'Unione e includano un adeguato livello di protezione per i diritti fondamentali degli interessati.

(103) La Commissione può decidere, con effetto nell'intera Unione, che un paese terzo, un territorio o un settore specifico 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 del paese terzo o dell'organizzazione internazionale che si ritiene offra tale livello di protezione. In tali casi, i trasferimenti di dati personali verso tale paese terzo od organizzazione internazionale possono avere luogo senza ulteriori autorizzazioni. La Commissione può inoltre decidere, dopo aver fornito una dichiarazione completa che illustra le motivazioni al paese terzo o all'organizzazione internazionale, di revocare una tale decisione.

(104) 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 del paese terzo, o di un territorio o di un settore specifico all'interno di un paese terzo, tenga conto del modo in cui tale paese rispetta lo stato di diritto, l'accesso alla giustizia e le norme e gli standard internazionali in

materia di diritti dell'uomo, 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 di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione, segnatamente quando i dati personali sono 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 giudiziale.

(105) Al di là degli impegni internazionali che il paese terzo o l'organizzazione internazionale hanno assunto, la Commissione dovrebbe tenere 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.

(106) 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, e controlli il funzionamento delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, o dell'articolo 26, paragrafo 4, della direttiva 95/46/CE.. Nella sua decisione di adeguatezza, la Commissione dovrebbe prevedere un meccanismo di riesame periodico del loro funzionamento. Tale riesame periodico dovrebbe essere effettuato 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. Ai fini del controllo e dello svolgimento dei riesami periodici, la Commissione dovrebbe tener conto delle posizioni e delle conclusioni del Parlamento europeo e del Consiglio, nonché di altri organismi e fonti pertinenti. La Commissione dovrebbe valutare, entro un termine ragionevole, il funzionamento di tali ultime decisioni e riferire eventuali riscontri pertinenti al comitato ai sensi del regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio (12), come stabilito a norma del presente regolamento, al Parlamento europeo e al Consiglio.

(107) La Commissione può riconoscere che un paese terzo, un territorio o un settore specifico all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello adeguato di protezione dei dati. Di conseguenza il trasferimento di dati personali verso tale paese terzo od organizzazione internazionale dovrebbe essere vietato, a meno che non siano soddisfatti i requisiti di cui al presente regolamento relativamente ai trasferimenti sottoposti a garanzie adeguate, comprese norme vincolanti d'impresa, e a deroghe per situazioni particolari. In tal caso è opportuno prevedere consultazioni 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.

(108) In mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento dovrebbe provvedere a compensare la carenza di protezione dei dati in un paese terzo con adeguate garanzie a tutela dell'interessato. Tali adeguate garanzie possono consistere nell'applicazione di norme vincolanti d'impresa, clausole tipo di protezione dei dati adottate dalla Commissione, clausole tipo di protezione dei dati adottate da un'autorità di controllo o clausole contrattuali autorizzate da un'autorità di controllo. Tali garanzie dovrebbero assicurare un rispetto dei requisiti in materia di protezione dei dati e dei diritti degli interessati adeguato ai trattamenti all'interno dell'Unione, compresa la disponibilità di diritti azionabili degli interessati e di mezzi di ricorso effettivi, fra cui il ricorso effettivo in sede amministrativa o giudiziale e la richiesta di risarcimento, nell'Unione o in un paese terzo. Esse dovrebbero riguardare, in particolare, la conformità rispetto ai principi generali in materia di trattamento dei dati personali e ai principi di protezione dei dati fin dalla progettazione e di protezione dei dati per impostazione predefinita. I trasferimenti possono essere effettuati anche da autorità pubbliche o organismi pubblici ad autorità pubbliche o organismi pubblici di paesi terzi, o organizzazioni internazionali con analoghi compiti o funzioni, anche sulla base di disposizioni da inserire in accordi amministrativi, quali un memorandum d'intesa, che prevedano per gli interessati diritti effettivi e azionabili. L'autorizzazione dell'autorità di controllo competente dovrebbe essere ottenuta quando le garanzie sono offerte nell'ambito di accordi amministrativi giuridicamente non vincolanti.

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

(110) Un gruppo imprenditoriale o un gruppo di imprese che svolge un'attività economica comune dovrebbe poter applicare le norme vincolanti d'impresa approvate per i trasferimenti internazionali dall'Unione agli organismi dello stesso gruppo imprenditoriale o gruppo d'imprese che svolge un'attività economica comune, purché tali norme contemplino tutti i principi fondamentali e diritti azionabili che costituiscano adeguate garanzie per i trasferimenti o categorie di trasferimenti di dati personali.

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

(112) Tali deroghe dovrebbero in particolare valere per i trasferimenti di dati richiesti e necessari per importanti motivi di interesse pubblico, ad esempio nel caso di scambio internazionale di dati tra autorità garanti della concorrenza, amministrazioni fiscali o doganali, autorità di controllo finanziario, servizi competenti in materia di sicurezza sociale o sanità pubblica, ad esempio in caso di ricerca di contatti per malattie contagiose o al fine di ridurre e/o eliminare il doping nello sport. Il trasferimento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per salvaguardare un interesse che è essenziale per gli interessi vitali dell'interessato o di un'altra persona, comprese la vita o l'integrità fisica, qualora l'interessato si trovi nell'incapacità di prestare il proprio consenso. In mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri dovrebbero notificare tali disposizioni alla Commissione. Qualunque trasferimento a un'organizzazione internazionale umanitaria di dati personali di un interessato che si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso ai fini dell'esecuzione di un compito derivante dalle convenzioni di Ginevra o al fine di rispettare il diritto internazionale umanitario applicabile nei conflitti armati potrebbe essere considerato necessario per importanti motivi di interesse pubblico o nell'interesse vitale dell'interessato.

(113) Potrebbero altresì essere autorizzati i trasferimenti qualificabili come non ripetitivi e riguardanti soltanto un numero limitato di interessati ai fini del perseguimento degli interessi legittimi cogenti del titolare del trattamento, a meno che non prevalgano gli interessi o i diritti e le libertà dell'interessato e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento. Il titolare del trattamento dovrebbe considerare con particolare attenzione la natura dei dati personali, la finalità e la durata del trattamento o dei trattamenti proposti, nonché la situazione nel paese d'origine, nel paese terzo e nel paese di destinazione finale, e dovrebbe offrire garanzie adeguate per la tutela dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei loro dati personali. Tali trasferimenti dovrebbero essere ammessi soltanto nei casi residui in cui nessuno degli altri presupposti per il trasferimento è applicabile. Per finalità di ricerca scientifica o storica o a fini statistici, è opportuno tener conto delle legittime aspettative della società nei confronti di un miglioramento delle conoscenze. Il titolare del trattamento dovrebbe informare l'autorità di controllo e l'interessato in merito al trasferimento.

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

(115) Alcuni paesi terzi adottano leggi, regolamenti e altri atti normativi finalizzati a disciplinare direttamente le attività di trattamento di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. Essi possono includere le sentenze di autorità giurisdizionali o le decisioni di autorità amministrative di paesi terzi che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento e non sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria. L'applicazione extraterritoriale di tali leggi, regolamenti e altri atti normativi potrebbe essere contraria al diritto internazionale e ostacolare il conseguimento della protezione delle persone fisiche assicurata nell'Unione con il presente regolamento. I trasferimenti dovrebbero quindi essere consentiti solo se

ricorrono le condizioni previste dal presente regolamento per i trasferimenti a paesi terzi. Ciò vale, tra l'altro, quando la comunicazione è necessaria per un rilevante motivo di interesse pubblico riconosciuto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento.

(116) Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo 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 dall'insufficienza di poteri per prevenire e correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. Pertanto vi è la necessità di promuovere una più stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni e condurre indagini di concerto con le loro controparti internazionali. Al fine di sviluppare meccanismi di cooperazione internazionale per agevolare e prestare mutua assistenza a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali, la Commissione e le autorità di controllo dovrebbero scambiare informazioni e cooperare, nell'ambito di attività connesse con l'esercizio dei loro poteri, con le autorità competenti in paesi terzi, sulla base della reciprocità e in conformità del presente regolamento.

(117) L'istituzione di autorità di controllo a cui è conferito il potere di eseguire i loro compiti ed esercitare i loro poteri in totale indipendenza in ciascuno Stato membro è un elemento essenziale della protezione delle persone fisiche con riguardo al trattamento dei loro dati personali. Gli Stati membri dovrebbero poter istituire più di una autorità di controllo, al fine di rispecchiare la loro struttura costituzionale, organizzativa e amministrativa.

(118) L'indipendenza delle autorità di controllo non dovrebbe significare che tali autorità non possano essere assoggettate a meccanismi di controllo o monitoraggio con riguardo alle loro spese o a controllo giurisdizionale.

(119) Laddove siano istituite più autorità di controllo, lo Stato membro dovrebbe stabilire per legge meccanismi atti ad assicurare la partecipazione effettiva di dette autorità al meccanismo di coerenza. Lo Stato membro dovrebbe in particolare designare l'autorità di controllo che funge da punto di contatto unico per l'effettiva partecipazione di tutte le autorità al meccanismo, onde garantire la rapida e agevole cooperazione con altre autorità di controllo, il comitato e la Commissione.

(120) 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 quelli 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.

(121) Le condizioni generali applicabili al membro o ai membri dell'autorità di controllo dovrebbero essere stabilite per legge da ciascuno Stato membro e dovrebbero in particolare prevedere che tali membri devono essere nominati, attraverso una procedura trasparente, dal parlamento, dal

governo o dal capo di Stato dello Stato membro, sulla base di una proposta del governo, di un membro del governo, del parlamento o di una sua camera, o da un organismo indipendente incaricato ai sensi del diritto degli Stati membri. 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 incompatibile, remunerata o meno. L'autorità di controllo dovrebbe disporre di proprio personale, scelto dalla stessa autorità di controllo o da un organismo indipendente istituito ai sensi del diritto degli Stati membri, che dovrebbe essere soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo.

(122) Ogni autorità di controllo dovrebbe avere la competenza, nel territorio del proprio Stato membro, a esercitare i poteri e ad assolvere i compiti a essa attribuiti a norma del presente regolamento. Ciò dovrebbe comprendere in particolare il trattamento nell'ambito delle attività di uno stabilimento del titolare del trattamento o del responsabile del trattamento sul territorio del proprio Stato membro, il trattamento di dati personali effettuato dalle pubbliche autorità o dagli organismi privati che agiscono nel pubblico interesse, il trattamento riguardante gli interessati nel suo territorio o il trattamento effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione europea riguardante interessati residenti nel suo territorio. Ciò dovrebbe includere l'esame dei reclami proposti dall'interessato, lo svolgimento di indagini sull'applicazione del regolamento e la promozione della sensibilizzazione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali.

(123) Le autorità di controllo dovrebbero controllare l'applicazione delle disposizioni del presente regolamento e contribuire alla sua coerente applicazione in tutta l'Unione, così da tutelare le persone fisiche in relazione al trattamento dei loro dati personali e facilitare la libera circolazione di tali dati nel mercato interno. A tal fine, le autorità di controllo dovrebbero cooperare tra loro e con la Commissione, senza che siano necessari accordi tra gli Stati membri sulla mutua assistenza o su tale tipo di cooperazione.

(124) Qualora il trattamento dei dati personali abbia luogo nell'ambito delle attività di uno stabilimento di un titolare del trattamento o di un responsabile del trattamento nell'Unione e il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro o qualora il trattamento effettuato nell'ambito delle attività dello stabilimento unico di un titolare del trattamento o responsabile del trattamento nell'Unione incida o possa verosimilmente incidere in modo sostanziale su interessati in più di uno Stato membro, l'autorità di controllo dello stabilimento principale del titolare del trattamento o del responsabile del trattamento o dello stabilimento unico del titolare del trattamento o del responsabile del trattamento dovrebbe fungere da autorità capofila. Essa dovrebbe cooperare con le altre autorità interessate perché il titolare del trattamento o il responsabile del trattamento ha uno stabilimento nel territorio dei loro Stati membri, perché il trattamento incide in modo sostanziale sugli interessati residenti nel loro territorio o perché è stato proposto loro un reclamo. Anche in caso di reclamo proposto da un interessato non residente in tale Stato membro, l'autorità di controllo cui è stato proposto detto reclamo dovrebbe essere considerata un'autorità di controllo interessata. Nell'ambito del suo compito di rilascio di linee guida su qualsiasi questione relativa all'applicazione del presente regolamento, il comitato dovrebbe essere in grado di pubblicare linee guida in particolare sui criteri da prendere in considerazione per accertare se il trattamento in questione incida in modo sostanziale su interessati in più di uno Stato membro e su cosa costituisca obiezione pertinente e motivata.

(125) L'autorità capofila dovrebbe essere competente per l'adozione di decisioni vincolanti riguardanti misure di applicazione dei poteri di cui gode a norma del presente regolamento. Nella sua qualità di autorità capofila, l'autorità di controllo dovrebbe coinvolgere e coordinare strettamente le autorità di controllo interessate nel processo decisionale. In caso di decisione di rigetto del reclamo dell'interessato, in tutto o in parte, tale decisione dovrebbe essere adottata dall'autorità di controllo a cui il reclamo è stato proposto.

(126) La decisione dovrebbe essere adottata congiuntamente dall'autorità di controllo capofila e dalle autorità di controllo interessate e dovrebbe essere rivolta allo stabilimento principale o unico del titolare del trattamento o del responsabile del trattamento ed essere vincolante per il titolare del trattamento e il responsabile del trattamento. Il titolare del trattamento o il responsabile del trattamento dovrebbe adottare le misure necessarie per garantire la conformità al presente regolamento e l'attuazione della decisione notificata dall'autorità di controllo capofila allo stabilimento principale del titolare del trattamento o del responsabile del trattamento per quanto riguarda le attività di trattamento nell'Unione.

(127) Ogni autorità di controllo che non agisce in qualità di autorità di controllo capofila dovrebbe essere competente a trattare casi locali qualora il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro, ma l'oggetto dello specifico trattamento riguardi unicamente il trattamento effettuato in un singolo Stato membro e coinvolga soltanto interessati in tale singolo Stato membro, ad esempio quando l'oggetto riguardi il trattamento di dati personali di dipendenti nell'ambito di specifici rapporti di lavoro in uno Stato membro. In tali casi, l'autorità di controllo dovrebbe informare senza ritardo l'autorità di controllo capofila sulla questione. Dopo essere stata informata, l'autorità di controllo capofila dovrebbe decidere se intende trattare il caso a norma della disposizione sulla cooperazione tra l'autorità di controllo capofila e altre autorità di controllo interessate («meccanismo dello sportello unico»), ovvero se l'autorità di controllo che l'ha informata debba trattarlo a livello locale. Al momento di decidere se intende trattare il caso, l'autorità di controllo capofila dovrebbe tenere conto dell'eventuale esistenza, nello Stato membro dell'autorità di controllo che l'ha informata, di uno stabilimento del titolare del trattamento o del responsabile del trattamento, al fine di garantire l'effettiva applicazione di una decisione nei confronti del titolare del trattamento o del responsabile del trattamento. Qualora l'autorità di controllo capofila decida di trattare il caso, l'autorità di controllo che l'ha informata dovrebbe avere la possibilità di presentare un progetto di decisione, che l'autorità di controllo capofila dovrebbe tenere nella massima considerazione nella preparazione del proprio progetto di decisione nell'ambito di tale meccanismo di sportello unico.

(128) Le norme sull'autorità di controllo capofila e sul meccanismo di sportello unico non dovrebbero applicarsi quando il trattamento è effettuato da autorità pubbliche o da organismi privati nell'interesse pubblico. In tali casi l'unica autorità di controllo competente a esercitare i poteri a essa conferiti a norma del presente regolamento dovrebbe essere l'autorità di controllo dello Stato membro in cui l'autorità pubblica o l'organismo privato sono stabiliti.

(129) Al fine di garantire un monitoraggio e un'applicazione coerenti del presente regolamento in tutta l'Unione, le autorità di controllo dovrebbero avere in ciascuno Stato membro gli stessi compiti e poteri effettivi, fra cui poteri di indagine, poteri correttivi e sanzionatori, e poteri autorizzativi e consultivi, segnatamente in caso di reclamo proposto da persone fisiche, e fatti salvi i poteri delle autorità preposte all'esercizio dell'azione penale ai sensi del diritto degli Stati membri, il potere di intentare un'azione e di agire in sede giudiziale o stragiudiziale in caso di violazione del presente

regolamento. Tali poteri dovrebbero includere anche il potere di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento. Gli Stati membri possono precisare altri compiti connessi alla protezione dei dati personali ai sensi del presente regolamento. È opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e degli Stati membri, 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 al presente regolamento, tenuto conto delle circostanze di ciascun singolo caso, rispettare il diritto di ogni persona di essere ascoltata prima che nei suoi confronti sia adottato un provvedimento individuale che le rechi pregiudizio ed evitare costi superflui ed eccessivi disagi per le persone interessate. I poteri di indagine per quanto riguarda l'accesso ai locali dovrebbero essere esercitati nel rispetto dei requisiti specifici previsti dal diritto processuale degli Stati membri, quale l'obbligo di ottenere un'autorizzazione giudiziaria preliminare. Ogni misura giuridicamente vincolante dell'autorità di controllo dovrebbe avere forma scritta, essere chiara e univoca, riportare l'autorità di controllo che ha adottato la misura e la relativa data di adozione, recare la firma del responsabile o di un membro dell'autorità di controllo da lui autorizzata, precisare i motivi della misura e fare riferimento al diritto a un ricorso effettivo. Ciò non dovrebbe precludere requisiti supplementari ai sensi del diritto processuale degli Stati membri. L'adozione di una decisione giuridicamente vincolante implica che essa può essere soggetta a controllo giurisdizionale nello Stato membro dell'autorità di controllo che ha adottato la decisione.

(130) Qualora l'autorità di controllo cui sia stato proposto il reclamo non sia l'autorità di controllo capofila, l'autorità di controllo capofila dovrebbe cooperare strettamente con l'autorità di controllo cui è stato proposto il reclamo in conformità delle disposizioni sulla cooperazione e la coerenza previste dal presente regolamento. In tali casi, l'autorità di controllo capofila, nell'adottare le misure intese a produrre effetti giuridici, compresa l'imposizione di sanzioni amministrative pecuniarie, dovrebbe tenere nella massima considerazione il parere dell'autorità di controllo cui è stato proposto il reclamo e che dovrebbe rimanere competente per svolgere indagini nel territorio del proprio Stato membro in collegamento con l'autorità di controllo capofila.

(131) Qualora un'altra autorità di controllo agisca in qualità di autorità di controllo capofila per le attività di trattamento del titolare del trattamento o del responsabile del trattamento, ma il concreto oggetto di un reclamo o la possibile violazione riguardi solo attività di trattamento del titolare del trattamento o del responsabile del trattamento nello Stato membro di presentazione del reclamo o di accertamento della possibile violazione e la questione non incida in modo sostanziale o è improbabile che incida in modo sostanziale su interessati in altri Stati membri, l'autorità di controllo che riceva un reclamo o che accerti o sia altrimenti informata di situazioni che implicano possibili violazioni del regolamento dovrebbe tentare una composizione amichevole con il titolare del trattamento e, qualora ciò non abbia esito, esercitare l'intera sua gamma di poteri. Ciò dovrebbe includere: il trattamento specifico effettuato nel territorio dello Stato membro dell'autorità di controllo o con riguardo agli interessati nel territorio di tale Stato membro; il trattamento effettuato nell'ambito di un'offerta di beni o prestazione di servizi specificamente riguardante gli interessati nel territorio dello Stato membro dell'autorità di controllo; o il trattamento che deve essere oggetto di valutazione tenuto conto dei pertinenti obblighi giuridici ai sensi della legislazione degli Stati membri.

(132) Le attività di sensibilizzazione delle autorità di controllo nei confronti del pubblico dovrebbero comprendere misure specifiche per i titolari del trattamento e i responsabili del trattamento,

comprese le micro, piccole e medie imprese, e le persone fisiche in particolare nel contesto educativo.

(133) Le autorità di controllo dovrebbero prestarsi assistenza reciproca nell'adempimento dei loro compiti, in modo da garantire la coerente applicazione e attuazione del presente regolamento nel mercato interno. L'autorità di controllo che chiede assistenza reciproca può adottare una misura provvisoria in caso di mancato riscontro a una richiesta di assistenza reciproca entro un mese dal ricevimento di tale richiesta da parte dell'altra autorità di controllo.

(134) Ciascuna autorità di controllo dovrebbe, se del caso, partecipare alle operazioni congiunte con altre autorità di controllo. L'autorità di controllo che riceve una richiesta dovrebbe darvi seguito entro un termine determinato.

(135) È opportuno istituire un meccanismo di coerenza per la cooperazione tra le autorità di controllo, al fine di assicurare un'applicazione coerente del presente regolamento in tutta l'Unione. Tale meccanismo dovrebbe applicarsi in particolare quando un'autorità di controllo intenda adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di trattamento che incidono in modo sostanziale su un numero significativo di interessati in vari Stati membri. È opportuno che il meccanismo si attivi anche quando un'autorità di controllo interessata o la Commissione chiede che tale questione sia trattata nell'ambito del meccanismo di coerenza. Tale meccanismo non dovrebbe pregiudicare le misure che la Commissione può adottare nell'esercizio dei suoi poteri a norma dei trattati.

(136) In applicazione del meccanismo di coerenza il comitato dovrebbe emettere un parere entro un termine determinato, se i suoi membri lo decidono a maggioranza o se a richiederlo è un'autorità di controllo interessata o la Commissione. Il comitato dovrebbe altresì avere il potere di adottare decisioni giuridicamente vincolanti qualora insorgano controversie tra autorità di controllo. A tal fine, dovrebbe adottare, in linea di principio a maggioranza dei due terzi dei suoi membri, decisioni giuridicamente vincolanti in casi chiaramente determinati in cui vi siano pareri divergenti tra le autorità di controllo segnatamente nell'ambito del meccanismo di cooperazione tra l'autorità di controllo capofila e le autorità di controllo interessate sul merito del caso, in particolare sulla sussistenza di una violazione del presente regolamento.

(137) Potrebbe essere necessario intervenire urgentemente per tutelare i diritti e le libertà degli interessati, in particolare quando sussiste il pericolo che l'esercizio di un diritto possa essere gravemente ostacolato. Un'autorità di controllo potrebbe pertanto essere in grado di adottare misure provvisorie debitamente giustificate nel proprio territorio, con un periodo di validità determinato che non dovrebbe superare tre mesi.

(138) L'applicazione di tale meccanismo dovrebbe essere un presupposto di liceità di una misura intesa a produrre effetti giuridici adottata dall'autorità di controllo nei casi in cui la sua applicazione è obbligatoria. In altri casi di rilevanza transfrontaliera, si dovrebbe applicare il meccanismo di cooperazione tra autorità di controllo capofila e autorità di controllo interessate e le autorità di controllo interessate potrebbero prestarsi assistenza reciproca ed effettuare operazioni congiunte, su base bilaterale o multilaterale, senza attivare il meccanismo di coerenza.

(139) Per promuovere l'applicazione coerente del presente regolamento, il comitato dovrebbe essere istituito come un organismo indipendente dell'Unione. Per conseguire i suoi obiettivi, il comitato dovrebbe essere dotato di personalità giuridica. Il comitato dovrebbe essere rappresentato dal suo presidente. Esso dovrebbe sostituire il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito con direttiva 95/46/CE. Il comitato dovrebbe essere composto dalla figura di vertice dell'autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti. È opportuno che la Commissione partecipi alle attività del comitato senza diritto di voto e che il garante europeo della protezione dei dati abbia diritti di voto specifici. Il comitato dovrebbe contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, anche fornendo consulenza alla Commissione, in particolare sul livello di protezione garantito dai paesi terzi o dalle organizzazioni internazionali, e promuovendo la cooperazione delle autorità di controllo in tutta l'Unione. Esso dovrebbe assolvere i suoi compiti in piena indipendenza.

(140) Il comitato dovrebbe essere assistito da un segretariato messo a disposizione dal garante europeo della protezione dei dati. Il personale del garante europeo della protezione dei dati impegnato nell'assolvimento dei compiti attribuiti al comitato dal presente regolamento dovrebbe svolgere i suoi compiti esclusivamente secondo le istruzioni del presidente del comitato e riferire a quest'ultimo.

(141) Ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente, e il diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento 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 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.

(142) Qualora l'interessato ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento, dovrebbe avere il diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto di uno Stato membro, con obiettivi statutari di pubblico interesse, e che siano attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto a un'autorità di controllo, esercitare il diritto a un ricorso giurisdizionale per conto degli interessati o esercitare il diritto di ottenere il risarcimento del danno per conto degli interessati se quest'ultimo è previsto dal diritto degli Stati membri. Gli Stati membri possono prescrivere che tale organismo, organizzazione o associazione abbia il diritto di proporre reclamo in tale Stato membro, indipendentemente dall'eventuale mandato dell'interessato, e il diritto di proporre un ricorso giurisdizionale effettivo qualora abbia motivo di ritenere che i diritti di un interessato siano stati violati in conseguenza di un trattamento dei dati personali che violi il presente regolamento. Tale organismo, organizzazione o associazione può non essere autorizzato a chiedere il risarcimento del danno per conto di un interessato indipendentemente dal mandato dell'interessato.

(143) Qualsiasi persona fisica o giuridica ha diritto di proporre un ricorso per l'annullamento delle decisioni del comitato dinanzi alla Corte di giustizia, alle condizioni previste all'articolo 263 TFUE. In quanto destinatari di tali decisioni, le autorità di controllo interessate che intendono impugnarle, devono proporre ricorso entro due mesi dalla loro notifica, conformemente all'articolo 263 TFUE. Ove le decisioni del comitato si riferiscano direttamente e individualmente a un titolare del trattamento, a un responsabile del trattamento o al reclamante, quest'ultimo può proporre un ricorso per l'annullamento di tali decisioni e dovrebbe farlo entro due mesi dalla loro pubblicazione sul sito web del comitato, conformemente all'articolo 263 TFUE. Fatto salvo tale diritto ai sensi dell'articolo 263 TFUE, ogni persona fisica o giuridica dovrebbe poter proporre un ricorso giurisdizionale effettivo dinanzi alle competenti autorità giurisdizionali nazionali contro una decisione dell'autorità di controllo che produce effetti giuridici nei confronti di detta 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 a un ricorso giurisdizionale effettivo non comprende altre misure adottate dalle autorità di controllo che non sono giuridicamente vincolanti, come pareri o consulenza forniti dall'autorità di controllo. Le azioni contro l'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 in conformità del diritto processuale 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.

Se un reclamo è stato rigettato o archiviato da un'autorità di controllo, il reclamante può proporre ricorso giurisdizionale nello stesso Stato membro. Nell'ambito dei ricorsi giurisdizionali relativi all'applicazione del presente regolamento, le autorità giurisdizionali nazionali che ritengano necessario, ai fini di una sentenza, disporre di una decisione in merito, possono, o nel caso di cui all'articolo 267 TFUE, devono chiedere alla Corte di giustizia di pronunciarsi, in via pregiudiziale, sull'interpretazione del diritto dell'Unione, compreso il presente regolamento. Inoltre, se una decisione dell'autorità di controllo che attua una decisione del comitato è impugnata dinanzi a un'autorità giurisdizionale nazionale ed è in questione la validità della decisione del comitato, tale autorità giurisdizionale nazionale non ha il potere di invalidare la decisione del comitato, ma deve deferire la questione di validità alla Corte di giustizia ai sensi dell'articolo 267 TFUE quale interpretato dalla Corte di giustizia, ove ritenga la decisione non valida. Tuttavia, un'autorità giurisdizionale nazionale non può deferire una questione relativa alla validità di una decisione del comitato su richiesta di una persona fisica o giuridica che ha avuto la possibilità di proporre un ricorso per l'annullamento di tale decisione, specialmente se direttamente e individualmente interessata da siffatta decisione, ma non ha agito in tal senso entro il termine stabilito dall'articolo 263 TFUE.

(144) Qualora un'autorità giurisdizionale adita per un'azione contro una decisione di un'autorità di controllo abbia motivo di ritenere che le azioni riguardanti lo stesso trattamento, quale lo stesso oggetto relativamente al trattamento da parte dello stesso titolare del trattamento o dello stesso responsabile del trattamento, o lo stesso titolo, siano sottoposte a un'autorità giurisdizionale competente in un altro Stato membro, l'autorità giurisdizionale adita dovrebbe contattare tale autorità giurisdizionale al fine di confermare l'esistenza di tali azioni connesse. Se le azioni connesse sono pendenti dinanzi a un'autorità giurisdizionale in un altro Stato membro, qualsiasi autorità giurisdizionale successivamente adita può sospendere l'azione proposta dinanzi a essa o, su richiesta di una delle parti, può dichiarare la propria incompetenza a favore della prima autorità giurisdizionale adita se tale autorità giurisdizionale è competente a conoscere delle azioni in questione e la sua legge consente la riunione delle azioni. Le azioni sono considerate connesse quando hanno tra loro un legame così stretto da rendere opportuno trattarle e decidere in merito contestualmente, per evitare il rischio di sentenze incompatibili risultanti da azioni separate.

(145) Nelle azioni contro un titolare del trattamento o responsabile del trattamento, il ricorrente dovrebbe poter avviare un'azione legale dinanzi all'autorità giurisdizionale dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento o in cui risiede l'interessato, salvo che il titolare del trattamento sia un'autorità pubblica di uno Stato membro che agisce nell'esercizio dei suoi poteri pubblici.

(146) Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento.

(147) Qualora il presente regolamento preveda disposizioni specifiche in materia di giurisdizione, in particolare riguardo a procedimenti che prevedono il ricorso giurisdizionale, compreso quello per risarcimento, contro un titolare del trattamento o un responsabile del trattamento, disposizioni generali in materia di giurisdizione quali quelle di cui al regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio (13) non dovrebbero pregiudicare l'applicazione di dette disposizioni specifiche.

(148) Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento,in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento. In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria. Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo.

(149) Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia.

(150) Al fine di rafforzare e armonizzare le sanzioni amministrative applicabili per violazione del presente regolamento, ogni autorità di controllo dovrebbe poter imporre sanzioni amministrative pecuniarie. Il presente regolamento dovrebbe specificare le violazioni, indicare il limite massimo e i criteri per prevedere la relativa sanzione amministrativa pecuniaria, che dovrebbe essere stabilita dall'autorità di controllo competente in ogni singolo caso, tenuto conto di tutte le circostanze pertinenti della situazione specifica, in particolare della natura, gravità e durata dell'infrazione e delle relative conseguenze, nonché delle misure adottate per assicurare la conformità agli obblighi derivanti dal presente regolamento e prevenire o attenuare le conseguenze della violazione. Se le sanzioni amministrative sono inflitte a imprese, le imprese dovrebbero essere intese quali definite agli articoli 101 e 102 TFUE a tali fini. Se le sanzioni amministrative sono inflitte a persone che non sono imprese, l'autorità di controllo dovrebbe tenere conto del livello generale di reddito nello Stato membro come pure della situazione economica della persona nel valutare l'importo appropriato della sanzione pecuniaria. Il meccanismo di coerenza può essere utilizzato anche per favorire un'applicazione coerente delle sanzioni amministrative pecuniarie. Dovrebbe spettare agli Stati membri determinare se e in che misura le autorità pubbliche debbano essere soggette a sanzioni amministrative pecuniarie. Imporre una sanzione amministrativa pecuniaria o dare un avvertimento non incide sull'applicazione di altri poteri delle autorità di controllo o di altre sanzioni a norma del regolamento.

(151) I sistemi giudiziari di Danimarca ed Estonia non consentono l'irrogazione di sanzioni amministrative pecuniarie come previsto dal presente regolamento. Le norme relative alle sanzioni amministrative pecuniarie possono essere applicate in maniera tale che in Danimarca la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali quale sanzione penale e in Estonia la sanzione pecuniaria sia imposta dall'autorità di controllo nel quadro di una procedura d'infrazione, purché l'applicazione di tali norme in detti Stati membri abbia effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. Le competenti autorità giurisdizionali nazionali dovrebbero pertanto tener conto della raccomandazione dell'autorità di controllo che avvia l'azione sanzionatoria. In ogni caso, le sanzioni pecuniarie irrogate dovrebbero essere effettive, proporzionate e dissuasive.

(152) Se il presente regolamento non armonizza le sanzioni amministrative o se necessario in altri casi, ad esempio in caso di gravi violazioni del regolamento, gli Stati membri dovrebbero attuare un sistema che preveda sanzioni effettive, proporzionate e dissuasive. La natura di tali sanzioni, penali o amministrative, dovrebbe essere determinata dal diritto degli Stati membri.

(153) Il diritto degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali ai sensi del presente regolamento. Il trattamento dei dati personali effettuato unicamente a scopi giornalistici o di espressione accademica, artistica o letteraria dovrebbe essere soggetto a deroghe o esenzioni rispetto ad

alcune disposizioni del presente regolamento se necessario per conciliare il diritto alla protezione dei dati personali e il diritto alla libertà d'espressione e di informazione sancito nell'articolo 11 della Carta. Ciò dovrebbe applicarsi in particolare al trattamento dei dati personali nel settore audiovisivo, negli archivi stampa e nelle emeroteche. È pertanto opportuno che gli Stati adottino misure legislative che prevedano le deroghe e le esenzioni necessarie ai fini di un equilibrio tra tali diritti fondamentali. Gli Stati membri dovrebbero adottare tali esenzioni e deroghe con riferimento alle disposizioni riguardanti i principi generali, i diritti dell'interessato, il titolare del trattamento e il responsabile del trattamento, il trasferimento di dati personali verso paesi terzi o a organizzazioni internazionali, le autorità di controllo indipendenti, la cooperazione e la coerenza nonché situazioni di trattamento dei dati specifiche. Qualora tali esenzioni o deroghe differiscano da uno Stato membro all'altro, dovrebbe applicarsi il diritto dello Stato membro cui è soggetto il titolare del trattamento. Per tenere conto dell'importanza del diritto alla libertà di espressione in tutte le società democratiche è necessario interpretare in modo esteso i concetti relativi a detta libertà, quali la nozione di giornalismo.

(154) Il presente regolamento ammette, nell'applicazione delle sue disposizioni, che si tenga conto del principio del pubblico accesso ai documenti ufficiali. L'accesso del pubblico ai documenti ufficiali può essere considerato di interesse pubblico. I dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti. Tali disposizioni legislative dovrebbero conciliare l'accesso del pubblico ai documenti ufficiali e il riutilizzo delle informazioni del settore pubblico con il diritto alla protezione dei dati personali e possono quindi prevedere la necessaria conciliazione con il diritto alla protezione dei dati personali, in conformità del presente regolamento. Il riferimento alle autorità pubbliche e agli organismi pubblici dovrebbe comprendere, in tale contesto, tutte le autorità o altri organismi cui si applica il diritto degli Stati membri sull'accesso del pubblico ai documenti. La direttiva 2003/98/CE del Parlamento europeo e del Consiglio (14) non pregiudica in alcun modo il livello di tutela delle persone fisiche con riguardo al trattamento dei dati personali ai sensi delle disposizioni di diritto dell'Unione e degli Stati membri e non modifica, in particolare, gli obblighi e i diritti previsti dal presente regolamento. Nello specifico, tale direttiva non dovrebbe applicarsi ai documenti il cui accesso è escluso o limitato in virtù dei regimi di accesso per motivi di protezione dei dati personali, e a parti di documenti accessibili in virtù di tali regimi che contengono dati personali il cui riutilizzo è stato previsto per legge come incompatibile con la normativa in materia di tutela delle persone fisiche con riguardo al trattamento dei dati personali.

(155) Il diritto degli Stati membri o i contratti collettivi, ivi compresi gli «accordi aziendali», possono prevedere norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per quanto riguarda le condizioni alle quali i dati personali nei rapporti di lavoro possono essere trattati sulla base del consenso del dipendente, per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

(156) Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici dovrebbe essere soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie dovrebbero

assicurare che siano state predisposte misure tecniche e organizzative al fine di garantire, in particolare, il principio della minimizzazione dei dati. L'ulteriore trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è da effettuarsi quando il titolare del trattamento ha valutato la fattibilità di conseguire tali finalità trattando dati personali che non consentono o non consentono più di identificare l'interessato, purché esistano garanzie adeguate (come ad esempio la pseudonimizzazione dei dati personali). Gli Stati membri dovrebbero prevedere garanzie adeguate per il trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche. Gli Stati membri dovrebbero essere autorizzati a fornire, a specifiche condizioni e fatte salve adeguate garanzie per gli interessati, specifiche e deroghe relative ai requisiti in materia di informazione e ai diritti alla rettifica, alla cancellazione, all'oblio, alla limitazione del trattamento, alla portabilità dei dati personali, nonché al diritto di opporsi in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica o storica o per finalità statistiche. Le condizioni e le garanzie in questione possono comprendere procedure specifiche per l'esercizio di tali diritti da parte degli interessati, qualora ciò sia appropriato alla luce delle finalità previste dallo specifico trattamento, oltre a misure tecniche e organizzative intese a ridurre al minimo il trattamento dei dati personali conformemente ai principi di proporzionalità e di necessità. Il trattamento dei dati personali per finalità scientifiche dovrebbe rispettare anche altre normative pertinenti, ad esempio quelle sulle sperimentazioni cliniche.

(157) Combinando informazioni provenienti dai registri, i ricercatori possono ottenere nuove conoscenze di grande utilità relativamente a patologie diffuse come le malattie cardiovascolari, il cancro e la depressione. Avvalendosi dei registri, i risultati delle ricerche possono acquistare maggiore rilevanza, dal momento che si basano su una popolazione più ampia. Nell'ambito delle scienze sociali, la ricerca basata sui registri consente ai ricercatori di ottenere conoscenze essenziali sulla correlazione a lungo termine tra numerose condizioni sociali, quali la disoccupazione e il livello di istruzione, e altre condizioni di vita. I risultati delle ricerche ottenuti dai registri forniscono conoscenze solide e di alta qualità, che possono costituire la base per l'elaborazione e l'attuazione di politiche basate sulla conoscenza, migliorare la qualità della vita per molte persone, migliorare l'efficienza dei servizi sociali. Al fine di facilitare la ricerca scientifica, i dati personali possono essere trattati per finalità di ricerca scientifica fatte salve condizioni e garanzie adeguate previste dal diritto dell'Unione o degli Stati membri.

(158) Qualora i dati personali siano trattati a fini di archiviazione, il presente regolamento dovrebbe applicarsi anche a tale tipo di trattamento, tenendo presente che non dovrebbe applicarsi ai dati delle persone decedute. Le autorità pubbliche o gli organismi pubblici o privati che tengono registri di interesse pubblico dovrebbero essere servizi che, in virtù del diritto dell'Unione o degli Stati membri, hanno l'obbligo legale di acquisire, conservare, valutare, organizzare, descrivere, comunicare, promuovere, diffondere e fornire accesso a registri con un valore a lungo termine per l'interesse pubblico generale. Gli Stati membri dovrebbero inoltre essere autorizzati a prevedere il trattamento ulteriore dei dati personali per finalità di archiviazione, per esempio al fine di fornire specifiche informazioni connesse al comportamento politico sotto precedenti regimi statali totalitari, a genocidi, crimini contro l'umanità, in particolare l'Olocausto, o crimini di guerra.

(159) Qualora i dati personali siano trattati per finalità di ricerca scientifica, il presente regolamento dovrebbe applicarsi anche a tale trattamento. Nell'ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire

uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica. Per rispondere alle specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica. Se il risultato della ricerca scientifica, in particolare nel contesto sanitario, costituisce motivo per ulteriori misure nell'interesse dell'interessato, le norme generali del presente regolamento dovrebbero applicarsi in vista di tali misure.

(160) Qualora i dati personali siano trattati a fini di ricerca storica, il presente regolamento dovrebbe applicarsi anche a tale trattamento. Ciò dovrebbe comprendere anche la ricerca storica e la ricerca a fini genealogici, tenendo conto del fatto che il presente regolamento non dovrebbe applicarsi ai dati delle persone decedute.

(161) Ai fini del consenso alla partecipazione ad attività di ricerca scientifica nell'ambito di sperimentazioni cliniche dovrebbero applicarsi le pertinenti disposizioni del regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio (15).

(162) Qualora i dati personali siano trattati per finalità statistiche, il presente regolamento dovrebbe applicarsi a tale trattamento. Il diritto dell'Unione o degli Stati membri dovrebbe, entro i limiti del presente regolamento, determinare i contenuti statistici, il controllo dell'accesso, le specifiche per il trattamento dei dati personali per finalità statistiche e le misure adeguate per tutelare i diritti e le libertà dell'interessato e per garantire il segreto statistico. Per finalità statistiche si intende qualsiasi operazione di raccolta e trattamento di dati personali necessari alle indagini statistiche o alla produzione di risultati statistici. Tali risultati statistici possono essere ulteriormente usati per finalità diverse, anche per finalità di ricerca scientifica. La finalità statistica implica che il risultato del trattamento per finalità statistiche non siano dati personali, ma dati aggregati, e che tale risultato o i dati personali non siano utilizzati a sostegno di misure o decisioni riguardanti persone fisiche specifiche.

(163) È opportuno proteggere le informazioni riservate raccolte dalle autorità statistiche nazionali e dell'Unione per la produzione di statistiche ufficiali europee e nazionali. Le statistiche europee dovrebbero essere sviluppate, prodotte e diffuse conformemente ai principi statistici di cui all'articolo 338, paragrafo 2, TFUE, mentre le statistiche nazionali dovrebbero essere conformi anche al diritto degli Stati membri. Il regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio (16) fornisce ulteriori specificazioni in merito al segreto statistico per quanto riguarda le statistiche europee.

(164) Per quanto riguarda il potere delle autorità di controllo di ottenere, dal titolare del trattamento o dal responsabile del trattamento, accesso ai dati personali e accesso ai loro locali, gli Stati membri possono stabilire per legge, nei limiti del presente regolamento, norme specifiche per tutelare il segreto professionale o altri obblighi equivalenti di segretezza, qualora si rendano necessarie per conciliare il diritto alla protezione dei dati personali con il segreto professionale. Ciò non pregiudica gli obblighi esistenti degli Stati membri di adottare norme relative al segreto professionale laddove richiesto dal diritto dell'Unione.

(165) Il presente regolamento rispetta e non pregiudica lo status di cui godono le chiese e le associazioni o comunità religiose negli Stati membri in virtù del diritto costituzionale vigente, in conformità dell'articolo 17 TFUE.

(166) Al fine di conseguire gli obiettivi del regolamento, segnatamente tutelare i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, e garantire la libera circolazione di tali dati nell'Unione, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE. In particolare, dovrebbero essere adottati atti delegati riguardanti i criteri e i requisiti dei meccanismi di certificazione, le informazioni da presentare sotto forma di icone standardizzate e le procedure per fornire tali icone. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti. Nella preparazione e nell'elaborazione degli atti delegati, la Commissione dovrebbe provvedere alla contestuale, tempestiva e appropriata trasmissione dei documenti pertinenti al Parlamento europeo e al Consiglio.

(167) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione ove previsto dal presente regolamento. Tali competenze dovrebbero essere esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio.A tal fine, la Commissione dovrebbe contemplare misure specifiche per le micro, piccole e medie imprese.

(168) È opportuno applicare la procedura d'esame per l'adozione di atti di esecuzione su: clausole contrattuali tipo tra i titolari del trattamento e i responsabili del trattamento e tra responsabili del trattamento; codici di condotta; norme tecniche e meccanismi di certificazione; adeguato livello di protezione offerto da un paese terzo, un territorio o settore specifico all'interno del paese terzo, o da un'organizzazione internazionale; clausole tipo di protezione dei dati; formati e procedure per lo scambio di informazioni per via elettronica tra i titolari del trattamento, i responsabili del trattamento e le autorità di controllo per norme vincolanti d'impresa; assistenza reciproca; e modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato.

(169) È opportuno che la Commissione adotti atti di esecuzione immediatamente applicabili quando gli elementi a disposizione indicano che un paese terzo, un territorio o settore di specifico all'interno di tale paese terzo, o un'organizzazione internazionale non garantisce un livello di protezione adeguato e ciò è reso necessario da imperativi motivi di urgenza.

(170) Poiché l'obiettivo del presente regolamento, vale a dire garantire un livello equivalente di tutela delle persone fisiche e la libera circolazione dei dati personali nell'Unione, non può essere conseguito in misura sufficiente dagli Stati membri ma, a motivo della portata e degli effetti dell'azione in questione, può essere conseguito meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea (TUE). Il presente regolamento si limita a quanto è necessario per conseguire tale obiettivo in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(171) Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di applicazione del presente regolamento dovrebbe essere reso conforme al presente

regolamento entro un periodo di due anni dall'entrata in vigore del presente regolamento. Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione del presente regolamento. Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate.

(172) Il Garante europeo della protezione dei dati è stato consultato conformemente all'articolo 28, paragrafo 2, del regolamento (CE) n. 45/2001 e ha espresso un parere il 7 marzo 2012 (17).

(173) È opportuno che il presente regolamento si applichi a tutti gli aspetti relativi alla tutela dei diritti e delle libertà fondamentali con riguardo al trattamento dei dati personali che non rientrino in obblighi specifici, aventi lo stesso obiettivo, di cui alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio (18), compresi gli obblighi del titolare del trattamento e i diritti delle persone fisiche. Per chiarire il rapporto tra il presente regolamento e la direttiva 2002/58/CE, è opportuno modificare quest'ultima di conseguenza. Una volta adottato il presente regolamento, la direttiva 2002/58/CE dovrebbe essere riesaminata in particolare per assicurare la coerenza con il presente regolamento,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I
Disposizioni generali

Articolo 1
Oggetto e finalità (C1-14, C170, C172)

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

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

3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 2
Ambito di applicazione materiale (C 15-21)

1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

2. Il presente regolamento 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 dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; (C18)

d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

3. Per il trattamento dei dati personali da parte di istituzioni, organi, uffici e agenzie dell'Unione, si applica il regolamento (CE) n. 45/2001. Il regolamento (CE) n. 45/2001 e gli altri atti giuridici dell'Unione applicabili a tale trattamento di dati personali devono essere adeguati ai principi e alle norme del presente regolamento conformemente all'articolo 98.

4. Il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE, in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui agli articoli da 12 a 15 della medesima direttiva.

Articolo 3
Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del

trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. (C22)

2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: (C23, C24)

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure

b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico. (C25)

Articolo 4

Definizioni

Ai fini del presente regolamento s'intende per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale; (C26, C27, C30)

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; (C67)

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; (C24, C30, C71-C72)

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 tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (C26, C28-C29)

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; (C15)

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo 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 degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (C74)

8) «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;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento; (C31)

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

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; (C32, C33)

12) «violazione dei dati personali»: la violazione di 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; (C85)

13) «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; (C34)

14) «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; (C51)

15) «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; (C35)

16) «stabilimento principale»: (C36, C37)

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento; (C80)

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate; (C37, C48)

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune; (C37, C110)

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: (C124)

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

26) «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 5
Principi applicabili al trattamento di dati personali

1. I dati personali sono: (C39)

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

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

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

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

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

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»). (C74)

Articolo 6
Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (C40)

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (C42, C43)

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; (C44)

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; (C45)

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; (C46)

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; (C45, C46)

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. (C47-C50)

La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX. (C8, C10, C41, C45, C51)

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: (C8, C10, C41, C45, C51)

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito.

4. Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: (C50)

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

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

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10;

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

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

Articolo 7

Condizioni per il consenso (C42, C43)

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

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

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

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

Articolo 8

Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione (C38)

1. Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni.

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

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

Articolo 9

Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati

biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. (C51)

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: (C51, C52)

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

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

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

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;

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

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; (C55, C56)

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; (C53)

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; (C54)

j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

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

segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. (C53)

4. Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute. (C8, C10, C41, C45, C53)

Articolo 10

Trattamento dei dati personali relativi a condanne penali e reati

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.

Articolo 11

Trattamento che non richiede l'identificazione (C57, C64)

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

2. Qualora, nei casi di cui al paragrafo 1 del presente articolo, il titolare del trattamento possa dimostrare di non essere in grado di identificare l'interessato, ne informa l'interessato, se possibile. In tali casi, gli articoli da 15 a 20 non si applicano tranne quando l'interessato, al fine di esercitare i diritti di cui ai suddetti articoli, fornisce ulteriori informazioni che ne consentano l'identificazione.

CAPO III

Diritti dell'interessato

Sezione 1

Trasparenza e modalità

Articolo 12

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato (C58-C60, C64)

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai

minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

2. Il titolare del trattamento agevola l'esercizio dei diritti dell'interessato ai sensi degli articoli da 15 a 22. Nei casi di cui all'articolo 11, paragrafo 2, il titolare del trattamento non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti ai sensi degli articoli da 15 a 22, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

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

5. Le informazioni fornite ai sensi degli articoli 13 e 14 ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 e dell'articolo 34 sono gratuite. Se le richieste dell'interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento può:

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

b) rifiutare di soddisfare la richiesta.

Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

6. Fatto salvo l'articolo 11, qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta di cui agli articoli da 15 a 21, può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

7. Le informazioni da fornire agli interessati a norma degli articoli 13 e 14 possono essere fornite in combinazione con icone standardizzate per dare, in modo facilmente visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto. Se presentate elettronicamente, le icone sono leggibili da dispositivo automatico.

8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di stabilire le informazioni da presentare sotto forma di icona e le procedure per fornire icone standardizzate.

Sezione 2

Informazione e accesso ai dati personali

Articolo 13

Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato (C60-C62)

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

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

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

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

d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

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

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

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

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

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

c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

d) il diritto di proporre reclamo a un'autorità di controllo;

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

f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

3. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce

all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

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

Articolo 14

Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato (C60-C62)

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

a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;

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

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

d) le categorie di dati personali in questione;

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

f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, paragrafo 1, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili.

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

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

b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;

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

d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca;

e) il diritto di proporre reclamo a un'autorità di controllo;

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

g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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

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

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

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

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

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

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni;

c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure

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

Articolo 15

Diritto di accesso dell'interessato (C63, C64)

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

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

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

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

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

f) il diritto di proporre reclamo a un'autorità di controllo;

g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;

h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

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

Sezione 3

Rettifica e cancellazione

Articolo 16

Diritto di rettifica (C65)

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

Articolo 17

Diritto alla cancellazione («diritto all'oblio») (C65, C66)

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

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

b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

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

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

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

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

b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;

d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

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

Articolo 18

Diritto di limitazione di trattamento (C67)

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

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

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

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

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

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

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

Articolo 19

Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento (C31)

Il titolare del trattamento comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche o cancellazioni o limitazioni del trattamento effettuate a norma dell'articolo 16, dell'articolo 17, paragrafo 1, e dell'articolo 18, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato. Il titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda.

Articolo 20

Diritto alla portabilità dei dati (C68)

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

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

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

Sezione 4

Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

Articolo 21

Diritto di opposizione (C69, C70)

1. L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

2. Qualora i dati personali siano trattati per finalità di marketing diretto, l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto.

3. Qualora l'interessato si opponga al trattamento per finalità di marketing diretto, i dati personali non sono più oggetto di trattamento per tali finalità.

4. Il diritto di cui ai paragrafi 1 e 2 è esplicitamente portato all'attenzione dell'interessato ed è presentato chiaramente e separatamente da qualsiasi altra informazione al più tardi al momento della prima comunicazione con l'interessato.

5. Nel contesto dell'utilizzo di servizi della società dell'informazione e fatta salva la direttiva 2002/58/CE, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.

6. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici a norma dell'articolo 89, paragrafo 1, l'interessato, per motivi connessi alla sua situazione particolare, ha il diritto di opporsi al trattamento di dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Articolo 22

Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione (C71, C72)

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

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

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

b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul consenso esplicito dell'interessato.

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

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Sezione 5
Limitazioni

Articolo 23
Limitazioni (C73)

1. Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui agli articoli da 12 a 22, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

d) la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;

e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale;

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

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

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

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

j) l'esecuzione delle azioni civili.

2. In particolare qualsiasi misura legislativa di cui al paragrafo 1 contiene disposizioni specifiche riguardanti almeno, se del caso:

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

b) le categorie di dati personali;

c) la portata delle limitazioni introdotte;

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

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

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

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

h) il diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

CAPO IV
Titolare del trattamento e responsabile del trattamento

Sezione 1
Obblighi generali

Articolo 24
Responsabilità del titolare del trattamento (C74-C78)

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

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

3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Articolo 25
Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita (C75-C78)

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

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

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

Articolo 26

Contitolari del trattamento (C79)

1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

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

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

Articolo 27

Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione (C80)

1. Ove si applichi l'articolo 3, paragrafo 2, il titolare del trattamento o il responsabile del trattamento designa per iscritto un rappresentante nell'Unione.

2. L'obbligo di cui al paragrafo 1 del presente articolo non si applica:

a) al trattamento se quest'ultimo è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento; oppure

b) alle autorità pubbliche o agli organismi pubblici.

3. Il rappresentante è stabilito in uno degli Stati membri in cui si trovano gli interessati e i cui dati personali sono trattati nell'ambito dell'offerta di beni o servizi o il cui comportamento è monitorato.

4. Ai fini della conformità con il presente regolamento, il rappresentante è incaricato dal titolare del trattamento o dal responsabile del trattamento a fungere da interlocutore, in aggiunta o in sostituzione del titolare del trattamento o del responsabile del trattamento, in particolare delle autorità di controllo e degli interessati, per tutte le questioni riguardanti il trattamento.

5. La designazione di un rappresentante a cura del titolare del trattamento o del responsabile del trattamento fa salve le azioni legali che potrebbero essere promosse contro lo stesso titolare del trattamento o responsabile del trattamento.

Articolo 28

Responsabile del trattamento (C81)

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

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

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

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

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

c) adotti tutte le misure richieste ai sensi dell'articolo 32;

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

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

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

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

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

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

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

5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo.

6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43.

7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63.

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

10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.

Articolo 29

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento (C81)

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

Articolo 30

Registri delle attività di trattamento (C82)

1. Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

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

b) le finalità del trattamento;

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

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

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

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

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

2. Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

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

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

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

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

4. Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

5. Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10.

Articolo 31

Cooperazione con l'autorità di controllo (C82)

Il titolare del trattamento, il responsabile del trattamento e, ove applicabile, il loro rappresentante cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

Sezione 2

Sicurezza dei dati personali

Articolo 32

Sicurezza del trattamento (C83)

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

a) la pseudonimizzazione e la cifratura dei dati personali;

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

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

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

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

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

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

Articolo 33

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

(C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

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

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

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

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

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

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

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

5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34

Comunicazione di una violazione dei dati personali all'interessato (C86-C88)

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

2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

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

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

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

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

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

Sezione 3

Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Articolo 35

Valutazione d'impatto sulla protezione dei dati (C84, C89-C93, C95)

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

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

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

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

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

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

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

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

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

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

Articolo 36

Consultazione preventiva (C94-C96)

1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

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

3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

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

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

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; e

f) ogni altra informazione richiesta dall'autorità di controllo.

4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.

5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

Sezione 4

Responsabile della protezione dei dati

Articolo 37

Designazione del responsabile della protezione dei dati (C97)

1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

2. Un gruppo imprenditoriale può nominare un unico responsabile della protezione dei dati, a condizione che un responsabile della protezione dei dati sia facilmente raggiungibile da ciascuno stabilimento.

3. Qualora il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica o un organismo pubblico, un unico responsabile della protezione dei dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione.

4. Nei casi diversi da quelli di cui al paragrafo 1, il titolare del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

5. 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 39.

6. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

7. Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

Articolo 38

Posizione del responsabile della protezione dei dati (C97)

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

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

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

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

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

Articolo 39

Compiti del responsabile della protezione dei dati (C97)

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

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

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

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo; e

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 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Sezione 5

Codici di condotta e certificazione

Articolo 40

Codici di condotta (C98, C99, C167-C168)

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

2. Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a:

a) il trattamento corretto e trasparente dei dati;

b) i legittimi interessi perseguiti dai titolari del trattamento in contesti specifici;

c) la raccolta dei dati personali;

d) la pseudonimizzazione dei dati personali;

e) l'informazione fornita al pubblico e agli interessati;

f) l'esercizio dei diritti degli interessati;

g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore;

h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32;

i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'interessato;

j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; o

k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra titolari del trattamento e interessati in materia di trattamento, fatti salvi i diritti degli interessati ai sensi degli articoli 77 e 79.

3. Oltre all'adesione ai codici di condotta approvati ai sensi del paragrafo 5 del presente articolo e aventi validità generale a norma del paragrafo 9 del presente articolo da parte di titolari o responsabili soggetti al presente regolamento, possono aderire a tali codici di condotta anche i

titolari del trattamento o i responsabili del trattamento che non sono soggetti al presente regolamento ai sensi dell'articolo 3, al fine di fornire adeguate garanzie nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera e). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

4. Il codice di condotta di cui al paragrafo 2 del presente articolo contiene i meccanismi che consentono all'organismo di cui all'articolo 41, paragrafo 1, di effettuare il controllo obbligatorio del rispetto delle norme del codice da parte dei titolari del trattamento o dei responsabili del trattamento che si impegnano ad applicarlo, fatti salvi i compiti e i poteri delle autorità di controllo competenti ai sensi degli articoli 55 o 56.

5. Le associazioni e gli altri organismi di cui al paragrafo 2 del presente articolo che intendono elaborare un codice di condotta o modificare o prorogare un codice esistente sottopongono il progetto di codice, la modifica o la proroga all'autorità di controllo competente ai sensi dell'articolo 55. L'autorità di controllo esprime un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga e approva tale progetto, modifica o proroga, se ritiene che offra in misura sufficiente garanzie adeguate.

6. Qualora il progetto di codice, la modifica o la proroga siano approvati ai sensi dell'articolo 55, e se il codice di condotta in questione non si riferisce alle attività di trattamento in vari Stati membri, l'autorità di controllo registra e pubblica il codice.

7. Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvare il progetto, la modifica o la proroga, l'autorità di controllo che è competente ai sensi dell'articolo 55 lo sottopone, tramite la procedura di cui all'articolo 63, al comitato, il quale formula un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 del presente articolo, sulla previsione di adeguate garanzie.

8. Qualora il parere di cui al paragrafo 7 confermi che il progetto di codice di condotta, la modifica o la proroga è conforme al presente regolamento o, nel caso di cui al paragrafo 3, fornisce adeguate garanzie, il comitato trasmette il suo parere alla Commissione.

9. La Commissione può decidere, mediante atti di esecuzione, che il codice di condotta, la modifica o la proroga approvati, che le sono stati sottoposti ai sensi del paragrafo 8 del presente articolo, hanno validità generale all'interno dell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

10. La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 9.

11. Il comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

Articolo 41

Controllo dei codici di condotta approvati

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, il controllo della conformità con un codice di condotta ai sensi dell'articolo 40 può essere effettuato da un organismo in possesso del livello adeguato di competenze riguardo al contenuto del codice e del necessario accreditamento a tal fine dell'autorità di controllo competente.

2. L'organismo di cui al paragrafo 1 può essere accreditato a controllare l'osservanza di un codice di condotta se esso ha:

a) dimostrato in modo convincente all'autorità di controllo competente di essere indipendente e competente riguardo al contenuto del codice;

b) istituito procedure che gli consentono di valutare l'ammissibilità dei titolari del trattamento e dei responsabili del trattamento in questione ad applicare il codice, di controllare che detti titolari e responsabili ne rispettino le disposizioni e di riesaminarne periodicamente il funzionamento;

c) istituito procedure e strutture atte a gestire i reclami relativi a violazioni del codice o il modo in cui il codice è stato o è attuato da un titolare del trattamento o un responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e

d) dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da esso svolti non danno adito a conflitto di interessi.

3. L'autorità di controllo competente presenta al comitato il progetto di requisiti per l'accreditamento dell'organismo di cui al paragrafo 1 del presente articolo, ai sensi del meccanismo di coerenza di cui all'articolo 63.

4. Fatti salvi i compiti e i poteri dell'autorità di controllo competente e le disposizioni del capo VIII, un organismo di cui al paragrafo 1 del presente articolo adotta, stanti garanzie appropriate, le opportune misure in caso di violazione del codice da parte di un titolare del trattamento o responsabile del trattamento, tra cui la sospensione o l'esclusione dal codice del titolare del trattamento o del responsabile del trattamento. Esso informa l'autorità di controllo competente di tali misure e dei motivi della loro adozione.

5. L'autorità di controllo competente revoca l'accreditamento dell'organismo di cui al paragrafo 1, se i requisiti per l'accreditamento non sono, o non sono più, rispettati o se le misure adottate dall'organismo violano il presente regolamento.

6. Il presente articolo non si applica al trattamento effettuato da autorità pubbliche e da organismi pubblici.

Articolo 42

Certificazione (C100)

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

2. Oltre all'adesione dei titolari del trattamento o responsabili del trattamento soggetti al presente regolamento, i meccanismi, i sigilli o i marchi approvati ai sensi del paragrafo 5 del presente articolo possono essere istituiti al fine di dimostrare la previsione di garanzie appropriate da parte dei titolari del trattamento o responsabili del trattamento non soggetti al presente regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

3. La certificazione è volontaria e accessibile tramite una procedura trasparente.

4. La certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti a norma degli articoli 55 o 56.

5. La certificazione ai sensi del presente articolo è rilasciata dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente in base ai criteri approvati da tale autorità di controllo competente ai sensi dell'articolo 58, paragrafo 3, o dal comitato, ai sensi dell'articolo 63. Ove i criteri siano approvati dal comitato, ciò può risultare in una certificazione comune, il sigillo europeo per la protezione dei dati.

6. Il titolare del trattamento o il responsabile del trattamento che sottopone il trattamento effettuato al meccanismo di certificazione fornisce all'organismo di certificazione di cui all'articolo 43 o, ove applicabile, all'autorità di controllo competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione.

7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino a essere soddisfatti i criteri pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i criteri per la certificazione.

8. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli e i marchi di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

Articolo 43

Organismi di certificazione (C166-C168)

1. Fatti salvi i compiti e i poteri dell'autorità di controllo competente di cui agli articoli 57 e 58, gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:

a) dall'autorità di controllo competente ai sensi degli articoli 55 o 56;

b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio (20) conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56.

2. Gli organismi di certificazione di cui al paragrafo 1 sono accreditati in conformità di tale paragrafo solo se:

a) hanno dimostrato in modo convincente all'autorità di controllo competente di essere indipendenti e competenti riguardo al contenuto della certificazione;

b) si sono impegnati a rispettare i criteri di cui all'articolo 42, paragrafo 5, e approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63;

c) hanno istituito procedure per il rilascio, il riesame periodico e la revoca delle certificazioni, dei sigilli e dei marchi di protezione dei dati;

d) hanno istituito procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal titolare del trattamento o dal

responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e

e) hanno dimostrato in modo convincente all'autorità di controllo competente che i compiti e le funzioni da loro svolti non danno adito a conflitto di interessi.

3. L'accreditamento degli organi di certificazione di cui ai paragrafi 1 e 2 del presente articolo ha luogo in base ai requisiti approvati dall'autorità di controllo competente ai sensi degli articoli 55 o 56 o dal comitato, ai sensi dell'articolo 63. In caso di accreditamento ai sensi del paragrafo 1, lettera b), del presente articolo, tali requisiti integrano quelli previsti dal regolamento (CE) n. 765/2008 nonché le norme tecniche che definiscono i metodi e le procedure degli organismi di certificazione.

4. Gli organismi di certificazione di cui al paragrafo 1 sono responsabili della corretta valutazione che comporta la certificazione o la revoca di quest'ultima, fatta salva la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di certificazione soddisfi i requisiti.

5. L'organismo di certificazione di cui al paragrafo 1 trasmette all'autorità di controllo competente i motivi del rilascio o della revoca della certificazione richiesta.

6. I requisiti di cui al paragrafo 3 del presente articolo e i criteri di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in forma facilmente accessibile. Le autorità di controllo provvedono a trasmetterli anche al comitato.

7. Fatto salvo il capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento di un organismo di certificazione di cui al paragrafo 1 del presente articolo, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il presente regolamento.

8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati di cui all'articolo 42, paragrafo 1.

9. La Commissione può adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

CAPO V

Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

Articolo 44

Principio generale per il trasferimento (C101, C102)

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo

soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Articolo 45

Trasferimento sulla base di una decisione di adeguatezza (C103, C107, C167-C169)

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

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

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

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

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

3. La Commissione, previa valutazione dell'adeguatezza del livello di protezione, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo. L'atto di esecuzione prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. L'atto di esecuzione specifica il proprio ambito di applicazione geografico e settoriale e, ove applicabile, identifica la o le autorità di controllo di cui al paragrafo 2, lettera b), del presente articolo. L'atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

4. La Commissione controlla su base continuativa gli sviluppi nei paesi terzi e nelle organizzazioni internazionali che potrebbero incidere sul funzionamento delle decisioni adottate a norma del paragrafo 3 del presente articolo e delle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE.

5. Se risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui al paragrafo 3 del presente articolo, che un paese terzo, un territorio o uno o più settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono più un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, la Commissione revoca, modifica o sospende nella misura necessaria la decisione di cui al paragrafo 3 del presente articolo mediante atti di esecuzione senza effetto retroattivo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2, o, in casi di estrema urgenza, secondo la procedura di cui all'articolo 93, paragrafo 3.

Per imperativi motivi di urgenza debitamente giustificati, la Commissione adotta atti di esecuzione immediatamente applicabili secondo la procedura di cui all'articolo 93, paragrafo 3.

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

7. Una decisione ai sensi del paragrafo 5 del presente articolo lascia impregiudicato il trasferimento di dati personali verso il paese terzo, il territorio o uno o più settori specifici all'interno del paese terzo, o verso l'organizzazione internazionale in questione, a norma degli articoli da 46 a 49.

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

9. Le decisioni adottate dalla Commissione in base all'articolo 25, paragrafo 6, della direttiva 95/46/CE restano in vigore fino a quando non sono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al paragrafo 3 o 5 del presente articolo.

Articolo 46

Trasferimento soggetto a garanzie adeguate (C108, C109, C114)

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

2. Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo:

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

b) le norme vincolanti d'impresa in conformità dell'articolo 47;

c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;

d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;

e) un codice di condotta approvato a norma dell'articolo 40,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o

f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

3. Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1:

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

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

4. L'autorità di controllo applica il meccanismo di coerenza di cui all'articolo 63 nei casi di cui al paragrafo 3 del presente articolo.

5. Le autorizzazioni rilasciate da uno Stato membro o dall'autorità di controllo in base all'articolo 26, paragrafo 2, della direttiva 95/46/CE restano valide fino a quando non vengono modificate, sostituite o abrogate, se necessario, dalla medesima autorità di controllo. Le decisioni adottate dalla Commissione in base all'articolo 26, paragrafo 4, della direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate, se necessario, da una decisione della Commissione adottata conformemente al paragrafo 2 del presente articolo.

Articolo 47

Norme vincolanti d'impresa (C110, C167-C168)

1. L'autorità di controllo competente approva le norme vincolanti d'impresa in conformità del meccanismo di coerenza di cui all'articolo 63, a condizione che queste:

a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti;

b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali; e

c) soddisfino i requisiti di cui al paragrafo 2.

2. Le norme vincolanti d'impresa di cui al paragrafo 1 specificano almeno:

a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;

b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;

c) la loro natura giuridicamente vincolante, a livello sia interno che esterno;

d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;

e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente

all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;

f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;

g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14;

h) i compiti di qualunque responsabile della protezione dei dati designato ai sensi dell'articolo 35 o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami;

i) le procedure di reclamo;

j) i meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;

k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;

l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j);

m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e

n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

3. La Commissione può specificare il formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa ai sensi del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Articolo 48

Trasferimento o comunicazione non autorizzati dal diritto dell'Unione (C115)

Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da parte di un titolare del trattamento o di un responsabile del trattamento possono essere riconosciute o assumere

qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria, fatti salvi gli altri presupposti di trasferimento a norma del presente capo.

Articolo 49

Deroghe in specifiche situazioni (C111-C114)

1. In mancanza di una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 3, o di garanzie adeguate ai sensi dell'articolo 46, comprese le norme vincolanti d'impresa, è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle seguenti condizioni:

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

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

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

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

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

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

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

Se non è possibile basare il trasferimento su una disposizione dell'articolo 45 o 46, comprese le disposizioni sulle norme vincolanti d'impresa, e nessuna delle deroghe in specifiche situazioni a norma del primo comma del presente paragrafo è applicabile, il trasferimento verso un paese terzo o un'organizzazione internazionale sia ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali. Il titolare del trattamento informa del trasferimento l'autorità di controllo. In aggiunta alla fornitura di informazioni di cui agli articoli 13 e 14, il titolare del trattamento informa l'interessato del trasferimento e degli interessi legittimi cogenti perseguiti.

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

3. Il primo comma, lettere a), b) e c), e il secondo comma del paragrafo 1 non si applicano alle attività svolte dalle autorità pubbliche nell'esercizio dei pubblici poteri.

4. L'interesse pubblico di cui al paragrafo 1, primo comma, lettera d), è riconosciuto dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento.

5. In mancanza di una decisione di adeguatezza, il diritto dell'Unione o degli Stati membri può, per importanti motivi di interesse pubblico, fissare espressamente limiti al trasferimento di categorie specifiche di dati verso un paese terzo o un'organizzazione internazionale. Gli Stati membri notificano tali disposizioni alla Commissione.

6. Il titolare del trattamento o il responsabile del trattamento attesta nel registro di cui all'articolo 30 la valutazione e le garanzie adeguate di cui al paragrafo 1, secondo comma, del presente articolo.

Articolo 50

Cooperazione internazionale per la protezione dei dati personali (C116)

In relazione ai paesi terzi e alle organizzazioni internazionali, la Commissione e le autorità di controllo adottano misure appropriate per:

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

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

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

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

CAPO VI

Autorità di controllo indipendenti

Sezione 1

Indipendenza

Articolo 51

Autorità di controllo (C117)

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

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

3. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63.

4. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo al più tardi entro il 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

Articolo 52

Indipendenza (C118-C120)

1. Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente regolamento.

2. Nell'adempimento dei rispettivi compiti e nell'esercizio dei rispettivi poteri previsti dal presente regolamento, il membro o i membri di ogni autorità di controllo non subiscono pressioni esterne, né dirette, né indirette, e non sollecitano né accettano istruzioni da alcuno.

3. Il membro o i membri dell'autorità di controllo si astengono da qualunque azione incompatibile con le loro funzioni e per tutta la durata del mandato non possono esercitare alcuna altra attività incompatibile, remunerata o meno.

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

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

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

Articolo 53

Condizioni generali per i membri dell'autorità di controllo (C121)

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

— dal rispettivo parlamento;

— dal rispettivo governo;

— dal rispettivo capo di Stato; oppure

— da un organismo indipendente incaricato della nomina a norma del diritto dello Stato membro.

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

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

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

Articolo 54

Norme sull'istituzione dell'autorità di controllo

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

a) l'istituzione di ogni autorità di controllo;

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

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

d) la durata del mandato del membro o dei membri di ogni autorità di controllo non inferiore a quattro anni, salvo per le prime nomine dopo il 24 maggio 2016, alcune delle quali possono avere una durata inferiore qualora ciò sia necessario per tutelare l'indipendenza dell'autorità di controllo mediante una procedura di nomina scaglionata;

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

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

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

Sezione 2

Competenza, compiti e poteri

Articolo 55

Competenza (C122, C123, C128)

1. Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro.

2. Se il trattamento è effettuato da autorità pubbliche o organismi privati che agiscono sulla base dell'articolo 6, paragrafo 1, lettera c) o e), è competente l'autorità di controllo dello Stato membro interessato. In tal caso, non si applica l'articolo 56.

3. Le autorità di controllo non sono competenti per il controllo dei trattamenti effettuati dalle autorità giurisdizionali nell'esercizio delle loro funzioni giurisdizionali.

Articolo 56

Competenza dell'autorità di controllo capofila

(C124, C125, C127, C128, C131)

1. Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60.

2. In deroga al paragrafo 1, ogni autorità di controllo è competente per la gestione dei reclami a essa proposti o di eventuali violazioni del presente regolamento se l'oggetto riguarda unicamente uno stabilimento nel suo Stato membro o incide in modo sostanziale sugli interessati unicamente nel suo Stato membro.

3. Nei casi indicati al paragrafo 2 del presente articolo, l'autorità di controllo informa senza ritardo l'autorità di controllo capofila in merito alla questione. Entro un termine di tre settimane da quando è stata informata, l'autorità di controllo capofila decide se intende o meno trattare il caso secondo la procedura di cui all'articolo 60, tenendo conto dell'esistenza o meno di uno stabilimento del titolare del trattamento o responsabile del trattamento nello Stato membro dell'autorità di controllo che l'ha informata.

4. Qualora l'autorità di controllo capofila decida di trattare il caso, si applica la procedura di cui all'articolo 60. L'autorità di controllo che ha informato l'autorità di controllo capofila può presentare a quest'ultima un progetto di decisione. L'autorità di controllo capofila tiene nella massima considerazione tale progetto nella predisposizione del progetto di decisione di cui all'articolo 60, paragrafo 3.

5. Nel caso in cui l'autorità di controllo capofila decida di non trattarlo, l'autorità di controllo che ha informato l'autorità di controllo capofila tratta il caso conformemente agli articoli 61 e 62.

6. L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare del trattamento o responsabile del trattamento.

Articolo 57

Compiti (C122, C129, C132)

1. Fatti salvi gli altri compiti indicati nel presente regolamento, sul proprio territorio ogni autorità di controllo:

a) sorveglia e assicura l'applicazione del presente regolamento;

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

c) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;

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

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

f) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 80, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;

g) collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento;

h) svolge indagini sull'applicazione del presente regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;

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

j) adotta le clausole contrattuali tipo di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);

k) redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;

l) offre consulenza sui trattamenti di cui all'articolo 36, paragrafo 2;

m) incoraggia l'elaborazione di codici di condotta ai sensi dell'articolo 40, paragrafo 1, e fornisce un parere su tali codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma dell'articolo 40, paragrafo 5;

n) incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5;

o) ove applicabile, effettua un riesame periodico delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;

p) definisce e pubblica i requisiti per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;

q) effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;

r) autorizza le clausole contrattuali e le altre disposizioni di cui all'articolo 46, paragrafo 3;

s) approva le norme vincolanti d'impresa ai sensi dell'articolo 47;

t) contribuisce alle attività del comitato;

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

v) svolge qualsiasi altro compito legato alla protezione dei dati personali.

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

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

4. Qualora le richieste siano manifestamente infondate o eccessive, in particolare per il carattere ripetitivo, l'autorità di controllo può addebitare un contributo spese ragionevole basato sui costi

amministrativi o rifiutarsi di soddisfare la richiesta. Incombe all'autorità di controllo dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Articolo 58

Poteri (C122, C129)

1. Ogni autorità di controllo ha tutti i poteri di indagine seguenti:

a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;

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

c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;

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

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

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

2. Ogni autorità di controllo ha tutti i poteri correttivi seguenti:

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

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

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

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

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

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

g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;

h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;

i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e

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

3. Ogni autorità di controllo ha tutti i poteri autorizzativi e consultivi seguenti:

a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36;

b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali;

c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare;

d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5;

e) accreditare gli organismi di certificazione a norma dell'articolo 43;

f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5;

g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);

h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a);

i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b);

j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47.

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

5. Ogni Stato membro dispone per legge che la sua autorità di controllo abbia il potere di intentare un'azione o di agire in sede giudiziale o, ove del caso, stragiudiziale in caso di violazione del presente regolamento per far rispettare le disposizioni dello stesso.

6. Ogni Stato membro può prevedere per legge che la sua autorità di controllo abbia ulteriori poteri rispetto a quelli di cui ai paragrafi 1, 2 e 3. L'esercizio di tali poteri non pregiudica l'operatività effettiva del capo VII.

Articolo 59

Relazioni sull'attività

Ogni autorità di controllo elabora una relazione annuale sulla propria attività, in cui può figurare un elenco delle tipologie di violazioni notificate e di misure adottate a norma dell'articolo 58, paragrafo 2. Tali relazioni sono trasmesse al parlamento nazionale, al governo e alle altre autorità designate dal diritto dello Stato membro. Esse sono messe a disposizione del pubblico, della Commissione e del comitato.

CAPO VII
Cooperazione e coerenza

Sezione 1
Cooperazione

Articolo 60
Cooperazione tra l'autorità di controllo capofila e le altre autorità di controllo interessate (C123-C126, C130)

1. L'autorità di controllo capofila coopera con le altre autorità di controllo interessate conformemente al presente articolo nell'adoperarsi per raggiungere un consenso. L'autorità di controllo capofila e le autorità di controllo interessate si scambiano tutte le informazioni utili.

2. L'autorità di controllo capofila può chiedere in qualunque momento alle altre autorità di controllo interessate di fornire assistenza reciproca a norma dell'articolo 61 e può condurre operazioni congiunte a norma dell'articolo 62, in particolare per lo svolgimento di indagini o il controllo dell'attuazione di una misura riguardante un titolare del trattamento o responsabile del trattamento stabilito in un altro Stato membro.

3. L'autorità di controllo capofila comunica senza ritardo le informazioni utili sulla questione alle altre autorità di controllo interessate. Trasmette senza indugio alle altre autorità di controllo interessate un progetto di decisione per ottenere il loro parere e tiene debitamente conto delle loro opinioni.

4. Se una delle altre autorità di controllo interessate solleva un'obiezione pertinente e motivata al progetto di decisione entro un termine di quattro settimane dopo essere stata consultata conformemente al paragrafo 3 del presente articolo, l'autorità di controllo capofila, ove non dia seguito all'obiezione pertinente e motivata o ritenga l'obiezione non pertinente o non motivata, sottopone la questione al meccanismo di coerenza di cui all'articolo 63.

5. L'autorità di controllo capofila, qualora intenda dare seguito all'obiezione pertinente e motivata sollevata, trasmette un progetto di decisione riveduto alle altre autorità di controllo interessate per ottenere il loro parere. Tale progetto di decisione riveduto è soggetto alla procedura di cui al paragrafo 4 entro un termine di due settimane.

6. Se nessuna delle altre autorità di controllo interessate ha sollevato obiezioni al progetto di decisione trasmesso dall'autorità di controllo capofila entro il termine di cui ai paragrafi 4 e 5, si deve considerare che l'autorità di controllo capofila e le autorità di controllo interessate concordano su tale progetto di decisione e sono da esso vincolate.

7. L'autorità di controllo capofila adotta la decisione e la notifica allo stabilimento principale o allo stabilimento unico del titolare del trattamento o responsabile del trattamento, a seconda dei casi, e informa le altre autorità di controllo interessate e il comitato la decisione in questione, compresa una sintesi dei fatti e delle motivazioni pertinenti. L'autorità di controllo cui è stato proposto un reclamo informa il reclamante riguardo alla decisione.

8. In deroga al paragrafo 7, in caso di archiviazione o di rigetto di un reclamo, l'autorità di controllo cui è stato proposto il reclamo adotta la decisione e la notifica al reclamante e ne informa il titolare del trattamento.

9. Se l'autorità di controllo capofila e le autorità di controllo interessate convengono di archiviare o rigettare parti di un reclamo e di intervenire su altre parti di tale reclamo, è adottata una decisione separata per ciascuna di tali parti della questione. L'autorità di controllo capofila adotta la decisione per la parte riguardante azioni in relazione al titolare del trattamento e la notifica allo stabilimento principale o allo stabilimento unico del responsabile del trattamento o del responsabile del trattamento sul territorio del suo Stato membro e ne informa il reclamante, mentre l'autorità di controllo del reclamante adotta la decisione per la parte riguardante l'archiviazione o il rigetto di detto reclamo, la notifica a detto reclamante e ne informa il titolare del trattamento o il responsabile del trattamento.

10. Dopo aver ricevuto la notifica della decisione dell'autorità di controllo capofila a norma dei paragrafi 7 e 9, il titolare del trattamento o responsabile del trattamento adotta le misure necessarie per garantire la conformità alla decisione per quanto riguarda le attività di trattamento nel contesto di tutti i suoi stabilimenti nell'Unione. Il titolare del trattamento o responsabile del trattamento notifica le misure adottate per conformarsi alla decisione all'autorità di controllo capofila, che ne informa le altre autorità di controllo interessate.

11. Qualora, in circostanze eccezionali, un'autorità di controllo interessata abbia motivo di ritenere che urga intervenire per tutelare gli interessi degli interessati, si applica la procedura d'urgenza di cui all'articolo 66.

12. L'autorità di controllo capofila e le altre autorità di controllo interessate si scambiano reciprocamente con mezzi elettronici, usando un modulo standard, le informazioni richieste a norma del presente articolo.

Articolo 61

Assistenza reciproca (C123, C133, C167-C168)

1. Le autorità di controllo si scambiano le informazioni utili e si prestano assistenza reciproca al fine di attuare e applicare il presente regolamento in maniera coerente, e mettono in atto misure per cooperare efficacemente tra loro. L'assistenza reciproca comprende, in particolare, le richieste di informazioni e le misure di controllo, quali le richieste di autorizzazioni e consultazioni preventive e le richieste di effettuare ispezioni e indagini.

2. Ogni autorità di controllo adotta tutte le misure opportune necessarie per dare seguito alle richieste delle altre autorità di controllo senza ingiustificato ritardo e comunque entro un mese dal ricevimento della richiesta. Tali misure possono consistere, in particolare, nella trasmissione di informazioni utili sullo svolgimento di un'indagine.

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

4. L'autorità di controllo richiesta non deve rifiutare di dare seguito alla richiesta, salvo che:

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

b) l'accoglimento della richiesta violi le disposizioni del presente regolamento o il diritto dell'Unione o dello Stato membro cui è soggetta l'autorità di controllo che riceve la richiesta.

5. L'autorità di controllo richiesta informa l'autorità di controllo richiedente dell'esito o, a seconda dei casi, dei progressi delle misure adottate per rispondere alla richiesta. L'autorità di controllo richiesta deve fornire le motivazioni del rigetto della richiesta.

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

7. Le autorità di controllo richieste non impongono alcuna spesa per le misure da loro adottate a seguito di una richiesta di assistenza reciproca. Le autorità di controllo possono concordare disposizioni di indennizzo reciproco per spese specifiche risultanti dalla prestazione di assistenza reciproca in circostanze eccezionali.

8. Qualora l'autorità di controllo non fornisca le informazioni di cui al paragrafo 5 del presente articolo, entro un mese dal ricevimento della richiesta di un'altra autorità di controllo, l'autorità di controllo richiedente può adottare misure provvisorie nel territorio del suo Stato membro ai sensi dell'articolo 55, paragrafo 1. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 66, paragrafo 1, e che sia necessaria una decisione vincolante d'urgenza da parte del comitato a norma dell'articolo 66, paragrafo 2.

9. La Commissione può, mediante atti di esecuzione, specificare il formato e le procedure per l'assistenza reciproca di cui al presente articolo e le modalità per lo scambio di informazioni con mezzi elettronici tra autorità di controllo e tra le autorità di controllo e il comitato, in particolare il modulo standard di cui al paragrafo 6 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Articolo 62

Operazioni congiunte delle autorità di controllo (C134)

1. Se del caso, le autorità di controllo conducono operazioni congiunte, incluse indagini congiunte e misure di contrasto congiunte, cui partecipano membri o personale di autorità di controllo di altri Stati membri.

2. Qualora il titolare del trattamento o responsabile del trattamento abbia stabilimenti in vari Stati membri o qualora esista la probabilità che il trattamento abbia su un numero significativo di interessati in più di uno Stato membro un impatto negativo sostanziale, un'autorità di controllo di ogni Stato membro in questione ha il diritto di partecipare alle operazioni congiunte. L'autorità di controllo che è competente conformemente all'articolo 56, paragrafo 1, o all'articolo 56 paragrafo 4, invita l'autorità di controllo di ogni Stato membro interessato a partecipare all'operazione congiunta in questione e risponde senza ritardo alle richieste di partecipazione delle autorità di controllo.

3. Un'autorità di controllo può, in conformità del diritto degli Stati membri e con l'autorizzazione dell'autorità di controllo ospitata, conferire poteri, anche d'indagine, ai membri o al personale dell'autorità di controllo ospitata che partecipano alle operazioni congiunte o consentire ai membri o al personale dell'autorità di controllo ospitata, nella misura in cui il diritto dello Stato membro dell'autorità di controllo ospite lo permette, di esercitare i loro poteri d'indagine in conformità del diritto dello Stato membro dell'autorità di controllo ospitata. Tali poteri d'indagine possono essere esercitati unicamente sotto il controllo e in presenza di membri o personale dell'autorità di controllo ospite. I membri o il personale dell'autorità di controllo ospitata sono soggetti al diritto dello Stato membro dell'autorità di controllo ospite.

4. Qualora, in conformità del paragrafo 1, il personale di un'autorità di controllo ospitata operi in un altro Stato membro, lo Stato membro dell'autorità di controllo ospite si assume la responsabilità del suo operato, compreso l'obbligo di risarcimento, per i danni causati da detto personale nel corso delle operazioni, conformemente al diritto dello Stato membro nel cui territorio esso opera.

5. Lo Stato membro nel cui territorio sono stati causati i danni risarcisce tali danni alle condizioni applicabili ai danni causati dal proprio personale. Lo Stato membro dell'autorità di controllo ospitata il cui personale ha causato danni a terzi nel territorio di un altro Stato membro rimborsa integralmente a tale altro Stato membro importi corrisposti agli aventi diritto per conto di detti terzi.

6. Fatto salvo l'esercizio dei suoi diritti nei confronti di terzi e fatta eccezione per il paragrafo 5, ciascuno Stato membro rinuncia, nel caso previsto al paragrafo 1, a chiedere a un altro Stato membro il risarcimento dei danni di cui al paragrafo 4.

7. Qualora sia prevista un'operazione congiunta e un'autorità di controllo non si conformi entro un mese all'obbligo di cui al paragrafo 2, seconda frase, del presente articolo, le altre autorità di controllo possono adottare misure provvisorie nel territorio del loro Stato membro ai sensi dell'articolo 55. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 66, paragrafo 1, e che siano necessari un parere o una decisione vincolante d'urgenza da parte del comitato a norma dell'articolo 66, paragrafo 2.

Sezione 2

Coerenza

Articolo 63

Meccanismo di coerenza (C135, C138)

Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'Unione, le autorità di controllo cooperano tra loro e, se del caso, con la Commissione mediante il meccanismo di coerenza stabilito nella presente sezione.

Articolo 64

Parere del comitato europeo per la protezione dei dati (C135, C136, C138)

1. Il comitato emette un parere ove un'autorità di controllo competente intenda adottare una delle misure in appresso. A tal fine, l'autorità di controllo competente comunica il progetto di decisione al comitato, quando la decisione:

a) è finalizzata a stabilire un elenco di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;

b) riguarda una questione di cui all'articolo 40, paragrafo 7, relativa alla conformità al presente regolamento di un progetto di codice di condotta o una modifica o proroga di un codice di condotta;

c) è finalizzata ad approvare i requisiti per l'accreditamento di un organismo ai sensi dell'articolo 41, paragrafo 3, di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3, o i criteri per la certificazione di cui all'articolo 42, paragrafo 5;

d) è finalizzata a determinare clausole tipo di protezione dei dati di cui all'articolo 46, paragrafo 2, lettera d), e all'articolo 28, paragrafo 8;

e) è finalizzata ad autorizzare clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a); oppure

f) è finalizzata ad approvare norme vincolanti d'impresa ai sensi dell'articolo 47.

2. Qualsiasi autorità di controllo, il presidente del comitato o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal comitato al fine di ottenere un parere, in particolare se un'autorità di controllo

competente non si conforma agli obblighi relativi all'assistenza reciproca ai sensi dell'articolo 61 o alle operazioni congiunte ai sensi dell'articolo 62.

3. Nei casi di cui ai paragrafi 1 e 2, il comitato emette un parere sulla questione che gli è stata presentata, purché non abbia già emesso un parere sulla medesima questione. Tale parere è adottato entro un termine di otto settimane a maggioranza semplice dei membri del comitato. Tale termine può essere prorogato di sei settimane, tenendo conto della complessità della questione. Per quanto riguarda il progetto di decisione di cui al paragrafo 1 trasmesso ai membri del comitato conformemente al paragrafo 5, il membro che non abbia sollevato obiezioni entro un termine ragionevole indicato dal presidente è considerato assentire al progetto di decisione.

4. Senza ingiustificato ritardo, le autorità di controllo e la Commissione comunicano per via elettronica, usando un modulo standard, al comitato tutte le informazioni utili, in particolare, a seconda del caso, una sintesi dei fatti, il progetto di decisione, i motivi che rendono necessaria l'attuazione di tale misura e i pareri delle altre autorità di controllo interessate.

5. Il presidente del comitato informa, senza ingiustificato ritardo, con mezzi elettronici:

a) i membri del comitato e la Commissione di tutte le informazioni utili che sono state comunicate al comitato con modulo standard. Se necessario, il segretariato del comitato fornisce una traduzione delle informazioni utili; e

b) l'autorità di controllo di cui, secondo i casi, ai paragrafi 1 e 2, e la Commissione in merito al parere, che rende pubblico.

6. L'autorità di controllo competente di cui al paragrafo 1 si astiene dall'adottare il suo progetto di decisione di cui al paragrafo 1 entro il termine di cui al paragrafo 3.

7. L'autorità di controllo competente di cui al paragrafo 1 tiene nella massima considerazione il parere del comitato e, entro due settimane dal ricevimento del parere, comunica per via elettronica, usando un modulo standard, al presidente del comitato se intende mantenere o modificare il progetto di decisione e, se del caso, il progetto di decisione modificato.

8. Se entro il termine di cui al paragrafo 7 del presente articolo l' autorità di controllo competente di cui al paragrafo 1 informa il presidente del comitato, fornendo le pertinenti motivazioni, che non intende conformarsi al parere del comitato, in tutto o in parte, si applica l'articolo 65, paragrafo 1.

Articolo 65

Composizione delle controversie da parte del comitato (C136, C138, C143)

1. Al fine di assicurare l'applicazione corretta e coerente del presente regolamento nei singoli casi, il comitato adotta una decisione vincolante nei seguenti casi:

a) se, in un caso di cui all'articolo 60, paragrafo 4, un'autorità di controllo interessata ha sollevato un'obiezione pertinente e motivata a un progetto di decisione dell'autorità di controllo capofila e l'autorità capofila di controllo non abbia dato seguito all'obiezione o abbia rigettato tale obiezione in quanto non pertinente o non motivata. La decisione vincolante riguarda tutte le questioni oggetto dell'obiezione pertinente e motivata, in particolare se sussista una violazione del presente regolamento;

b) se vi sono opinioni contrastanti in merito alla competenza delle autorità di controllo interessate per lo stabilimento principale;

c) se un'autorità di controllo competente non richiede il parere del comitato nei casi di cui all'articolo 64, paragrafo 1, o non si conforma al parere del comitato emesso a norma dell'articolo 64. In tal caso qualsiasi autorità di controllo interessata o la Commissione può comunicare la questione al comitato.

2. La decisione di cui al paragrafo 1 è adottata entro un mese dal deferimento della questione da parte di una maggioranza di due terzi dei membri del comitato. Tale termine può essere prorogato di un mese, in considerazione della complessità della questione. La decisione di cui al paragrafo 1 è motivata e trasmessa all'autorità di controllo capofila e a tutte le autorità di controllo interessate ed è per esse vincolante.

3. Qualora non sia stato in grado di adottare una decisione entro i termini di cui al paragrafo 2, il comitato adotta la sua decisione entro due settimane dalla scadenza del secondo mese di cui al paragrafo 2, a maggioranza semplice dei membri del comitato. In caso di parità di voti dei membri del comitato, prevale il voto del presidente.

4. Le autorità di controllo interessate non adottano una decisione sulla questione sottoposta al comitato a norma del paragrafo 1 entro i termini di cui ai paragrafi 2 e 3.

5. Il presidente del comitato notifica senza ingiustificato ritardo alle autorità di controllo interessate la decisione di cui al paragrafo 1 e ne informa la Commissione. La decisione è pubblicata senza ritardo sul sito web del comitato dopo che l'autorità di controllo ha notificato la decisione definitiva di cui al paragrafo 6.

6. L'autorità di controllo capofila o, se del caso, l'autorità di controllo a cui è stato proposto il reclamo adotta la sua decisione definitiva in base alla decisione di cui al paragrafo 1 del presente articolo senza ingiustificato ritardo e al più tardi entro un mese dalla notifica della decisione da parte del comitato. L'autorità di controllo capofila o, se del caso, l'autorità di controllo a cui è stato proposto il reclamo, informa il comitato circa la data in cui la decisione definitiva è notificata rispettivamente al titolare del trattamento o al responsabile del trattamento e all'interessato. La decisione definitiva delle autorità di controllo interessate è adottata ai sensi dell'articolo 60, paragrafi 7, 8 e 9. La decisione finale fa riferimento alla decisione di cui al paragrafo 1 del presente articolo e precisa che la decisione di cui a tale paragrafo sarà pubblicata sul sito web del comitato conformemente al paragrafo 5 del presente articolo. La decisione finale deve accludere la decisione di cui al paragrafo 1 del presente articolo.

Articolo 66

Procedura d'urgenza (C137)

1. In circostanze eccezionali, qualora ritenga che urga intervenire per proteggere i diritti e le libertà degli interessati, un'autorità di controllo interessata può, in deroga al meccanismo di coerenza di cui agli articoli 63, 64 e 65, o alla procedura di cui all'articolo 60, adottare immediatamente misure provvisorie intese a produrre effetti giuridici nel proprio territorio, con un periodo di validità determinato che non supera i tre mesi. L'autorità di controllo comunica senza ritardo tali misure e la motivazione della loro adozione alle altre autorità di controllo interessate, al comitato e alla Commissione.

2. Qualora abbia adottato una misura ai sensi del paragrafo 1 e ritenga che urga adottare misure definitive, l'autorità di controllo può chiedere un parere d'urgenza o una decisione vincolante d'urgenza del comitato, motivando tale richiesta.

3. Qualsiasi autorità di controllo può chiedere un parere d'urgenza o una decisione vincolante d'urgenza, a seconda dei casi, del comitato qualora un'autorità di controllo competente non abbia adottato misure adeguate in una situazione in cui urge intervenire per proteggere i diritti e le libertà degli interessati, motivando la richiesta di tale parere o decisione, in particolare l'urgenza dell'intervento.

4. In deroga all'articolo 64, paragrafo 3, e all'articolo 65, paragrafo 2, il parere d'urgenza o la decisione vincolante d'urgenza di cui ai paragrafi 2 e 3 del presente articolo sono adottati entro due settimane a maggioranza semplice dei membri del comitato.

Articolo 67

Scambio di informazioni (C167-C168)

La Commissione può adottare atti di esecuzione di portata generale per specificare le modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato, in particolare il modulo standard di cui all'articolo 64.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Sezione 3

Comitato europeo per la protezione dei dati

Articolo 68

Comitato europeo per la protezione dei dati (C139)

1. Il comitato europeo per la protezione dei dati («comitato») è istituito quale organismo dell'Unione ed è dotato di personalità giuridica.

2. Il comitato è rappresentato dal suo presidente.

3. Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.

4. Qualora, in uno Stato membro, più autorità di controllo siano incaricate di sorvegliare l'applicazione delle disposizioni del presente regolamento, è designato un rappresentante comune conformemente al diritto di tale Stato membro.

5. La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato comunica alla Commissione le attività del comitato.

6. Nei casi di cui all'articolo 65, il garante europeo della protezione dei dati ha diritto di voto solo per decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione che corrispondono nella sostanza a quelli del presente regolamento.

Articolo 69

Indipendenza (C139)

1. Nell'esecuzione dei suoi compiti o nell'esercizio dei suoi poteri ai sensi degli articoli 70 e 71, il comitato opera con indipendenza.

2. Fatte salve le richieste della Commissione di cui all'articolo 70, paragrafi 1 e 2, nell'esecuzione dei suoi compiti o nell'esercizio dei suoi poteri il comitato non sollecita né accetta istruzioni da alcuno.

Articolo 70

Compiti del comitato (C139)

1. Il comitato garantisce l'applicazione coerente del presente regolamento. A tal fine, il comitato, di propria iniziativa o, se del caso, su richiesta della Commissione, in particolare:

a) monitora il presente regolamento e ne assicura l'applicazione corretta nei casi previsti agli articoli 64 e 65 fatti salvi i compiti delle autorità nazionali di controllo;

b) fornisce consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, comprese eventuali proposte di modifica del presente regolamento;

c) fornisce consulenza alla Commissione sul formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa;

d) pubblica linee guida, raccomandazioni e migliori prassi in materia di procedure per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico di cui all'articolo 17, paragrafo 2;

e) esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del presente regolamento e pubblica linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del presente regolamento;

f) pubblica linee guida, raccomandazioni e migliori pratiche conformemente alla lettera e) del presente paragrafo, per specificare ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione ai sensi dell'articolo 22, paragrafo 2;

g) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, per accertare la violazione di dati personali e determinare l'ingiustificato ritardo di cui all'articolo 33, paragrafi 1 e 2, e le circostanze particolari in cui il titolare del trattamento o il responsabile del trattamento è tenuto a notificare la violazione dei dati personali;

h) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, relative alle circostanze in cui una violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche di cui all'articolo 34, paragrafo 1;

i) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, al fine di specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali basati sulle norme vincolanti d'impresa applicate, rispettivamente, dai titolari del trattamento e dai responsabili del trattamento, nonché gli ulteriori requisiti per assicurare la protezione dei dati personali degli interessati di cui all'articolo 47;

j) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, al fine di specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali sulla base dell'articolo 49, paragrafo 1;

k) elabora per le autorità di controllo linee guida riguardanti l'applicazione delle misure di cui all'articolo 58, paragrafi 1, 2 e 3, e la previsione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 83;

l) valuta l'applicazione pratica delle linee guida, raccomandazioni e migliori prassi;

m) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, per stabilire procedure comuni per le segnalazioni da parte di persone fisiche di violazioni del presente regolamento ai sensi dell'articolo 54, paragrafo 2;

n) incoraggia l'elaborazione di codici di condotta e l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati ai sensi degli articoli 40 e 42;

o) approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5, e tiene un registro pubblico di meccanismi di certificazione e di sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 8, e dei titolari o responsabili del trattamento certificati, stabiliti in paesi terzi a norma dell'articolo 42, paragrafo 7;

p) approva i requisiti di cui all'articolo 43, paragrafo 3, ai fini dell'accreditamento degli organismi di certificazione di cui all'articolo 43;

q) fornisce alla Commissione un parere in merito ai requisiti di certificazione di cui all'articolo 43, paragrafo 8;

r) fornisce alla Commissione un parere in merito alle icone di cui all'articolo 12, paragrafo 7;

s) fornisce alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale, così come per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione. A tal fine, la Commissione fornisce al comitato tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, con riguardo a tale paese terzo, territorio o settore specifico, o con l'organizzazione internazionale;

t) emette pareri sui progetti di decisione delle autorità di controllo conformemente al meccanismo di coerenza di cui all'articolo 64, paragrafo 1, e sulle questioni presentate conformemente all'articolo 64, paragrafo 2, ed emette decisioni vincolanti ai sensi dell'articolo 65, anche nei casi di cui all'articolo 66;

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

v) promuove programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di organizzazioni internazionali;

w) promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo;

x) emette pareri sui codici di condotta redatti a livello di Unione a norma dell'articolo 40, paragrafo 9; e

y) tiene un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza.

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

3. Il comitato trasmette pareri, linee guida, raccomandazioni e migliori prassi alla Commissione e al comitato di cui all'articolo 93, e li pubblica.

4. Se del caso, il comitato consulta le parti interessate e offre loro la possibilità di esprimere commenti entro un termine ragionevole. Fatto salvo l'articolo 76, il comitato rende pubblici i risultati della procedura di consultazione.

Articolo 71

Relazioni

1. Il comitato redige una relazione annuale sulla protezione delle persone fisiche con riguardo al trattamento nell'Unione e, se del caso, nei paesi terzi e nelle organizzazioni internazionali. La relazione è pubblicata ed è trasmessa al Parlamento europeo, al Consiglio e alla Commissione.

2. La relazione annuale include la valutazione dell'applicazione pratica delle linee guida, raccomandazioni e migliori prassi di cui all'articolo 70, paragrafo 1, lettera l), nonché delle decisioni vincolanti di cui all'articolo 65.

Articolo 72

Procedura

1. Il comitato decide a maggioranza semplice dei suoi membri, salvo se diversamente previsto dal presente regolamento.

2. Il comitato adotta il proprio regolamento interno deliberando a maggioranza di due terzi dei suoi membri e stabilisce le modalità del proprio funzionamento.

Articolo 73

Presidente

1. Il comitato elegge un presidente e due vicepresidenti tra i suoi membri a maggioranza semplice.

2. Il presidente e i vicepresidenti hanno un mandato di cinque anni, rinnovabile una volta.

Articolo 74

Compiti del presidente (C139)

1. Il presidente ha il compito di:

a) convocare le riunioni del comitato e stabilirne l'ordine del giorno;

b) notificare le decisioni adottate dal comitato a norma dell'articolo 65 all'autorità di controllo capofila e alle autorità di controllo interessate;

c) assicurare l'esecuzione tempestiva dei compiti del comitato, in particolare in relazione al meccanismo di coerenza di cui all'articolo 63.

2. Il comitato europeo stabilisce nel proprio regolamento interno la ripartizione dei compiti tra presidente e vicepresidenti.

Articolo 75

Segreteria (C140)

1. Il comitato dispone di una segreteria messa a disposizione dal garante europeo della protezione dei dati.

2. La segreteria svolge i propri compiti seguendo esclusivamente le istruzioni del presidente del comitato.

3. Il personale del garante europeo della protezione dei dati coinvolto nell'assolvimento dei compiti attribuiti al comitato dal presente regolamento è soggetto a linee gerarchiche separate rispetto al personale coinvolto nello svolgimento dei compiti attribuiti al garante europeo della protezione dei dati.

4. Se del caso, il comitato e il garante europeo della protezione dei dati stabiliscono e pubblicano un protocollo d'intesa che attua il presente articolo, stabilisce i termini della loro cooperazione e si applica al personale del garante europeo della protezione dei dati coinvolto nell'assolvimento dei compiti attribuiti al comitato dal presente regolamento.

5. La segreteria presta assistenza in materia di analisi, amministrativa e logistica al comitato.

6. La segreteria è incaricata in particolare:

a) della gestione ordinaria del comitato;

b) della comunicazione tra i membri del comitato, il suo presidente e la Commissione;

c) della comunicazione con le altre istituzioni e il pubblico;

d) dell'uso di mezzi elettronici per la comunicazione interna ed esterna;

e) della traduzione delle informazioni rilevanti;

f) della preparazione delle riunioni del comitato e del relativo seguito;

g) della preparazione, redazione e pubblicazione dei pareri, delle decisioni sulla composizione delle controversie tra le autorità di controllo e di altri testi adottati dal comitato.

Articolo 76

Riservatezza

1. Se il comitato europeo lo ritiene necessario, le sue deliberazioni hanno carattere riservato, come previsto dal suo regolamento interno.

2. L'accesso ai documenti trasmessi ai membri del comitato, agli esperti e ai rappresentanti di terzi è disciplinato dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio (21).

CAPO VIII

Mezzi di ricorso, responsabilità e sanzioni

Articolo 77

Diritto di proporre reclamo all'autorità di controllo (C141)

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.

2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

Articolo 78

Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo (C141, C143)

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

2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.

3. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

4. Qualora siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del meccanismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

Articolo 79

Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento (C141, C145, C147)

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.

2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

Articolo 80

Rappresentanza degli interessati (C142)

1. L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82.

2. Gli Stati membri possono prevedere che un organismo, organizzazione o associazione di cui al paragrafo 1 del presente articolo, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79, qualora ritenga che i diritti di cui un interessato gode a norma del presente regolamento siano stati violati in seguito al trattamento.

Articolo 81

Sospensione delle azioni (C144, C147)

1. L'autorità giurisdizionale competente di uno Stato membro che venga a conoscenza di azioni riguardanti lo stesso oggetto relativamente al trattamento dello stesso titolare del trattamento o dello stesso responsabile del trattamento pendenti presso un'autorità giurisdizionale in un altro Stato membro, prende contatto con tale autorità giurisdizionale nell'altro Stato membro per confermare l'esistenza delle azioni.

2. Qualora azioni riguardanti lo stesso oggetto relativamente al trattamento dello stesso titolare del trattamento o dello stesso responsabile del trattamento siano pendenti presso un'autorità giurisdizionale in un altro Stato membro, qualunque autorità giurisdizionale competente successivamente adita può sospendere le azioni.

3. Se tali azioni sono pendenti in primo grado, qualunque autorità giurisdizionale successivamente adita può parimenti dichiarare la propria incompetenza su richiesta di una delle parti a condizione che l'autorità giurisdizionale adita per prima sia competente a conoscere delle domande proposte e la sua legge consenta la riunione dei procedimenti.

Articolo 82

Diritto al risarcimento e responsabilità (C142, C146, C147)

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Articolo 83

Condizioni generali per infliggere sanzioni amministrative pecuniarie

(C148, C150-C152)

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

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

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro il 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

Articolo 84

Sanzioni (C149, C152)

1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

2. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro il 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

CAPO IX

Disposizioni relative a specifiche situazioni di trattamento

Articolo 85

Trattamento e libertà d'espressione e di informazione (C153)

1. Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria.

2. Ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono esenzioni o deroghe rispetto ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 2 e comunica senza ritardo ogni successiva modifica.

Articolo 86

Trattamento e accesso del pubblico ai documenti ufficiali (C154)

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 comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri 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 ai sensi del presente regolamento.

Articolo 87

Trattamento del numero di identificazione nazionale

Gli Stati membri possono precisare ulteriormente le condizioni specifiche per il trattamento di un numero di identificazione nazionale o di qualsiasi altro mezzo d'identificazione d'uso generale. In tal caso, il numero di identificazione nazionale o qualsiasi altro mezzo d'identificazione d'uso generale sono utilizzati soltanto in presenza di garanzie adeguate per i diritti e le libertà dell'interessato conformemente al presente regolamento.

Articolo 88

Trattamento dei dati nell'ambito dei rapporti di lavoro (C155)

1. Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul

posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro il 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Articolo 89

Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (C33, C156-C163)

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

2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

4. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi.

Articolo 90

Obblighi di segretezza (C164)

1. Gli Stati membri possono adottare norme specifiche per stabilire i poteri delle autorità di controllo di cui all'articolo 58, paragrafo 1, lettere e) e f), in relazione ai titolari del trattamento o ai responsabili del trattamento che sono soggetti, ai sensi del diritto dell'Unione o degli Stati membri o di norme stabilite dagli organismi nazionali competenti, al segreto professionale o a un obbligo di segretezza equivalente, ove siano necessarie e proporzionate per conciliare il diritto alla protezione dei dati personali e l'obbligo di segretezza. Tali norme si applicano solo ai dati personali che il

titolare del trattamento o il responsabile del trattamento ha ricevuto o ha ottenuto in seguito a un'attività protetta da tale segreto professionale.

2. Ogni Stato membro notifica alla Commissione le norme adottate ai sensi del paragrafo 1 al più tardi entro il 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Articolo 91

Norme di protezione dei dati vigenti presso chiese e associazioni religiose (C165)

1. Qualora in uno Stato membro chiese e associazioni o comunità religiose applichino, al momento dell'entrata in vigore del presente regolamento, corpus completi di norme a tutela delle persone fisiche con riguardo al trattamento, tali corpus possono continuare ad applicarsi purché siano resi conformi al presente regolamento.

2. Le chiese e le associazioni religiose che applicano i corpus completi di norme di cui al paragrafo 1 del presente articolo sono soggette al controllo di un'autorità di controllo indipendente che può essere specifica, purché soddisfi le condizioni di cui al capo VI del presente regolamento.

CAPO X

Atti delegati e atti di esecuzione

Articolo 92

Esercizio della delega (C166)

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. La delega di potere di cui all'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, è conferita alla Commissione per un periodo indeterminato a decorrere dal 24 maggio 2016.

3. La delega di potere di cui all'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella Gazzetta ufficiale dell'Unione europea o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

5. L'atto delegato adottato ai sensi dell'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di tre mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di tre mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 93

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

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

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

CAPO XI

Disposizioni finali

Articolo 94

Abrogazione della direttiva 95/46/CE (C171)

1. La direttiva 95/46/CE è abrogata a decorrere dal 25 maggio 2018.

2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento.

Articolo 95

Rapporto con la direttiva 2002/58/CE (C173)

Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE.

Articolo 96

Rapporto con accordi precedentemente conclusi (C102)

Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali che comportano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali conclusi dagli Stati membri prima del 24 maggio 2016 e conformi al diritto dell'Unione applicabile prima di tale data.

Articolo 97

Relazioni della Commissione

1. Entro il 25 maggio 2020 e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio relazioni di valutazione e sul riesame del presente regolamento.

2. Nel contesto delle valutazioni e del riesame del presente regolamento di cui al paragrafo 1, la Commissione esamina, in particolare, l'applicazione e il funzionamento:

a) del capo V sul trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, con particolare riguardo alle decisioni adottate ai sensi dell'articolo 45, paragrafo 3, del presente regolamento, e alle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE;

b) del capo VII su cooperazione e coerenza.

3. Ai fini del paragrafo 1, la Commissione può richiedere informazioni agli Stati membri e alle autorità di controllo.

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

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

Articolo 98

Riesame di altri atti legislativi dell'Unione in materia di protezione dei dati

Se del caso, la Commissione presenta proposte legislative di modifica di altri atti legislativi dell'Unione in materia di protezione dei dati personali, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche con riguardo al trattamento. Ciò riguarda in particolare le norme relative alla protezione delle persone fisiche con riguardo al trattamento da parte di istituzioni, organi, uffici e agenzie dell'Unione e le norme sulla libera circolazione di tali dati.

Articolo 99

Entrata in vigore e applicazione

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

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

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

Fatto a Bruxelles, il 27 aprile 2016

Per il Parlamento europeo

Il presidente

M. SCHULZ

Per il Consiglio

Il presidente

J.A. HENNIS-PLASSCHAERT

(1) GU C 229 del 31.7.2012, pag. 90.

(2) GU C 391 del 18.12.2012, pag. 127.

(3) Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura dell'8 aprile 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 14 aprile 2016.

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

(5) Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (C(2003) 1422) (GU L 124 del 20.5.2003, pag. 36).

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

(7) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Cfr. pagina 89 della presente Gazzetta ufficiale).

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

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

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

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

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

(13) Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU L 351 del 20.12.2012, pag. 1).

(14) Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico (GU L 345 del 31.12.2003, pag. 90).

(15) Regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE (GU L 158 del 27.5.2014, pag. 1).

(16) Regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio, dell'11 marzo 2009, relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del

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

(17) GU C 192 del 30.6.2012, pag. 7.

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

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

(20) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

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

GRUPPO DI LAVORO ARTICOLO 29
IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

16/EN
WP 243 rev. 01

Linee-guida sui responsabili della protezione dei dati (RPD)[1]

Adottate il 13 dicembre 2016
Versione emendata e adottata in data 5 aprile 2017

Traduzione a cura del Garante per la protezione dei dati personali - Unità Documentazione Internazionale e Revisione UE

[1] **Comunemente noti con l'acronimo inglese di "DPO", ossia Data Protection Officers**

INDICE

IL GRUPPO DI LAVORO SULLA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli Articoli 29 e 30 della stessa,

visto il proprio regolamento,

HA ADOTTATO LE PRESENTI LINEE-GUIDA:

I. Introduzione

Il regolamento generale sulla protezione dei dati (RGPD)[1], che esplicherà i propri effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di *compliance* per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (*accountability*). I responsabili della protezione dei dati (RPD) saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del RGPD.

In base al RGPD, alcuni titolari e responsabili del trattamento sono tenuti a nominare un RPD in via obbligatoria.[2] Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali (dati sensibili).

Anche ove il regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "articolo 29" (WP29) incoraggia gli approcci di questo genere.

[1] Regolamento (Ue) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119, 4.5.2016). Il RGPD è rilevante ai fini del SEE e sarà applicabile una volta incorporato nell'Accordo relativo al SEE.

[2] La nomina di un RPD è obbligatoria anche con riguardo alle autorità competenti di cui all'art. 32 della 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 ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119, 4.5.2016), alla luce della normativa nazionale di recepimento. Le presenti linee-guida guardano con particolare attenzione alla figura del RPD come prevista dal RGPD, ma le indicazioni in esse formulate valgono anche per i RPD previsti dalla direttiva 2016/680 con riferimento alle disposizioni di carattere analogo contenute nei due strumenti.

La figura del RPD non costituisce una novità assoluta. La direttiva 95/46/CE[3] non prevedeva alcun obbligo di nomina di un RPD, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni.

Ancor prima dell'adozione del RGPD, il WP29 ha sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del RPD possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese.[4] Oltre a favorire l'osservanza attraverso strumenti di *accountability* (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.

I RPD non rispondono personalmente in caso di inosservanza del RGPD. Quest'ultimo chiarisce che spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, primo paragrafo). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare o sul responsabile.

Inoltre, al titolare o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il RPD è preposto. La nomina di un RPD è solo il primo passo, perché il RPD deve disporre anche di autonomia e risorse sufficienti a svolgere in modo efficace i compiti cui è chiamato.

Il RGPD riconosce nel RPD uno degli elementi-chiave all'interno del nuovo sistema di *governance* dei dati, e prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici. Le presenti linee-guida intendono fare chiarezza sulle pertinenti disposizioni del regolamento al fine di favorire l'osservanza della normativa da parte di titolari e responsabili del trattamento; inoltre, le linee-guida vogliono essere di ausilio ai RPD nell'esecuzione dei compiti loro attribuiti. Il presente documento contiene anche alcune raccomandazioni, in termini di migliori prassi, che scaturiscono dall'esperienza accumulata in alcuni Stati membri. Il WP29 monitorerà l'attuazione delle linee-guida qui presentate e provvederà alle integrazioni che si riveleranno opportune.

2. Nomina di un RPD

2.1. Nomina obbligatoria

In base all'articolo 37, primo paragrafo, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici:[5]

[3] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GU L 281, 23.11.95).

[4] Si veda http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

[5] Si osservi che, in base all'art. 37, quarto paragrafo, il diritto dell'Unione o dello Stato membro può prevedere casi ulteriori di nomina obbligatoria di un RPD.

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;[6]

b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati[7] o[8] di dati personali relativi a condanne penali e reati[9].

In questo paragrafo, il WP29 intende fornire indicazioni rispetto ai criteri e alle formulazioni utilizzati nell'articolo 37, paragrafo 1.

Tranne quando sia evidente che un soggetto non è tenuto a nominare un RPD, il WP29 raccomanda a titolari e responsabili di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RPD, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti.[10] Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario, per esempio se i titolari o i responsabili intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'art. 37, paragrafo 1.

Se si procede alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli artt. 37-39 per quanto concerne la nomina stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.

Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un RPD e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di responsabile per la protezione dei dati (RPD).[11]

---

[6] Con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali. V. art. 32 della direttiva (Ue) 2016/680.

[7] Ai sensi dell'art. 9, si tratta dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell'identificazione univoca di una persona fisica, e di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.

[8] Nel testo in lingua inglese dell'art. 37, primo paragrafo, lettera c) compare la congiunzione "*and*" (e); si veda il paragrafo 2.1.5 *infra* per maggiori chiarimenti sull'utilizzo della congiunzione "o" anziché "e" nello specifico contesto.

[9] Articolo 10.

[10] Si veda l'art. 24, primo paragrafo.

[11] Queste considerazioni valgono anche per i *chief privacy officers* (CPO) o altri professionisti in materia di privacy già operanti presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel regolamento per quanto riguarda, per esempio, le risorse disponibili o le salvaguardie della loro indipendenza e che, in tal caso, non possono essere considerati e denominati "RPD".

Il RPD viene designato, su base obbligatoria o meno, per tutti i trattamenti svolti dal titolare o dal responsabile.

2.1.1. "Autorità pubblica o organismo pubblico"

Nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il WP29 ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico.[12] In questi casi la nomina di un RPD è obbligatoria.

Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri[13] non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.

In tutti questi casi la situazione in cui versano gli interessati è probabilmente molto simile a quella in cui il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. Più in particolare, i trattamenti perseguono finalità simili e spesso il singolo ha, in modo analogo, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali; pertanto, è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un RPD.

Benché nei casi sopra descritti non sussista l'obbligo di nominare un RPD, il WP29 raccomanda, in termini di buone prassi, che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD. Le attività del RPD nominato nei termini sopra indicati si estendono a tutti i trattamenti svolti, compresi quelli che non sono connessi all'espletamento di funzioni pubbliche o all'esercizio di pubblici poteri quali, per esempio, la gestione di un database del personale.

2.1.2. "Attività principali"

L'articolo 37, paragrafo 1, lettere b) e c) del RGPD contiene un riferimento alle "*attività principali del titolare del trattamento o del responsabile del trattamento"*. Nel considerando 97 si afferma che le attività principali di un titolare del trattamento "*riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*". Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento.

Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare o dal responsabile. Per esempio, l'attività principale di un ospedale consiste nella

[12] Si vedano, per esempio, le definizioni di "ente pubblico" e "organismo di diritto pubblico" contenute nell'art. 2, paragrafi 1 e 2, della direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico.
[13] Articolo 6, paragrafo 1, lettera e).

prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un RPD.

A titolo di ulteriore esemplificazione, si può citare il caso di un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L'attività principale dell'impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali. Ne consegue che anche l'impresa in oggetto deve nominare un RPD.

D'altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

2.1.3. "Larga scala"

In base all'articolo 37, paragrafo 1, lettere b) e c) del RGPD, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito.[14]

In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il WP29 intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina di un RPD.

A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

[14] Il considerando in questione vi ricomprende, in particolare, "*trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*". D'altro canto, lo stesso considerando prevede in modo specifico che "*Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato*". Si deve tener conto del fatto che il considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che fra tali estremi si colloca un'ampia zona grigia. Inoltre, va sottolineato che il considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un RPD negli stessi identici termini.

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

2.1.4. "Monitoraggio regolare e sistematico"

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "*monitoraggio del comportamento di detti interessati*"[15] ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati.[16]

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del WP29:

[15] "*Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*."

[16] Si osservi che il considerando 24 riguarda l'applicazione extraterritoriale del RGPD; inoltre, vi è una differenza fra l'espressione "*monitoraggio del loro comportamento*" (art. 3, paragrafo 2, lettera b)) e "*monitoraggio regolare e sistematico degli interessati*" (art. 37, paragrafo 1, lettera b)), per cui le due espressioni potrebbero ben riferirsi a concetti distinti.

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

2.1.5. Categorie particolari di dati e dati relativi a condanne penali e a reati

Le disposizioni dell'art. 37, paragrafo 1, lettera c), riguardano il trattamento di categorie particolari di dati ai sensi dell'articolo 9 *e* di dati personali relativi a condanne penali e a reati di cui all'articolo 10. Nonostante l'utilizzo della congiunzione "e" nel testo, non vi sono motivazioni sistematiche che impongano l'applicazione simultanea dei due criteri. Pertanto, il testo deve essere interpretato come se recasse la congiunzione "o". [NdT: il testo italiano del regolamento reca già la congiunzione "o"]

2.2. RPD del responsabile del trattamento

Per quanto riguarda la nomina di un RPD, l'art. 37 non distingue fra titolari[17] e responsabili[18] del trattamento in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare ovvero il solo responsabile, oppure sia l'uno sia l'altro a dover nominare un RPD; questi ultimi saranno poi tenuti alla reciproca collaborazione.

[17] Ai sensi della definizione contenuta all'art. 4, punto 7, il titolare del trattamento è la persona o l'organismo che determina le finalità e i mezzi del trattamento.
[18] Ai sensi della definizione contenuta all'art. 4, punto 8, il responsabile del trattamento è la persona o l'organismo che tratta dati personali per conto del titolare del trattamento.

Vale la pena di evidenziare che anche qualora il titolare sia tenuto, in base ai criteri suddetti, a nominare un RPD, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi.

Alcuni esempi:

- Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oltre all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata di attività. Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare, svolge, nel suo complesso, trattamenti su larga scala. Ne deriva che il responsabile deve nominare un RPD ai sensi dell'art. 37, primo paragrafo, lettera b); al contempo, l'azienda in quanto tale non è soggetta all'obbligo di nomina del RPD.
- Un'azienda di medie dimensioni che produce rivestimenti in ceramica incarica un responsabile esterno della gestione dei servizi di salute occupazionale; tale responsabile ha un numero elevato di clienti con caratteristiche analoghe. Il responsabile è tenuto a nominare un RPD ai sensi dell'art. 37, primo paragrafo, lettera b), poiché svolge trattamenti su larga scala. Tuttavia, l'azienda non è tenuta necessariamente allo stesso adempimento.

Il RPD nominato da un soggetto responsabile del trattamento vigila anche sulle attività svolte da tale soggetto quando operi in qualità di autonomo titolare del trattamento – per esempio, rispetto ai dati concernenti il personale, le risorse informatiche, la logistica.

2.3. Designazione di un unico RPD per più organismi

L'articolo 37, paragrafo 2, consente a un gruppo imprenditoriale di nominare un unico RPD a condizione che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati,[19] l'autorità di controllo[20] e i soggetti interni all'organismo o all'ente, visto che uno dei compiti del RPD consiste nell' "*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento*".[21]

Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD.[22]

[19] V. art. 38, paragrafo 4: "*Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento*."

[20] V. art. 39, paragrafo 1, lettera 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 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione*."

[21] Art. 39, paragrafo 1, lettera a).

[22] V. anche paragrafo 2.6 *infra*.

Il RPD, se necessario con il supporto di un *team* di collaboratori, deve essere in grado di comunicare con gli interessati[23] in modo efficiente e di collaborare[24] con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

Ai sensi dell'articolo 37, terzo paragrafo, è ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare o il responsabile deve assicurarsi che un unico RPD, se necessario supportato da un *team* di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

2.4. Accessibilità e localizzazione del RPD

Ai sensi dell'art. 4 [sic] del RGPD, l'accessibilità del RPD deve essere effettivamente tale. Per garantire tale accessibilità, il WP29 raccomanda che il RPD sia localizzato nel territorio dell'Unione europea, indipendentemente dal fatto che il titolare o il responsabile siano stabiliti nell'Ue.

Tuttavia, non si può escludere che, in alcuni casi ove il titolare o il responsabile non sono stabiliti nell'Ue[25], un RPD sia in grado di svolgere i propri compiti con maggiore efficacia operando al di fuori del territorio dell'Ue.

2.5. Conoscenze e competenze del RPD

In base all'articolo 37, paragrafo 5, il RPD "*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 39*". Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

- **Conoscenze specialistiche**

Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a

[23] V. art. 12, paragrafo 1: "*Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.*"
[24] V. art. 39, paragrafo 1, lettera d: "*cooperare con l'autorità di controllo.*"
[25] V. art. 3 del RGPD per quanto concerne l'ambito territoriale di applicazione.

trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del RPD, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi.

- **Qualità professionali**

L'articolo 37, paragrafo 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un RPD; tuttavia, sono pertinenti al riguardo la conoscenza da parte del RPD della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del RGPD. Proficua anche la promozione di una formazione adeguata e continua rivolta ai RPD da parte delle Autorità di controllo.

E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare; inoltre, il RPD dovrebbe avere buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

- **Capacità di assolvere i propri compiti**

Per capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del RPD, sia quanto dipende dalla posizione del RPD all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il RPD dovrebbe perseguire in via primaria l'osservanza delle disposizioni del RGPD. Il RPD svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento[26], i diritti degli interessati[27], la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita[28], i registri delle attività di trattamento[29], la sicurezza dei trattamenti[30] e la notifica e comunicazione delle violazioni di dati personali.[31]

- **RPD sulla base di un contratto di servizi**

La funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale RPD soddisfi tutti i requisiti applicabili come fissati nella Sezione 4

[26] Capo II
[27] Capo III
[28] Art. 25.
[29] Art. 30.
[30] Art. 32.
[31] Artt. 33 e 34

del RGPD; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Pari importanza riveste il fatto che ciascuno dei soggetti in questione goda delle tutele previste dal RGPD: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto RPD, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di RPD. Al contempo, si potranno associare le competenze e le capacità individuali affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.

Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il *team* RPD, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del *team* RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

2.6. Pubblicazione e comunicazione dei dati di contatto del RPD

L'articolo 37, settimo paragrafo, del RGPD impone al titolare o al responsabile del trattamento

- di pubblicare i dati di contatto del RPD, e
- di comunicare i dati di contatto del RPD alle pertinenti autorità di controllo.

Queste disposizioni mirano a garantire che tanto gli interessati (all'interno o all'esterno dell'ente/organismo titolare o responsabile) quanto le autorità di controllo possano contattare il RPD in modo facile e diretto senza doversi rivolgere a un'altra struttura operante presso il titolare/responsabile. Anche la confidenzialità riveste pari importanza; per esempio, i dipendenti possono essere riluttanti a presentare reclami al RPD se non viene garantita la confidenzialità delle loro comunicazioni. Il RPD è tenuto a osservare le norme in materia di segreto o confidenzialità nello svolgimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri (art. 38, paragrafo 5).

I dati di contatto del RPD dovrebbero comprendere tutte le informazioni che consentono agli interessati e all'autorità di controllo di raggiungere facilmente il RPD stesso: recapito postale, numero telefonico dedicato e/o indirizzo dedicato di posta elettronica. Se opportuno, per facilitare la comunicazione con il pubblico, si potrebbero indicare anche canali ulteriori: una hotline dedicata, un modulo specifico per contattare il RPD pubblicato sul sito del titolare/responsabile.

In base all'articolo 37, settimo paragrafo, del RGPD non è necessario pubblicare anche il nominativo del RPD. Seppure ciò rappresenti con ogni probabilità di una buona prassi, spetta al titolare o al responsabile e allo stesso RPD stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze.[32] Tuttavia, comunicare il nominativo del RPD all'autorità di controllo è fondamentale affinché il RPD funga da punto di contatto fra il singolo ente o organismo e l'autorità di controllo stessa (art. 39, paragrafo 1, lettera e)).

[32] Si osservi che l'art. 33, paragrafo 3, lettera b), ove sono indicate le informazioni da fornire all'autorità di controllo e agli interessati in caso di violazione dei dati personali, prevede, a differenza dell'art. 37, paragrafo 7, che tali informazioni comprendano anche il nominativo (e non solo le informazioni di contatto) del RPD.

In termini di buone prassi, il WP29 raccomanda, inoltre, che il titolare/responsabile comunichi ai dipendenti il nominativo e i dati di contatto del RPD. Per esempio, queste informazioni (nominativo e dati di contatto) potrebbero essere pubblicate sulla intranet del titolare/responsabile, inserite nell'elenco telefonico interno e nei diversi organigrammi della struttura.

3. Posizione del RPD

3.1. Coinvolgimento del RPD in tutte le questioni riguardanti la protezione dei dati personali

Ai sensi dell'articolo 38 del RGPD, il titolare e il responsabile assicurano che il RPD sia "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".

E' essenziale che il RPD, o il suo *team* di collaboratori, sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il RPD vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni.[33] Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Ciò significa che occorrerà garantire, per esempio:

- che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il WP29 raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD;
- che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Ove opportuno, il titolare o il responsabile potrebbero mettere a punto linee-guida ovvero programmazioni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria del RPD.

3.2. Risorse necessarie

[33] Art. 35, paragrafo 2.

L'articolo 38, secondo paragrafo, del RGPD obbliga il titolare o il responsabile a sostenere il RPD "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*". Ciò si traduce, in modo particolare, nelle indicazioni seguenti:

- supporto attivo delle funzioni del RPD da parte del *senior management* (per esempio, a livello del consiglio di amministrazione);
- tempo sufficiente per l'espletamento dei compiti affidati al RPD. Ciò riveste particolare importanza se viene designato un RPD interno con un contratto part-time, oppure se il RPD esterno si occupa di protezione dati oltre a svolgere altre incombenze. In caso contrario, il rischio è che le attività cui il RPD è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità. E' fondamentale disporre di tempo sufficiente da dedicare allo svolgimento dei compiti previsti per il RPD; una prassi da raccomandare consiste nel definire la percentuale del tempo lavorativo destinata alle attività di RPD quando quest'ultimo svolga anche altre funzioni. Un'altra buona prassi consiste nello stabilire il tempo necessario per adempiere alle relative incombenze, definire il livello di priorità spettante a tale incombenze, e prevedere che il RPD stesso (ovvero l'azienda/l'organismo titolare o responsabile) rediga un piano di lavoro;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della nomina del RPD a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/dell'organismo;
- accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al RPD supporto, informazioni e input essenziali;
- formazione permanente. I RPD devono avere la possibilità di curare il proprio aggiornamento con riguardo agli sviluppi nel settore della protezione dati. Ciò mira, in ultima analisi, a consentire un incremento continuo del livello di competenze proprio dei RPD, che dovrebbero essere incoraggiati a partecipare a corsi di formazione su materie attinenti alla protezione dei dati e ad altre occasioni di professionalizzazione (forum in materia di privacy, workshop, ecc.);
- alla luce delle dimensioni e della struttura della singola azienda/del singolo organismo, può risultare necessario costituire un ufficio o un gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale). In casi del genere, è opportuno definire con precisione la struttura interna del gruppo di lavoro nonché i compiti e le responsabilità individuali. Analogamente, se la funzione di RPD viene esercitata da un fornitore di servizi esterno all'azienda/all'organismo, potrà aversi la costituzione di un gruppo di lavoro formato da soggetti operanti per conto di tale fornitore e incaricati di svolgere le funzioni di RPD sotto la direzione di un responsabile che funga da contatto per il cliente.

In linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.

3.3. Istruzioni e [significato di] "adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente"

L'articolo 38, terzo paragrafo, fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile. In particolare, questi ultimi sono tenuti ad assicurare che il RPD "*non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti*". Il considerando 97 aggiunge che i RPD "*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente*".

Ciò significa che il RPD, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Tuttavia, l'autonomia del RPD non significa che quest'ultimo disponga di un margine decisionale superiore al perimetro dei compiti fissati nell'articolo 39.

Il titolare o il responsabile mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza.[34] Se il titolare o il responsabile assumono decisioni incompatibili con il RGPD e le indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al più alto livello del management e ai decisori. Al riguardo, l'art. 38, paragrafo 3, prevede che il RPD "riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nel quadro della sue funzioni di informazione e consulenza a favore del titolare o del responsabile. Un altro esempio di tale rapporto diretto consiste nella redazione di una relazione annuale delle attività svolte dal RPD da sottoporre al vertice gerarchico.

3.4. Rimozione o penalizzazioni in rapporto all'adempimento dei compiti di RPD

L'articolo 38, terzo paragrafo, prevede che il RPD "*non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti*".

Questa prescrizione mira a potenziare l'autonomia del RPD e ad assicurarne l'indipendenza nell'adempimento dei compiti assegnatigli, attraverso la previsione di un'adeguata tutela.

Il divieto di penalizzazioni menzionato nel RGPD si applica solo con riguardo a quelle penalizzazioni eventualmente derivanti dallo svolgimento dei compiti propri del RPD. Per esempio, un RPD può ritenere che un determinato trattamento comporti un rischio elevato e quindi raccomandare al titolare o al responsabile di condurre una valutazione di impatto, ma questi ultimi non concordano con la valutazione del RPD. In casi del genere non è ammissibile che il RPD sia rimosso dall'incarico per avere formulato la raccomandazione in oggetto.

[34] Articolo 5(2).

Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta. Per esempio, potrebbero consistere nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al RPD in rapporto alle attività da questi svolte.

Viceversa, e conformemente alle normali regole di gestione applicabili a ogni altro dipendente o fornitore soggetto alla disciplina del rispettivo contratto nazionale ovvero alle norme di diritto penale e del lavoro, sarebbe legittimamente possibile interrompere il rapporto con il RPD per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche.

In questo ambito va rilevato che il RGPD non specifica le modalità e la tempistica riferite alla cessazione del rapporto di lavoro del RPD o alla sua sostituzione. Tuttavia, quanto maggiore è la stabilità del contratto stipulato con il RPD e maggiori le tutele previste contro l'ingiusto licenziamento, tanto maggiore sarà la probabilità che l'azione del RPD si svolga in modo indipendente. Il WP29 vede, quindi, con favore ogni iniziativa assunta in tal senso dai titolari e responsabili di trattamento.

3.5. Conflitto di interessi

In base all'art. 38, paragrafo 6, al RPD è consentito di "*svolgere altri compiti e funzioni*", ma a condizione che il titolare o il responsabile del trattamento si assicuri che "*tali compiti e funzioni non diano adito a un conflitto di interessi*".

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un RPD può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi. Ciò significa, in modo particolare, che un RPD non può rivestire, all'interno dell'organizzazione del titolare o del responsabile, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare o responsabile.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare o del responsabile riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

A seconda delle attività, delle dimensioni e della struttura organizzativa del titolare o del responsabile, si possono indicare le seguenti buone prassi:

- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di RPD;
- redigere regole interne a tale scopo onde evitare conflitti di interessi;

- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;
- dichiarare che il RPD non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di RPD, al fine di sensibilizzare rispetto al requisito in questione;
- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale RPD ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da prevenire conflitti di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il RPD sia designato fra soggetti interni o esterni all'organizzazione.

4. Compiti del RPD

4.1. Sorvegliare l'osservanza del RGPD

L'art. 39, paragrafo 1, lettera b), affida al RPD, fra gli altri, il compito di sorvegliare l'osservanza del RGPD. Nel considerando 97 si specifica che il titolare o il responsabile del trattamento dovrebbe essere "*assistito [dal RPD] nel controllo del rispetto a livello interno del presente regolamento*".

Fanno parte di questi compiti di controllo svolti dal RPD, in particolare,

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità,
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Il controllo del rispetto del regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza. Il RGPD chiarisce che spetta al titolare, e non al RPD, "*mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*" (art. 24, paragrafo 1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del RPD.

4.2. Il ruolo del RPD nella valutazione di impatto sulla protezione dei dati

In base all'art. 35, paragrafo 1, spetta al titolare del trattamento, e non al RPD, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese). Tuttavia, il RPD svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o *data protection by design*), l'art. 35, secondo paragrafo, prevede in modo specifico che il titolare "*si consulta*" con il RPD quando svolge una DPIA. A sua volta, l'art. 39, primo paragrafo, lettera c) affida al RPD il compito di "*fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35*".

Il WP29 raccomanda che il titolare si consulti con il RPD, fra l'altro, sulle seguenti tematiche:[35]

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD.

Qualora il titolare non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.[36]

Inoltre, il WP29 raccomanda che il titolare definisca con chiarezza, per esempio nel contratto stipulato con il RPD, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa, i compiti specificamente affidati al RPD e i rispettivi ambiti, con particolare riguardo alla conduzione della DPIA.

4.3. Cooperazione con l'autorità di controllo e funzione di punto di contatto

In base all'art. 39, paragrafo 1, lettere d) ed e), il RPD deve "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 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".

Questi compiti attengono al ruolo di "facilitatore" attribuito al RPD e già menzionato nell'introduzione alle presenti Linee-guida. Il RPD funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuitile dall'art. 57 nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'art. 58. Si è già rilevato che il RPD è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità del diritto dell'Unione o degli Stati membri (art. 38, paragrafo 5); tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il RPD di contattare e chiedere lumi all'autorità di controllo. L'art. 39, paragrafo 1, prevede che il RPD possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

4.4. Approccio basato sul rischio

[35] I compiti del RPD sono elencati all'art. 39, paragrafo 1, ove si specifica che il RPD deve svolgere "*almeno*" i compiti in questione. Ne deriva che niente vieta al titolare di assegnare al RPD compiti ulteriori rispetto a quelli espressamente menzionati all'art. 39, paragrafo 1, ovvero di specificare ulteriormente i suddetti compiti.

[36] L'art. 24, paragrafo 1, prevede che "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire,* ***ed essere in grado di dimostrare****, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario"*.

In base all'art. 39, secondo paragrafo, il RPD deve "*considera[re] debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*".

Si tratta di una disposizione di portata generale e ispirata a criteri di buon senso, verosimilmente applicabile sotto molti riguardi all'attività quotidiana del RPD. In sostanza, si chiede al RPD di definire un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati. Seppure ciò non significhi che il RPD debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, di fatto la disposizione segnala l'opportunità di dedicare attenzione prioritaria agli ambiti che presentino rischi più elevati.

Attraverso questo approccio selettivo e pragmatico, il RPD dovrebbe essere più facilmente in grado di consigliare al titolare quale metodologia seguire nel condurre una DPIA, a quali settori riservare un audit interno o esterno in tema di protezione dei dati, quali attività di formazione interna prevedere per il personale o gli amministratori che trattino dati personali, e a quali trattamenti dedicare maggiori risorse e tempo.

4.5. Il ruolo del RPD nella tenuta del registro delle attività di trattamento

L'art. 30, primo e secondo paragrafo, prevede che sia il titolare o il responsabile del trattamento, e non il RPD, a "*ten[ere] un registro delle attività di trattamento svolte sotto la propria responsabilità*" ovvero "*un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento*".

Nella realtà, sono spesso i RPD a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'Ue.[37]

L'art. 39, primo paragrafo, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, niente vieta al titolare o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile.

In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'art. 30 deve essere considerato anche uno strumento che consente al titolare e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione.

[37] Si veda l'art. 24, paragrafo 1, lettera d), del regolamento (CE) 45/2001.

5. ALLEGATO ALLE LINEE-GUIDA SUL RPD – INDICAZIONI ESSENZIALI

L'allegato intende rispondere, in forma sintetica e semplificata, ad alcune delle domande fondamentali rispetto al nuovo obbligo di designazione di un RPD fissato nel regolamento generale sulla protezione dei dati

Designazione del RPD

1. Chi è tenuto a designare un RPD?

La designazione di un RPD è obbligatoria:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
- se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Si tenga presente che la designazione obbligatoria di un RPD può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'Ue. Inoltre, anche ove la designazione di un RPD non sia obbligatoria, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (WP29) incoraggia un approccio di questo genere. Qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria.

Fonte: articolo 37(1) RGPD

2. Cosa significa "attività principali"?

Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare o del responsabile. Per esempio, il trattamento di dati relativi alla salute (come le cartelle sanitarie dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un RPD.

D'altra parte, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale ovvero dispongono di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o perfino essenziali sono considerate solitamente di natura accessoria e non vengono annoverate fra le attività principali.

Fonte: art. 37, paragrafo 1, lettere b) e c) RGPD

3. Cosa significa "su larga scala"?

Il regolamento non definisce cosa rappresenti un trattamento "su larga scala". Il WP29 raccomanda di tenere conto, in particolare, dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Fonte: art. 37, paragrafo 1, lettere b) e c), RGPD

4. Cosa significa "monitoraggio regolare e sistematico"?

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, esso comprende senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Non si tratta, però, di un concetto riferito esclusivamente all'ambiente online.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta

elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Fonte*: *art. 37, paragrafo 1, lettera b), RGPD

5. E' ammessa la designazione congiunta di uno stesso RPD da parte di più soggetti? E a quali condizioni?

Sì. Un gruppo imprenditoriale può nominare un unico RPD a condizione che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente. Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD. Il RPD, supportato da un apposito *team* se necessario, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

È ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare o il responsabile deve assicurarsi che un unico RPD, se necessario supportato da un *team* di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici

Fonte: art. 37, paragrafi 2) e 3), RGPD

6. Dove dovrebbe collocarsi il RPD?

Per garantire l'accessibilità del RPD, il WP29 raccomanda la sua collocazione nel territorio dell'Unione europea, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile nell'Ue. Tuttavia, non si può escludere che un RPD sia in grado di adempiere ai propri compiti con maggiore efficacia operando al di fuori dell'Ue in alcuni casi ove titolare o responsabile non sono stabiliti nel territorio dell'Unione europea.

7. Si può designare un RPD esterno?

Sì. Il RPD può far parte del personale del titolare o del responsabile del trattamento (RPD interno) ovvero "*assolvere i suoi compiti in base a un contratto di servizi*". In quest'ultimo caso il RPD sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.
Se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un *team* operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale RPD soddisfi tutti i requisiti applicabili come fissati nel RGPD.
Per favorire efficienza e correttezza e prevenire conflitti di interesse a carico dei componenti il *team*, le linee-guida raccomandano di procedere a una chiara ripartizione dei compiti nel *team* del RPD esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

Fonte: art. 37, paragrafo 6, RGPD

8. Quali sono le qualità professionali che un RPD deve possedere?

Il RPD "*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 [rispettivi] compiti*".

Il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto.

Fra le competenze e conoscenze specialistiche pertinenti rientrano le seguenti:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del RGPD;
- familiarità con le operazioni di trattamento svolte;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;

- conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile:
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

Fonte: art. 37, paragrafo 5, RGPD

Posizione del RPD

9. Quali sono le risorse che titolare o responsabile dovrebbero mettere a disposizione del RPD?

Il RPD deve disporre delle risorse necessarie per assolvere i propri compiti.

A seconda della natura dei trattamenti, e delle attività e dimensioni della struttura del titolare o del responsabile del trattamento, il RPD dovrebbe poter contare sulle seguenti risorse:

- supporto attivo della funzione di RPD da parte del *senior management;*
- tempo sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della designazione del RPD a tutto il personale;
- accesso garantito ad altri servizi all'interno della struttura del titolare/del responsabile in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

Fonte: art. 38, paragrafo 2, RGPD

10. Quali sono le garanzie che possono consentire al RPD di operare con indipendenza? Cosa significa "conflitto di interessi"?

Vi sono numerose garanzie che possono consentire al RPD di operare in modo indipendente:

- nessuna istruzione da parte del titolare o del responsabile per quanto riguarda lo svolgimento dei compiti affidati al RPD;
- nessuna penalizzazione o rimozione dall'incarico in rapporto allo svolgimento dei compiti affidati al RPD;
- nessun conflitto di interessi con eventuali ulteriori compiti e funzioni.

Gli "altri compiti e funzioni" del RPD non devono comportare conflitti di interessi. Ciò significa, in primo luogo, che il RPD non può rivestire, all'interno dell'organizzazione del titolare o del responsabile, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare o responsabile.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione con riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane,

responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

Fonte: art. 38, paragrafi 3 e 6, RGPD

Compiti del RPD

11. Che cosa si intende per "sorvegliare l'osservanza"

Fanno parte di questi compiti di controllo svolti dal RPD, in particolare,

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità, e
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Fonte: art. 39, paragrafo 1, lettera b), RGPD

12. Il RPD è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati?

No, il RPD non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare / sul responsabile del trattamento.

13. Quale ruolo spetta al RPD con riguardo alla valutazione di impatto sulla protezione dei dati e alla tenuta del registro dei trattamenti?

Per quanto concerne la valutazione di impatto sulla protezione dei dati, il titolare o il responsabile dovrebbero consultarsi con il RPD, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

In merito al registro dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare o sul responsabile, e non sul RPD. Cionondimeno, niente vieta al titolare o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare o del responsabile.

Fonte: art. 39, paragrafo 1, lettera c) e art. 30, RGPD

Bruxelles, 13 dicembre 2016

Per il Gruppo di lavoro
La presidente

Isabelle FALQUE-PIERROTIN

Versione emendata e adottata in data 5 aprile 2017

17/EN
WP 248

Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679

Adottate il 4 aprile 2017
Versione successivamente emendata e adottata il 4 ottobre 2017

INDICE

IL GRUPPO DI LAVORO SULLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli Articoli 29 e 30 della stessa,

visto il proprio regolamento,

HA ADOTTATO LE PRESENTI LINEE-GUIDA:

I. Introduzione

Il regolamento 2016/679[1] (RGPD) sarà applicabile a partire dal 25 maggio 2018. L'art. 35 del RGPD introduce la nozione di valutazione di impatto sulla protezione dei dati (DPIA, utilizzando l'acronimo inglese per *Data Protection Impact Assessment*)[2], e lo stesso dicasi per la direttiva 2016/680[3].

Una DPIA consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali[4] (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli). La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di

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

[2] In altri contesti si trova spesso utilizzato anche l'acronimo "PIA" (*Privacy Impact Assessment*, ossia Valutazione di impatto sulla privacy), con identico riferimento concettuale.

[3] Anche in base all'art. 27 della direttiva (Ue) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento di 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, è necessario effettuare una valutazione di impatto sulla protezione dei dati con riguardo a un trattamento che "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

[4] Nel regolamento non si individua una definizione formale di DPIA in quanto tale, tuttavia

- i contenuti minimi della DPIA sono specificati come segue all'art. 35, paragrafo 7:
  - "*a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*
  - *b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*
  - *c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;*
  - *d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione*";
- il valore e il ruolo della DPIA sono chiariti nel Considerando 84 nei termini seguenti: "*Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio.*"

tali prescrizioni (si veda anche l'art. 24)[5]. In altri termini, **la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme**.

In base al regolamento, l'inosservanza degli obblighi concernenti la DPIA può comportare l'imposizione di sanzioni pecuniarie da parte della competente autorità di controllo. Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (art. 35, paragrafi 1 e 3-4), lo svolgimento non corretto di una DPIA (art. 35, paragrafi 2 e 7-9) o la mancata consultazione dell'autorità di controllo competente ove ciò sia necessario (art. 36, paragrafo 3, lettera e)) possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

II. Oggetto

Le presenti linee-guida tengono conto di quanto segue:

- la dichiarazione del Gruppo di lavoro "Articolo 29" (WP29), 14/EN WP218[6];
- le linee-guida del WP29 in materia di responsabili della protezione dei dati (RPD/DPO), 16/EN WP243;[7]
- il parere del WP29 sul principio di limitazione della finalità, 13/EN WP2013[8];
- standard internazionali[9].

Coerentemente con l'approccio basato sul rischio che informa l'intero RGPD, lo svolgimento di una DPIA non è obbligatorio per ogni singolo trattamento. La DPIA è necessaria solo se il trattamento "può comportare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35, paragrafo 1). Al fine di assicurare un'interpretazione coerente dei casi di obbligatorietà della DPIA (art. 35, paragrafo 3), le presenti linee-guida vogliono chiarire, in primo luogo, il concetto stesso di DPIA e fornire, quindi, alcuni criteri in vista dell'elaborazione degli elenchi che le autorità di controllo sono tenute ad adottare in base all'art. 35, paragrafo 4.

Ai sensi dell'art. 70, paragrafo 1, lettera e), il Comitato europeo per la protezione dei dati (CEPD) potrà pubblicare linee-guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del RGPD. Scopo del presente documento è precorrere questa funzione attribuita al CEPD e, quindi, chiarire le pertinenti disposizioni del regolamento così da contribuire all'osservanza delle norme da parte dei titolari e assicurare certezza del diritto per quei titolari che siano tenuti a svolgere una DPIA.

Le linee-guida vogliono, inoltre, favorire la definizione di

---

[5] Si veda anche il Considerando 84: "*L'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento*."

[6] Dichiarazione del WP29 (14/EN WP218) relativa al ruolo di un approccio basato sul rischio nel quadro normativo in materia di protezione dati, adottata il 30 maggio 2014 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[7] Linee-guida del WP29 sui responsabili della protezione dei dati, 16/EN WP243, adottate il 13 dicembre 2016 - http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

[8] Parere 3/2013 del WP29 sul principio di limitazione della finalità, 13/EN WP203, adottato il 2 aprile 2013 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[9] Per esempio ISO 31000:2009, *Risk management – Principles and guidelines*, International Organization for Standardization (ISO); ISO/IEC 20134 (project), *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

- un elenco condiviso a livello Ue di trattamenti per i quali la DPIA è obbligatoria (art. 35, paragrafo 4);
- un elenco condiviso a livello Ue di trattamenti per i quali la DPIA non è necessaria (art. 35, paragrafo 5);
- criteri condivisi rispetto alla metodologia di svolgimento della DPIA (art. 35, paragrafo 5);
- criteri condivisi rispetto ai casi di consultazione obbligatoria dell'autorità di controllo (art. 36, paragrafo 1);
- raccomandazioni, ove possibile fondate sull'esperienza raccolta negli Stati membri dell'Ue.

III. DPIA: cosa prevede il regolamento

Il regolamento impone ai titolari di mettere in atto misure idonee a garantire ed essere in grado di dimostrare l'osservanza del regolamento stesso, tenendo conto, fra gli altri, dei "*rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*" (art. 24, paragrafo 1). L'obbligo di condurre una DPIA, in determinate circostanze, deve essere collocato nel contesto del più generale obbligo imposto ai titolari di gestire correttamente i rischi connessi al trattamento di dati personali.

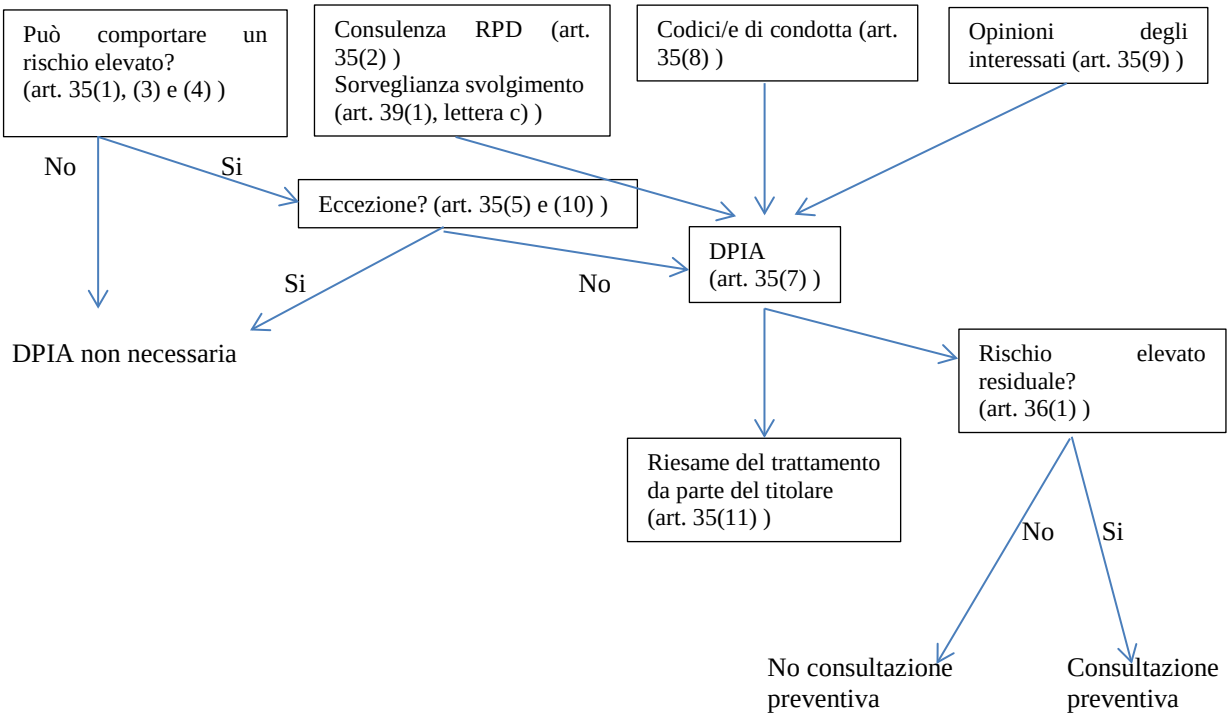
Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità. D'altro canto, la "gestione del rischio" è definibile come l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio.

L'art. 35 del regolamento menziona la probabilità di un rischio elevato "*per i diritti e le libertà delle persone fisiche*".

Come già chiarito dal Gruppo di lavoro "Articolo 29" nella "Dichiarazione" sul ruolo di un approccio basato sul rischio nel contesto giuridico della protezione dei dati, il riferimento ai "diritti e le libertà" degli interessati va inteso in primo luogo come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

Coerentemente con l'approccio basato sul rischio che informa il regolamento, non è obbligatorio condurre una DPIA per ogni singolo trattamento. Viceversa, la DPIA è obbligatoria solo se una determinata tipologia di trattamenti "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, paragrafo 1). Tuttavia, la semplice circostanza per cui non siano soddisfatte le condizioni che generano un obbligo di condurre la DPIA non riduce in alcun modo l'obbligo più generale cui soggiacciono i titolari di mettere in atto misure finalizzate a gestire in modo idoneo i rischi per i diritti e le libertà degli interessati. Nella pratica, ciò significa che i titolari devono valutare in modo continuativo i rischi creati dai propri trattamenti così da individuare quelle situazioni in cui una determinata tipologia di trattamenti "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche*".

La figura seguente illustra i principi fondamentali concernenti la DPIA in base al RGPD:



A. <u>Qual è l'oggetto della DPIA? Un singolo trattamento ovvero un insieme di trattamenti simili</u>

Una DPIA può riguardare un singolo trattamento; tuttavia, l'art. 35, paragrafo 1, prevede che "*Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*", e il considerando 92 aggiunge che "*Vi sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata*".

È **possibile utilizzare un'unica DPIA per valutare più trattamenti che presentano analogie** in termini di natura, ambito, contesto, finalità e rischi. In effetti, le valutazioni di impatto mirano a svolgere un'analisi sistematica di situazioni nuove che potrebbero comportare rischi elevati per i diritti e le libertà delle persone fisiche, e non occorre condurre una DPIA per quei trattamenti - svolti in un contesto specifico e per una specifica finalità – che siano già stati oggetto di analisi. Un esempio potrebbe essere offerto dall'utilizzo di tecnologie simili per raccogliere le stesse tipologie di dati per le identiche finalità; si pensi a un gruppo di autorità locali che decidano di installare ciascuna un analogo sistema di videosorveglianza: sarebbe possibile svolgere un'unica DPIA che prenda in esame il trattamento svolto da questi distinti titolari; oppure si pensi a un operatore ferroviario (unico titolare del trattamento) che potrebbe svolgere un'unica DPIA con riguardo all'impiego della videosorveglianza in tutte le stazioni ferroviarie di competenza. Lo stesso dicasi per trattamenti analoghi effettuati da titolari diversi; in casi del genere, sarebbe opportuno che una

DPIA utilizzabile come riferimento venga condivisa o resa accessibile al pubblico, con l'obbligo di dare attuazione alle misure in essa delineate, mentre si dovrebbe giustificare la scelta di condurre una DPIA isolata.

Quando un trattamento è svolto in contitolarità, è necessario che ciascun contitolare definisca con precisione gli obblighi rispettivamente incombenti. La DPIA dovrebbe stabilire chi ha la responsabilità delle singole misure finalizzate alla gestione dei rischi e alla tutela dei diritti e delle libertà degli interessati. Ciascun titolare dovrebbe indicare con chiarezza le rispettive esigenze e condividere tutte le informazioni utili senza pregiudicare quanto coperto da segreto (per esempio, informazioni tutelate dal segreto commerciale, soggette a diritti di proprietà intellettuale, informazioni economiche riservate) né rivelare eventuali vulnerabilità.

Una DPIA può rivelarsi utile anche per valutare l'impatto di un nuovo dispositivo tecnologico in termini di protezione dei dati; è il caso, per esempio, di un nuovo prodotto hardware o software, se utilizzabile da titolari diversi per svolgere trattamenti diversi. Naturalmente il titolare che utilizzi tale prodotto resta tenuto a condurre una distinta DPIA rispetto alla specifica implementazione, ma – ove opportuno – tale DPIA può essere informata alla DPIA predisposta dal fornitore del prodotto. A titolo di esempio, si pensi al rapporto che sussiste fra produttori di contatori intelligenti e società fornitrici di elettricità. Ciascun fornitore del prodotto come anche ciascun soggetto che effettui trattamenti attraverso tale prodotto dovrebbe condividere ogni informazione utile senza pregiudicare quanto è protetto da segreto né generare rischi in termini di sicurezza a causa della rivelazione di eventuali vulnerabilità.

B. Quali trattamenti sono soggetti a DPIA? Quelli che "*possono presentare un rischio elevato*", salve eccezioni

In questo paragrafo si esaminano i casi in cui la DPIA è obbligatoria e quelli in cui essa non è necessaria.

A meno che il trattamento ricada nelle eccezioni previste (III.B.b.), la DPIA deve essere condotta qualora un trattamento "possa presentare un rischio elevato" (III.B.a).

a) Quando sussiste l'obbligo di condurre una DPIA? Qualora un trattamento "*possa presentare un rischio elevato*"

Il regolamento non impone di condurre una DPIA con riguardo a ogni trattamento che possa comportare rischi per i diritti e le libertà delle persone fisiche. La DPIA è obbligatoria solo qualora un trattamento "*possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, paragrafo 1), come meglio chiarito dal paragrafo 3 dell'art. 35 e integrato da quanto prevede il paragrafo 4 dello stesso articolo. Si tratta di un requisito particolarmente pertinente qualora si intenda introdurre una tecnologia di trattamento innovativa.[10]

Se la necessità di una DPIA non emerge con chiarezza, il WP29 raccomanda di farvi comunque ricorso in quanto la DPIA contribuisce all'osservanza delle norme in materia di protezione dati da parte dei titolari di trattamento.

Benché una DPIA possa risultare necessaria in altre circostanze, l'art. 35, paragrafo 3, cita alcuni esempi di trattamenti che "*possono risultare in un rischio elevato*":

[10] Si vedano i considerando 89, 91 e l'art. 35, paragrafi (1) e (3), quanto a esemplificazioni ulteriori.

"(a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche[11]*;*
- (b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10[12]*; o*
- (c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

Come segnalato dall'utilizzo della locuzione "in particolare" nel paragrafo 3 dell'art. 35, l'elenco di cui sopra non ha pretese di esaustività. Possono esservi trattamenti "a rischio elevato" che non sono ricompresi nell'elenco in questione, pur comportando rischi elevati in misura analoga. Anche questi trattamenti dovrebbero essere oggetto di DPIA. Per tale motivo, i criteri elaborati nel prosieguo si spingono talora oltre la mera illustrazione di cosa debba intendersi in rapporto ai tre esempi forniti nell'art. 35, paragrafo 3, del regolamento.

Allo scopo di fornire indicazioni più concrete rispetto ai trattamenti che richiedono una DPIA a causa del rischio inerentemente elevato, e tenendo conto degli elementi specifici contenuti negli articoli 35, paragrafo 1, e 35, paragrafo 3, lettere a)-c), nonché degli elenchi di cui è prevista l'adozione a livello nazionale in base all'art. 35, paragrafo 4, dei considerando 71, 75 e 91, e degli altri riferimenti contenuti nel regolamento a trattamenti "*che possono presentare un rischio elevato*"[13], è opportuno prendere in esame i seguenti nove criteri:

1. Trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, in particolare a partire da "*aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*" (considerando 71 e 91). A titolo esemplificativo si possono citare un istituto finanziario che effettui lo screening dei propri clienti utilizzando un database di rischio creditizio ovvero un database per la lotta alle frodi o al riciclaggio e al finanziamento del terrorismo (AML/CTF); una società operante nel settore delle biotecnologie che offra test genetici direttamente ai consumatori per finalità predittive del rischio di determinate patologie o in generale per lo stato di salute; una società che crei profili comportamentali o di marketing a partire dalle operazioni o dalla navigazione compiute sul proprio sito web.
2. Decisioni automatizzate che producono significativi effetti giuridici o di analoga natura: trattamenti finalizzati ad assumere decisioni su interessati che producano "*effetti giuridici sulla persona fisica*" ovvero che "*incidono in modo analogo significativamente su dette persone fisiche*" (art. 35, paragrafo 3, lettera a)). Per esempio, il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione. Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio. Per maggiori dettagli sui concetti in gioco si rimanda alle Linee-guida in materia di profilazione che il Gruppo di lavoro si appresta a pubblicare.
3. Monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "*la sorveglianza sistematica di*

[11] Si veda il considerando 71: "*in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*".
[12] Si veda il considerando 75: "*se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza*".
[13] Si vedano, per esempio, i considerando 75, 76, 92, 116.

un'area accessibile al pubblico" (art. 35, paragrafo 3, lettera c)).[14] Questa tipologia di monitoraggio costituisce un criterio, ai fini della DPIA, in quanto la raccolta di dati personali può avvenire in circostanze tali da non consentire agli interessati di comprendere chi vi stia procedendo e per quali finalità. Inoltre, è talora impossibile per gli interessati sottrarsi a questa tipologia di trattamenti in aree pubbliche (o pubblicamente accessibili).

4. Dati sensibili o dati di natura estremamente personale: si tratta delle categorie particolari di dati personali di cui all'art. 9 (per esempio, informazioni sulle opinioni politiche di una persona fisica) oltre ai dati personali relativi a condanne penali o reati di cui all'art. 10. A titolo di esempio, si può citare un ospedale che conserva le cartelle cliniche dei pazienti, o un investigatore privato che conserva informazioni su soggetti responsabili di reati. Al di là di queste disposizioni del regolamento, vi sono talune categorie di dati che possono aumentare i rischi eventuali per i diritti e le libertà delle persone fisiche. Si tratta di dati personali considerati sensibili (nell'accezione comune del termine), in quanto connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza) ovvero in quanto incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) ovvero in quanto una loro violazione comporta evidentemente un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti). A tale proposito, può essere pertinente la circostanza per cui i dati siano già stati resi pubblici dall'interessato ovvero da terzi. Il fatto che un certo dato personale sia disponibile pubblicamente può essere un elemento da prendere in esame nel valutare l'aspettativa di un utilizzo ulteriore di tale dato per determinati scopi. Il criterio in oggetto può riferirsi anche a dati quali documenti personali, email, agende, appunti tratti da lettori elettronici dotati di dispositivi per la presa di appunti, e informazioni molto personali contenute in applicazioni che consentono di tenere traccia del proprio stile di vita.
5. Trattamenti di dati su larga scala: il regolamento non offre definizioni del concetto di "larga scala", anche se il considerando 91 fornisce indicazioni in merito. In ogni caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori seguenti al fine di stabilire se un trattamento sia svolto su larga scala[15]:
    a. numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;
    b. volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;
    c. durata, o persistenza, dell'attività di trattamento;
    d. ambito geografico dell'attività di trattamento.
6. Combinazione o raffronto di insiemi di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato.[16]
7. Dati relativi a interessati vulnerabili (considerando 75): il trattamento di questa tipologia di informazioni rappresenta un criterio ai fini della DPIA in quanto è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento, nel senso che il singolo può non

[14] L'interpretazione del termine "sistematico" fornita dal WP29 (si vedano le "Linee-guida sul responsabile della protezione dei dati" (16/EN WP243)) è la seguente:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Il WP29 interpreta l'espressione "area accessibile al pubblico" nel senso di un luogo aperto alla generalità delle persone, per esempio una piazza, un centro commerciale, una strada, una biblioteca pubblica.

[15] Si vedano le Linee-guida del WP29 in materia di responsabili della protezione dei dati 16/EN WP243.

[16] Si veda l'analisi svolta nel parere del WP29 sul principio di limitazione della finalità 13/EN WP203, p. 24.

disporre del potere di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i minori, che. si può ritenere non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.

8. Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative, come l'associazione fra tecniche dattiloscopiche e riconoscimento del volto per migliorare il controllo degli accessi fisici, e così via. Il regolamento chiarisce (art. 35, paragrafo 1, e considerando 89 e 91) che l'utilizzo di una nuova tecnologia, definito "*in conformità con il grado di conoscenze tecnologiche raggiunto*" (considerando 91), può comportare l'obbligo di condurre una DPIA, in quanto il ricorso a una nuova tecnologia può generare forme innovative di raccolta e utilizzo dei dati cui può associarsi un rischio elevato per i diritti e le libertà delle persone. Nei fatti, le conseguenze sul piano individuale e sociale del ricorso a una nuova tecnologia sono talora ignote. La DPIA aiuterà il titolare a comprendere e gestire tali rischi. Per esempio, alcune applicazioni legate all' "Internet delle cose" potrebbero avere impatti significativi sulla vita privata e le abitudini delle persone, e, quindi, necessitano di una DPIA.
9. Tutti quei trattamenti che, di per sé, "*impediscono [agli interessati] di esercitare un diritto o di avvalersi di un servizio o di un contratto*" (art. 22 e considerando 91). Ciò comprende i trattamenti finalizzati a consentire, modificare o negare l'accesso degli interessati a un servizio o la stipulazione di un contratto. Si pensi, a titolo di esempio, allo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento.

Un titolare può ritenere, nella maggioranza dei casi, che quando un trattamento soddisfa due dei criteri sopra indicati sia necessario condurre una DPIA. In linea di principio, il Gruppo di lavoro ritiene che quanto maggiore è il numero dei criteri soddisfatti da un determinato trattamento, tanto maggiore è la probabilità che esso presenti un rischio elevato per i diritti e le libertà degli interessati e, quindi, che si renda necessaria una DPIA indipendentemente dalle misure che il titolare prevede di adottare.

Tuttavia, in taluni casi **un titolare può ritenere che un trattamento che soddisfa solo uno dei criteri di cui sopra necessiti di una DPIA**.

Gli esempi riportati di seguito illustrano come utilizzare i criteri in oggetto per valutare se un determinato trattamento richieda la conduzione di una DPIA:

Esempi di trattamento	**Criteri pertinenti**	**Obbligo di DPIA probabile?**
Ospedale che tratta dati genetici e sanitari relativi ai pazienti (sistema informativo ospedaliero)	• Dati sensibili o dati di natura estremamente personale • Dati relativi a interessati vulnerabili • Dati trattati su larga scala	
Utilizzo di un sistema di	• Monitoraggio	

videosorveglianza per il controllo del traffico autostradale. Il titolare prevede di utilizzare un sistema intelligente di analisi delle immagini per l'individuazione dei veicoli e il riconoscimento automatico delle targhe	sistematico • Utilizzi innovativi o applicazione di soluzioni tecnologiche o organizzative	Sì
Azienda che controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su Internet, ecc.	• Monitoraggio sistematico • Dati relativi a interessati vulnerabili	
Raccolta di dati pubblici tratti dai *social media* per la creazione di profili	• Valutazione o scoring • Dati trattati su larga scala • Raffronto o combinazione di insiemi di dati • Dati sensibili o dati di natura estremamente personale	
Un'istituzione che crei un database nazionale di valutazioni creditizie o per finalità antifrode	• Valutazione o scoring • Decisioni automatizzate che producono effetti giuridici o incidono in modo analogo sull'interessato in misura significativa • Impedimenti all'esercizio di un diritto o all'utilizzo di un servizio o di un contratto da parte dell'interessato • Dati sensibili o dati di natura estremamente personale	
Conservazione per scopi di archiviazione di dati sensibili pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o studi clinici sperimentali	• Dati sensibili • Dati relativi a interessati vulnerabili • Impedimenti all'esercizio di un diritto o all'utilizzo di un servizio o di un contratto da parte dell'interessato	
Trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91)	• Dati sensibili o dati di natura estremamente personale • Dati relativi a interessati vulnerabili	No
Rivista online che utilizza una mailing list	• Dati trattati su larga	

per inviare agli abbonati un bollettino giornaliero di carattere generale	scala	
Sito di e-commerce che pubblicizza parti di ricambio per auto d'epoca con limitata profilazione riferita ad alcune sezioni del sito e basata sui pregressi acquisti effettuati	• Valutazione o scoring	

Viceversa, può darsi il caso di un trattamento che riflette gli esempi sopra indicati ma che, a giudizio del titolare, non "può presentare un rischio elevato". In casi del genere, il titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando l'opinione del responsabile della protezione dei dati.

Inoltre, il principio di responsabilizzazione prevede che ciascun titolare "*tiene un registro delle attività di trattamento svolte sotto la propria responsabilità*" comprendente, fra l'altro, le finalità del trattamento, una descrizione delle categorie di dati e i destinatari dei dati stessi, nonché "*ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1*" (art. 30, paragrafo 1) e deve valutare se vi sia la probabilità di un rischio elevato anche se potrà decidere, in ultima analisi, di non condurre una DPIA.

Nota: Le autorità di controllo sono tenute a redigere, pubblicare e comunicare al Comitato europeo per la protezione dei dati (CEPD) un elenco dei trattamenti che necessitano di una DPIA (art. 35, paragrafo 4).[17] I criteri sopra indicati possono facilitare la definizione di tale elenco da parte delle autorità di controllo, che potranno eventualmente aggiungere elementi più specifici col tempo. Per esempio, anche il trattamento di qualsiasi tipologia di dato biometrico o di dati relativi a minori potrebbe essere considerato pertinente ai fini dell'inserimento nell'elenco di cui all'art. 35, paragrafo 4.

b) Quando non è necessario condurre una DPIA? Quando il trattamento non "*può comportare un rischio elevato*" o esiste una DPIA simile, o il trattamento è già stato autorizzato prima del maggio 2018, o ha una base legale [SIC], o è compreso nella lista dei trattamenti che non richiedono una DPIA.

Il Gruppo di lavoro ritiene che una DPIA non sia necessaria nei casi seguenti:

- **se il trattamento non *"può comportare un rischio elevato per i diritti e le libertà di persone fisiche"*** (art. 35, paragrafo 1);
- **se la natura, l'ambito, il contesto e le finalità del trattamento sono molto simili a quelli del trattamento per cui è già stata condotta una DPIA**. In casi del genere, si possono utilizzare i risultati della DPIA per trattamenti analoghi (art. 35, paragrafo 1);[18]
- se il trattamento è stato sottoposto a verifica da parte di un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche[19] (v. III.C);

[17] Al riguardo, "*l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione*" (art. 35, paragrafo 6).

[18] "*Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*"

[19] "*Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE restano in vigore fino a quando non vengono modificate, sostituite o abrogate*" (considerando 171).

- **se un trattamento**, conformemente con la lettera c) o e) dell'articolo 6, paragrafo 1, **trova la propria base legale** nel diritto dell'Ue o di uno Stato membro, la base legale in questione disciplina lo specifico trattamento, **ed è già stata condotta una DPIA** all'atto della definizione della base giuridica suddetta (art. 35, paragrafo 10)[20], tranne ove uno Stato membro abbia previsto la necessità di condurre una DPIA per i trattamenti pregressi;
- **se il trattamento è compreso nell'elenco facoltativo (redatto dall'autorità di controllo ai sensi dell'art. 35, paragrafo 5) dei trattamenti** per i quali non è necessario procedere alla DPIA. Tale elenco può riguardare trattamenti conformi alle condizioni specificate dalla singola autorità, in particolare attraverso linee-guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (per esempio, in Francia, attraverso autorizzazioni, deroghe, norme semplificate, pacchetti di conformità, ecc.). In casi del genere, salvo riesame da parte della competente autorità di controllo, la DPIA non è necessaria – ma solo a condizione che il trattamento ricada nello specifico ambito della procedura menzionata nell'elenco e continui a risultare pienamente conforme ai relativi requisiti del regolamento.

C) Per quanto riguarda i trattamenti già in corso? Una DPIA è necessaria in talune circostanze.

L'obbligo di condurre una DPIA vige per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per i quali siano intervenute variazioni dei rischi tenuto conto della natura, dell'ambito, del contesto e delle finalità dei trattamenti stessi.

Non è necessario condurre una DPIA per quei trattamenti che siano stati oggetto di verifica preliminare da parte di un'autorità di controllo o da un responsabile della protezione dei dati(*) e che proseguano con le stesse modalità oggetto di tale verifica. Come indicato nel considerando 171, "*Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate*".

Viceversa, ciò significa che tutti i trattamenti le cui caratteristiche attuative (ambito, finalità, dati personali raccolti, identità di titolari o destinatari, periodi di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla valutazione preliminare svolta dall'autorità di controllo o da un responsabile della protezione dei dati(*), e che possono presentare un rischio elevato, dovrebbero essere oggetto di una DPIA. Inoltre, la necessità di una DPIA potrebbe insorgere al modificarsi dei rischi derivanti dai trattamenti, [21] per esempio a causa del ricorso a una nuova tecnologia oppure dell'utilizzo dei dati personali per una diversa finalità.

I trattamenti tendono a evolvere rapidamente e possono facilmente presentarsi nuove vulnerabilità; pertanto, occorre osservare che la revisione di una DPIA non è soltanto utile ai fini del miglioramento continuo, ma è anche indispensabile per mantenere inalterato il livello di protezione dei dati al mutare delle condizioni nel tempo.

[20] Si osservi che, qualora sia stata condotta una DPIA nella fase di elaborazione dello strumento che offre la base legale per il trattamento, è probabile che sia necessario un riesame prima dell'entrata in vigore poiché lo strumento giuridico adottato può differire da quello proposto in misura tale da incidere sull'impatto in termini di privacy e protezione dei dati. Inoltre, può darsi che non siano disponibili sufficienti informazioni di ordine tecnico rispetto al trattamento in quanto tale al momento dell'adozione dello strumento normativo suddetto, anche se accompagnato da una DPIA; in casi del genere, può risultare comunque necessario condurre una DPIA specifica prima di procedere al trattamento vero e proprio.

(*) Nel nostro paese, l'unico soggetto che dispone di tale potere è il Garante.

[21] In termini di contesto, dati raccolti, funzionalità, dati personali oggetto di trattamento, destinatari, incroci di dati, rischi (beni di supporto, fonti di rischio, impatti potenziali, minacce, ecc.), misure di sicurezza e trasferimenti internazionali.

Una DPIA può rendersi necessaria per il mutamento del contesto organizzativo o sociale relativo a uno specifico trattamento; è il caso, per esempio, degli effetti prodotti da decisioni automatizzate, che possono acquistare maggiore significatività, oppure del presentarsi di nuove categorie di interessati vulnerabili alla discriminazione. Ciascuno di tali esempi potrebbe costituire un elemento in grado di modificare il rischio derivante dallo specifico trattamento.

Peraltro, alcune variazioni potrebbero dare luogo di fatto a una diminuzione del rischio. Per esempio, un trattamento potrebbe evolvere nel senso di non comportare più decisioni automatizzate, oppure un'attività di monitoraggio potrebbe cessare di essere sistematica. In tal caso, il riesame dell'analisi dei rischi precedentemente condotta può indicare che non sussiste più la necessità di condurre una DPIA.

In termini di buone prassi, per i trattamenti in corso dovrebbe essere previsto un riesame continuo della DPIA, **ripetendo la valutazione a intervalli regolari.** Pertanto, anche qualora non vi sia l'obbligo di condurre una DPIA al 25 maggio 2018, sarà necessario che il titolare, al momento opportuno, conduca tale DPIA nel quadro degli obblighi più generali di responsabilizzazione cui ogni titolare soggiace.

D. Come si effettua una DPIA?

a) Quando è opportuno condurre la DPIA? Prima di procedere al trattamento

La DPIA dovrebbe essere condotta "*prima di procedere al trattamento*" (art. 35, paragrafo 1, e art. 35, paragrafo 10; considerando 80 e 93).[22]. Tale impostazione è coerente con i principi di protezione dei dati sin dalla fase di progettazione e per impostazione predefinita (art. 25 e considerando 78). La DPIA deve essere considerata uno strumento di ausilio nel processo decisionale relativo al trattamento.

L'effettuazione della DPIA dovrebbe collocarsi quanto più a monte possibile nella fase di progettazione di un trattamento, anche se non tutte le operazioni di tale trattamento sono già delineate. L'aggiornamento della DPIA nel corso dell'intero ciclo di vita di un determinato progetto garantirà la dovuta considerazione delle tematiche di privacy e protezione dei dati favorendo l'individuazione di soluzioni che promuovano l'osservanza. Talora potrà rendersi necessaria la ripetizione di singole tappe della valutazione con il procedere della fase di sviluppo, in quanto la scelta di determinate misure tecniche o organizzative potrà incidere sulla gravità o sulla probabilità dei rischi posti dal trattamento.

Il fatto che possa rendersi necessario un aggiornamento della DPIA dopo l'inizio effettivo del trattamento non è una buona ragione per differire o evitare di condurre una DPIA. La DPIA è un processo permanente, soprattutto se si ha a che fare con un trattamento dinamico e soggetto a continue trasformazioni. **Lo svolgimento della DPIA è un processo continuativo e non un'attività *una tantum*.**

b) Chi è tenuto a condurre la DPIA? Il titolare, insieme al RPD e al responsabile (o ai responsabili) del trattamento

[22] Tranne in presenza di un trattamento già in corso sottoposto a verifica preliminare da parte dell'autorità di controllo, nel qual caso la DPIA dovrebbe essere condotta prima di apportare modifiche significative al trattamento stesso.

Spetta al titolare garantire l'effettuazione della DPIA (art. 35, paragrafo 2). La conduzione materiale della DPIA può essere affidata a un altro soggetto, interno o esterno all'organismo; tuttavia, la responsabilità ultima dell'adempimento ricade sul titolare del trattamento.

Il titolare deve consultarsi con il responsabile della protezione dei dati (RPD/DPO), ove designato (art. 35, paragrafo 2); tale consultazione e le conseguenti decisioni assunte dal titolare devono essere documentate nell'ambito della DPIA. Il RPD è chiamato anche a monitorare lo svolgimento della DPIA (art. 39, paragrafo 1, lettera c)). Indicazioni ulteriori sono rinvenibili nelle linee-guida del WP29 sul responsabile della protezione dei dati (16/EN WP243).

Se il trattamento è svolto, in tutto o in parte, da un responsabile, **quest'ultimo deve assistere il titolare nella conduzione della DPIA** fornendo ogni informazione necessaria conformemente con l'art. 28, paragrafo 3, lettera f).

Il titolare *"raccoglie le opinioni degli interessati o dei loro rappresentanti" "se del caso"* (art. 35, paragrafo 9). A giudizio del WP29,

- per la raccolta delle opinioni in oggetto si possono individuare molteplici modalità, in rapporto al contesto: per esempio, uno studio generico relativo a finalità e mezzi del trattamento; un quesito rivolto ai rappresentanti del personale; un questionario inviato ai futuri clienti del titolare Il titolare dovrà aver cura di accertarsi dell'esistenza di una base legale per il trattamento di dati personali eventualmente connesso alla raccolta di tali opinioni. Occorre rilevare, tuttavia, che il consenso al trattamento in questione non rappresenta ovviamente una modalità idonea per raccogliere le opinioni degli interessati;
- qualora la decisione assunta in ultima analisi dal titolare si discosti dall'opinione degli interessati, è bene che il titolare documenti le motivazioni che hanno condotto alla prosecuzione o meno del progetto;
- il titolare dovrebbe documentare anche le motivazioni della mancata consultazione degli interessati, qualora decida che quest'ultima non sia opportuna – per esempio, perché potrebbe pregiudicare la riservatezza dei piani aziendali, oppure sarebbe sproporzionata o impraticabile.

Infine, una buona prassi consiste nel definire e documentare eventuali ulteriori ruoli e responsabilità in rapporto alle politiche, ai processi e alle disposizioni interne all'organismo – per esempio:

- se specifiche realtà aziendali propongono di condurre una DPIA, dovrebbero anche fornire input ai fini di tale DPIA e partecipare al relativo processo di validazione;
- se del caso, si raccomanda di consultare esperti indipendenti provenienti da diversi ambiti disciplinari[23] (legale, tecnologico, sicurezza, sociologico, etico, ecc.);
- ruoli e responsabilità dei responsabili di trattamento devono essere fissati in strumenti contrattuali, e la DPIA dovrebbe essere condotta con il supporto del responsabile, tenendo conto della natura del trattamento e delle informazioni di cui il responsabile dispone (art. 28, comma 3, lettera f));
- il responsabile della sicurezza dei sistemi informativi (*Chief Information Security Officer, CISO*), ove designato, nonché il RPD potrebbero proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborare con i soggetti interessati al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità del livello di rischio residuale, e definire un corpus di conoscenze specifiche del contesto operativo del titolare;

[23] *Recommendations for a privacy impact assessment framework for the European Union. Deliverable D3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

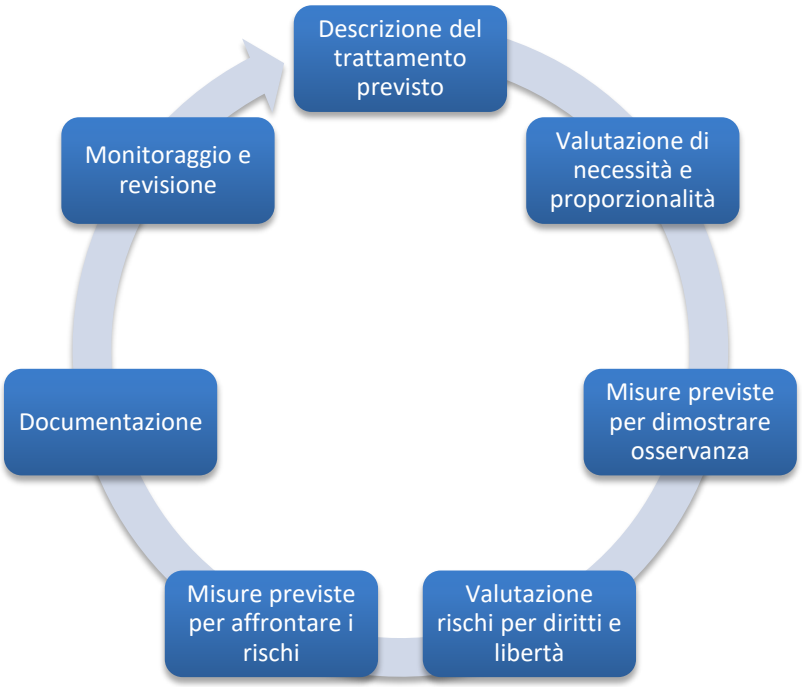
- ove designato, il responsabile della sicurezza dei sistemi informativi e/o l'ufficio o divisione IT dovrebbero fornire supporto al titolare e potrebbero proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza o operative.

c) Quale metodologia deve essere applicata per condurre una DPIA? Vi possono essere metodologie diverse, ma i criteri devono essere gli stessi

Il regolamento fissa le caratteristiche basilari di una DPIA all'art. 35, paragrafo 7, e nei considerando 84 e 90:

- "*una descrizione [sistematica] dei trattamenti previsti e delle finalità del trattamento*";
- "*una valutazione della necessità e proporzionalità dei trattamenti*";
- "*una valutazione dei rischi per i diritti e le libertà degli interessati*";
- "*le misure previste per*:
  - "*affrontare i rischi*";
  - "*dimostrare la conformità con il presente regolamento*".

La figura seguente illustra il processo iterativo generale relativo alla conduzione di una DPIA[24]:



Il rispetto di un codice di condotta (ai sensi dell'art. 40) deve essere tenuto in considerazione (ex art. 35, paragrafo 8) nel valutare l'impatto di un trattamento. È un elemento che può risultare utile a dimostrare la scelta o l'implementazione di misure adeguate, purché il codice di condotta sia idoneo con riguardo allo specifico trattamento. Si dovrebbe tenere conto anche di eventuali certificazioni, sigilli e marchi finalizzati a dimostrare che determinati trattamenti da parte di titolari e responsabili rispettano il regolamento (art. 42) nonché di norme vincolanti d'impresa (BCR).

[24] Occorre sottolineare che il processo raffigurato ha natura iterativa; in pratica, è verisimile che ogni fase debba essere ripetuta più volte prima di completare la DPIA.

Tutti i requisiti pertinenti fissati nel regolamento offrono uno schema di ampio respiro al fine della progettazione e della conduzione di una DPIA. La realizzazione di tale DPIA sarà guidata dai requisiti fissati nel regolamento integrati da linee-direttrici di natura più concreta. L'implementazione della valutazione di impatto è, dunque, un processo scalabile, nel senso che anche un titolare di piccole dimensioni può essere in grado di progettare e attuare una DPIA assolutamente idonea ai rispettivi trattamenti.

Nel considerando 90 del regolamento sono elencati alcuni elementi della DPIA che risultano sovrapponibili a elementi ben noti di schemi esistenti per la gestione del rischio (per esempio, ISO 31000[25]). In termini di gestione del rischio, una DPIA mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche attraverso i processi di seguito indicati:

- Definizione del contesto: "*tenendo conto della natura, dell'ambito, del contesto e delle finalità del trattamento e delle fonti di rischio"*;
- Valutazione dei rischi: "*valutare la particolare probabilità e gravità del rischio elevato";*
- Gestione dei rischi: "*attenuare tale rischio*" "*assicurando la protezione dei dati personali*" e "*dimostrando la conformità al presente regolamento*".

Si osservi che la DPIA, in base al regolamento, rappresenta uno strumento finalizzato alla gestione dei rischi per i diritti degli interessati e, conseguentemente, è informata a tale prospettiva così come avviene in altri campi (per esempio, la sicurezza sociale); viceversa, la gestione del rischio così come praticata in altri ambiti (per esempio, la sicurezza delle informazioni) è focalizzata sui rischi per l'organismo stesso.

Il regolamento dà ai titolari un margine di flessibilità nello stabilire la struttura e la forma della valutazione di impatto in modo da consentirne l'inclusione nelle prassi lavorative in essere. Vi sono già oggi alcuni schemi definiti nell'Ue e a livello mondiale che tengono conto degli elementi descritti al considerando 90; tuttavia, qualunque sia la forma prescelta, la DPIA deve configurare una vera valutazione dei rischi e consentire ai titolari di adottare misure per affrontare tali rischi.

Si possono utilizzare varie metodologie (si veda l'Allegato 1, che contiene esempi di metodologie per la valutazione di impatto sulla protezione dei dati e sulla privacy) per contribuire all'attuazione dei requisiti basilari fissati nel regolamento.

Per consentire la coesistenza di approcci diversificati quali quelli sopra descritti, e contemporaneamente permettere ai titolari di rispettare le disposizioni del regolamento, sono stati individuati alcuni criteri condivisi (Allegato 2). Tali criteri illustrano i requisiti basilari previsti dal regolamento, ma lasciano un margine sufficiente per il ricorso a differenti modalità di implementazione. I criteri sono utilizzabili per dimostrare che una specifica metodologia di DPIA è conforme agli standard fissati dal regolamento. **Spetta al titolare selezionare la metodologia, che comunque deve rispettare i criteri indicati nell'Allegato 2.**

Il WP29 promuove la definizione di schemi di DPIA settoriali che possano, quindi, trarre beneficio dalle specifiche conoscenze settoriali così da consentire alla DPIA di gestire le specificità di una determinata categoria di trattamenti (per esempio: categorie particolari di dati, beni societari, impatti potenziali, minacce, misure idonee). Ciò significa che la DPIA potrà affrontare le problematiche emergenti in un determinato settore economico, ovvero legate all'impiego di una specifica tecnologia o allo svolgimento di una particolare tipologia di trattamenti.

[25] Processi per la gestione del rischio: comunicazione e consultazione, definizione del contesto, valutazione del rischio, gestione del rischio, monitoraggio e revisione (si vedano termini e definizioni, e l'indice contenuto nella "anteprima" visionabile della norma 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en.)

Infine, ove necessario, "*il titolare procede a un riesame per valutare se il trattamento sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento*" (art. 35, paragrafo 11).[26]

d) È obbligatorio pubblicare la DPIA? No, ma pubblicarne una sintesi può favorire un rapporto fiduciario e la si deve inviare in forma completa all'autorità di controllo in caso di consultazione preventiva ovvero su richiesta dell'autorità stessa.

La pubblicazione della DPIA non costituisce un obbligo formale ai sensi del regolamento, ed è quindi rimessa alla discrezionalità del titolare. Tuttavia, sarebbe opportuno che i titolari valutassero di rendere pubbliche almeno parti della DPIA, quali una sintesi o le conclusioni: così facendo si promuoverebbe la fiducia nelle attività di trattamento svolte da quei titolari dando prova di un approccio responsabile e trasparente. La pubblicazione della DPIA appare particolarmente indicata se il trattamento produce effetti su una parte della popolazione, il che vale soprattutto nel caso sia un'autorità pubblica a condurre la DPIA.

Non è necessario che si pubblichi la DPIA nella sua interezza, specialmente se essa contiene informazioni dettagliate rispetto ai rischi di sicurezza che investono il titolare ovvero se può rivelare segreti commerciali o informazioni di rilevanza commerciale. In casi del genere, può essere sufficiente una sintesi delle principali risultanze del processo di valutazione di impatto, o anche una semplice dichiarazione relativa all'effettuazione di una DPIA.

Inoltre, se la DPIA indica l'esistenza di un rischio residuale elevato, il titolare dovrà consultare l'autorità di controllo prima di procedere al trattamento (art. 36, paragrafo 1), e in tal caso sussiste l'obbligo di fornire la DPIA nella sua interezza all'autorità (art. 36, paragrafo 3, lettera e)). L'autorità di controllo può fornire la propria consulenza[27] senza pregiudicare segreti commerciali o rivelare vulnerabilità in termini di sicurezza, salvi i principi applicabili in ciascun Stato membro con riguardo all'accesso ai documenti pubblici.

E. Quando occorre consultare l'autorità di controllo? Se i rischi residuali sono elevati

Si è già chiarito che:

- la DPIA è necessaria quando un trattamento "*può comportare un rischio elevato per i diritti e le libertà delle persone fisiche*" (art. 35, paragrafo 1, v. III.B.a). Per esempio, si ritiene che il trattamento su larga scala di dati relativi alla salute possa comportare un rischio elevato, e quindi si rende necessaria una DPIA;
- spetta poi al titolare valutare i rischi per i diritti e le libertà degli interessati e individuare le misure[28] previste al fine di ridurre tali rischi a un livello accettabile e dimostrare l'osservanza del regolamento (art. 35, paragrafo 7, v. III.C.c.). Si pensi, per esempio, alla conservazione di dati personali su computer portatili attraverso idonee misure di sicurezza tecniche e organizzative (cifratura dell'intero hard disk, chiavi robuste di autenticazione, idonei controlli sull'accesso, backup sicuri, ecc.) unite alle modalità in essere per quanto concerne informativa, consenso, esercizio del diritto di accesso o di opposizione, ecc. .

[26] L'art. 35, paragrafo 10, esclude espressamente solo l'applicazione dei paragrafi da 1 a 7 dello stesso.
[27] La necessità di fornire una consulenza per iscritto vige soltanto se l'autorità di controllo ritiene che il trattamento prefigurato non sia conforme al regolamento, come prevede l'art. 36, paragrafo 2.
[28] Tenendo conto anche delle indicazioni, ove esistenti, del Comitato europeo per la protezione dei dati e delle autorità di controllo, nonché dello stato dell'arte e dei costi di attuazione, come prescrive l'art. 35, paragrafo 1.

Nel caso del computer portatile sopra menzionato, se il titolare ritiene che vi sia una sufficiente riduzione dei rischi e sulla base di quanto prevede l'art. 36, paragrafo 1, alla luce dei considerando 84 e 94, si può procedere al trattamento senza consultare l'autorità di controllo. Ove i rischi in precedenza identificati non possano essere gestiti dal titolare in misura sufficiente (ossia, qualora vi sia un elevato rischio residuale) il titolare è tenuto a consultare l'autorità di controllo.

Un esempio di rischio residuale elevato non accettabile [SIC] è dato dalla possibilità che l'interessato patisca conseguenze significative, o addirittura irreversibili, e non eliminabili (per esempio, in caso di accesso illecito ai dati che comporti una minaccia per la vita degli interessati, la perdita o sospensione del rapporto lavorativo, un danno finanziario), e/o dai casi in cui appare evidente che il rischio paventato si manifesterà (per esempio, a causa dell'impossibilità di ridurre il numero di soggetti in grado di accedere ai dati in ragione delle modalità di condivisione, utilizzo o distribuzione di tali dati, ovvero per l'assenza di salvaguardie contro una vulnerabilità ampiamente nota).

Qualora il titolare non sia in grado di individuare misure sufficienti a ridurre il rischio a livelli accettabili (ossia, qualora il rischio residuale continui a permanere elevato), è necessario consultare l'autorità di controllo.[29]

Inoltre, il titolare dovrà consultare l'autorità se il diritto dello Stato membro prevede l'obbligo di consultare e/o ottenere la previa autorizzazione dell'autorità stessa in rapporto a trattamenti svolti da quel titolare per l'esecuzione di compiti nell'interesse pubblico, fra cui i trattamenti connessi alla protezione sociale e alla sanità pubblica (art. 36, paragrafo 5).

Tuttavia, occorre sottolineare che, indipendentemente dall'obbligo di consultare l'autorità di controllo in base al livello di rischio residuale, vale in ogni caso l'obbligo di conservare la documentazione della DPIA e di riesaminare la DPIA periodicamente.

IV. Conclusioni e raccomandazioni

La DPIA è uno strumento che consente ai titolari di implementare sistemi di trattamento dati conformi al regolamento, e in taluni casi di trattamento la sua conduzione è obbligatoria. Si tratta di una procedura scalabile che può assumere forme diverse, tuttavia i requisiti basilari di una DPIA efficace sono fissati nel regolamento. I titolari dovrebbero guardare alla DPIA come a un'attività utile e positiva che favorisce l'osservanza dei requisiti di legge.

L'art. 24, primo paragrafo, del regolamento fissa le responsabilità essenziali del titolare del trattamento in termini di osservanza: "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*."

[29] "*Pseudonimizzazione e cifratura di dati personali*" come pure la minimizzazione dei dati, i meccanismi di controllo, ecc. non costituiscono necessariamente misure idonee. Si tratta soltanto di esempi: l'idoneità delle misure dipende dal contesto e dai rischi specifici dei singoli trattamenti.

La DPIA è un elemento essenziale ai fini del rispetto del regolamento qualora si preveda di svolgere o si svolga un trattamento a rischio elevato. Ciò significa che i titolari dovrebbero utilizzare i criteri indicati nel presente documento per stabilire se sia o meno necessario condurre una DPIA. I titolari sono liberi, sulla base delle rispettive politiche interne, di ampliare la casistica dei trattamenti soggetti a DPIA oltre quanto richiesto dalla lettera del regolamento; in ultima analisi, così facendo si potranno accrescere la fiducia e l'affidamento degli interessati e degli altri titolari.

Se prevede di svolgere un trattamento che può presentare un rischio elevato, il titolare deve:

- selezionare una metodologia per la conduzione della DPIA (vedi esempi in Allegato 1) che soddisfi i criteri fissati nell'Allegato 2, ovvero specificare e mettere in atto una procedura sistematica di DPIA che
    - sia conforme ai criteri di cui all'Allegato 2;
    - sia parte integrante dei processi esistenti relativi alla progettazione, allo sviluppo, al cambiamento, al rischio e al riesame delle procedure operative, conformemente ai processi, ai contesti e alla cultura interni;
    - veda il coinvolgimento dei soggetti interessati e ne definisca con precisione le rispettive responsabilità (titolare, RPD/DPO, interessati o loro rappresentanti, area business, servizi tecnici, responsabili del trattamento, responsabile della sicurezza informativa, ecc.);
- fornire all'autorità di controllo competente, ove previsto, la relazione sulla DPIA svolta;
- consultare l'autorità di controllo se non è stato in grado di individuare misure sufficienti ad attenuare i rischi elevati;
- riesaminare periodicamente la DPIA e il trattamento che ne forma l'oggetto, quantomeno se intervengono variazioni del rischio posto dal trattamento in questione;
- documentare le decisioni assunte.

Allegato 1 – Esempi di schemi di DPIA attualmente esistenti nell'Ue

Il regolamento non specifica quale procedura debba essere seguita ai fini della DPIA, lasciando ai titolari la definizione di uno schema che integri le rispettive prassi e che deve, tuttavia, tenere conto delle componenti di cui all'art. 35, paragrafo 7. Può trattarsi di uno schema di DPIA sviluppato in rapporto alle specifiche esigenze del titolare, ovvero utilizzabile da un intero settore produttivo. Nel prosieguo si fornisce un elenco (non esaustivo) di schemi di DPIA già pubblicati ed elaborati da autorità per la protezione dei dati nell'Ue nonché su base settoriale:

Esempi di schemi di DPIA generali:

- DE: Standard Data Protection Model, V.1.0 – Trial version, 2016[30].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf

- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798

- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Esempi di schemi di DPIA settoriali:

- Privacy and Data Protection Impact Assessment Framework for RFID Applications.[31]
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf

- Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems[32]
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

[30] Approvato all'unanimità (con l'astensione del Land Baviera) dalla 92ma Conferenza delle autorità indipendenti per la protezione dei dati della Federazione e dei Länder a Kühlungsborn, 9-10 novembre 2016.

[31] Si veda anche:
- Raccomandazione della Commissione del 12 maggio 2009 sull'attuazione dei principi di privacy e protezione dati nelle applicazioni supportate dall'identificazione attraverso radiofrequenze.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Parere 9/2011 sulla proposta rivisitata, presentata dai produttori, di uno schema di valutazione di impatto sulla privacy e la protezione dei dati ai fini delle applicazioni RFID
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_en.pdf

[32] Si veda anche il Parere 7/2013 concernente il modello di valutazione di impatto sulla protezione dei dati per i sistemi basati sulle griglie intelligenti e i contatori intelligenti, predisposto dall'Expert Group 2 della Task Force della Commissione europea sulle griglie intelligenti.
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf

Inoltre, uno standard internazionale (ISO/IEC 29134) fornirà linee direttrici in merito alle metodologie utilizzabili per la conduzione di una DPIA.[33]

[33] ISO/IEC 29134 (progetto) *Information technology – Security techniques – Privacy impact assessment – Guidelines*, International Organization for Standardization (ISO).

Allegato 2 – Criteri riferiti a una DPIA accettabile

Il WP29 propone i seguenti criteri utilizzabili dai titolari di trattamento per stabilire se una DPIA, o una metodologia specifica di DPIA, comprenda un numero di elementi sufficienti a garantire il rispetto delle disposizioni del regolamento:

- descrizione sistematica del trattamento (art. 35, paragrafo 7, lettera a)):
  - si tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento (considerando 90);
  - sono indicati i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi;
  - si dà una descrizione funzionale del trattamento;
  - si specificano gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
  - si tiene conto dell'osservanza di codici di condotta approvati (art. 35, paragrafo 8);
- valutazione di necessità e proporzionalità del trattamento (art. 35, paragrafo 7, lettera b)):
  - si definiscono le misure previste per rispettare il regolamento (art. 35, paragrafo 7, lettera d) e considerando 90) tenendo conto di quanto segue:
    - misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
      - finalità specifiche, esplicite e legittime (art. 5(1), lettera b));
      - liceità del trattamento (art. 6);
      - dati adeguati, pertinenti e limitati a quanto necessario (art. 5(1)c));
      - periodo limitato di conservazione (art. 5(1), lettera e));
    - misure che contribuiscono ai diritti degli interessati:
      - informazioni fornite agli interessati (artt. 12, 13, 14);
      - diritto di accesso e portabilità dei dati (artt. 15 e 20);
      - diritto di rettifica e cancellazione (artt. 16, 17, 19); diritto di opposizione e limitazione del trattamento (artt. 18,19, 21);
      - rapporti con responsabili del trattamento (art. 28);
      - garanzie per i trasferimenti internazionali di dati (Capo V);
      - consultazione preventiva (art. 36);
- gestione dei rischi per i diritti e le libertà degli interessati (art. 35, paragrafo 7, lettera c):
  - si determinano l'origine, la natura, la particolarità e la gravità dei rischi (v. considerando 84) o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati:
    - si tiene conto delle fonti di rischio (considerando 90);
    - si identificano gli impatti potenziali sui diritti e le libertà degli interessati in caso di eventi fra cui accesso illegittimo, modifiche indesiderate e indisponibilità dei dati;
    - si identificano le minacce che potrebbero comportare accessi illegittimi, modifiche indesiderate e indisponibilità dei dati;
    - si stimano probabilità e gravità (considerando 90);
  - si stabiliscono le misure previste per gestire i rischi di cui sopra (art. 35, paragrafo 7, lettera d) e considerando 90);
- coinvolgimento dei soggetti interessati:
  - si chiede consulenza al RPD/DPO (art. 35, paragrafo 2);
  - si sentono gli interessati o i loro rappresentanti (art. 35, paragrafo 9), se del caso.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

17/IT

WP 253

Linee guida riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie ai fini del regolamento (UE) n. 2016/679

Adottate il 3 ottobre 2017

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL

TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 di detta direttiva,

visto il proprio regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Indice:

I. Introduzione

L'UE ha attuato una riforma globale della normativa sulla protezione dei dati in Europa. La riforma si basa su diversi pilastri (componenti fondamentali): norme coerenti, procedure semplificate, azioni coordinate, coinvolgimento degli utenti, informazioni più efficaci e rafforzamento dei poteri destinati a far rispettare le norme.

I titolari del trattamento e i responsabili del trattamento[1] hanno maggiori responsabilità nel garantire l'efficace tutela dei dati personali delle persone fisiche. Le autorità di controllo sono dotate di poteri per garantire che i principi del regolamento generale sulla protezione dei dati (di seguito "il regolamento") e i diritti delle persone interessate siano rispettati conformemente all'enunciato e alla ratio del regolamento.

L'applicazione coerente delle norme sulla protezione dei dati è fondamentale per un regime di protezione dei dati armonizzato. Le sanzioni amministrative pecuniarie rappresentano un elemento centrale del nuovo regime introdotto dal regolamento per far rispettare le norme, in quanto costituiscono un componente importante dell'insieme di strumenti di applicazione a disposizione delle autorità di controllo, congiuntamente alle altre misure previste dall'articolo 58.

Il presente documento è destinato a essere utilizzato dalle autorità di controllo per garantire una migliore applicazione e attuazione del regolamento ed espone l'interpretazione comune delle disposizioni di cui all'articolo 83 del regolamento nonché l'interazione di detto articolo con gli articoli 58 e 70 e i relativi considerando.

In particolare, ai sensi dell'articolo 70, paragrafo 1, lettera e), il comitato europeo per la protezione dei dati ha la facoltà di pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento, e l'articolo 70, paragrafo 1, lettera k), specifica che è prevista l'elaborazione di linee guida riguardanti la previsione di sanzioni amministrative pecuniarie.

Le presenti linee guida non sono esaustive e non forniscono spiegazioni in merito alle differenze esistenti tra sistemi amministrativi, civili o penali nell'imposizione di sanzioni amministrative in generale.

Al fine di adottare un approccio coerente all'imposizione di sanzioni amministrative pecuniarie, che rispecchi adeguatamente tutti i principi delle presenti linee guida, il comitato europeo per la protezione dei dati ha raggiunto un'intesa comune sui criteri di valutazione di cui all'articolo 83, paragrafo 2, del regolamento e, pertanto, il comitato e le singole autorità di controllo concordano sull'impiego delle presenti linee guida come approccio comune.

[1] NdT: La versione italiana del regolamento (UE) 2016/679 ha modificato alcuni termini della direttiva 95/46/CE (abrogata dal regolamento stesso). Per coerenza terminologica, questo testo riprende sempre la terminologia del regolamento. Pertanto "controller" è il "titolare del trattamento" ("responsabile del trattamento" nella direttiva) e "processor" è il "responsabile del trattamento" ("incaricato del trattamento" nella direttiva).

II. Principi

Una volta accertata la violazione del regolamento dopo aver valutato i fatti del caso, l'autorità di controllo competente deve individuare la o le misure correttive più appropriate per affrontare tale violazione. Le disposizioni di cui all'articolo 58, paragrafo 2, lettere da b) a j)[2], indicano gli strumenti che le autorità di controllo hanno a disposizione per far fronte a un'inadempienza da parte di un titolare del trattamento o responsabile del trattamento. Nel ricorrere a tali poteri, le autorità di controllo devono osservare i seguenti principi:

1. La violazione del regolamento dovrebbe comportare l'imposizione di "sanzioni equivalenti".

Il concetto di "equivalenza" è fondamentale nel determinare la portata degli obblighi delle autorità di controllo di garantire coerenza nel ricorso ai poteri correttivi di cui all'articolo 58, paragrafo 2, in generale e nell'applicazione delle sanzioni amministrative in particolare[3].

Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, ***il livello di protezione dovrebbe essere equivalente*** *in tutti gli Stati membri* (considerando 10). Il considerando 11 spiega che per garantire un livello equivalente di protezione dei dati personali in tutta l'Unione occorrono, tra l'altro, "*poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri*". Inoltre, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri sono considerate un modo per "*prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno*", in linea con il considerando 13 del regolamento.

Il regolamento offre una base più solida rispetto alla direttiva 95/46/CE ai fini di una maggiore coerenza, in quanto esso è direttamente applicabile negli Stati membri. Anche se le autorità di controllo agiscono in "piena indipendenza" (articolo 52) nei confronti dei governi nazionali, dei titolari del trattamento o dei responsabili del trattamento, esse devono collaborare "*al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento*" (articolo 57, paragrafo 1, lettera g)).

Il regolamento esorta a una maggiore coerenza rispetto alla direttiva 95/46/CE nell'imposizione delle sanzioni. Nei casi transfrontalieri, la coerenza deve essere garantita principalmente mediante il meccanismo di cooperazione (sportello unico) e in una certa misura tramite il meccanismo di coerenza introdotto dal nuovo regolamento.

Nei casi nazionali previsti dal regolamento, le autorità di controllo applicheranno le presenti linee guida nello spirito di collaborazione ai sensi dell'articolo 57, paragrafo 1, lettera g), e dell'articolo 63, al fine di garantire la coerenza dell'applicazione e dell'attuazione del regolamento. Sebbene continuino a essere indipendenti nello scegliere le misure correttive di cui all'articolo 58, paragrafo 2, le autorità di controllo dovrebbero evitare di scegliere misure correttive differenti in casi analoghi.

---

[2] L'articolo 58, paragrafo 2, stabilisce che è possibile rivolgere avvertimenti quando "i trattamenti previsti possono verosimilmente violare le disposizioni del regolamento". In altre parole, nel caso contemplato dalla disposizione, la violazione del regolamento non è ancora avvenuta.

[3] Anche quando i sistemi giuridici di alcuni paesi dell'UE non consentono l'irrogazione di sanzioni amministrative pecuniarie come previsto dal regolamento, l'applicazione di tali norme in detti Stati membri deve avere effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo (considerando 151). Le autorità giurisdizionali sono vincolate dal regolamento ma non sono vincolate dalle presenti linee guida del comitato europeo per la protezione dei dati.

Lo stesso principio si applica quando tali misure correttive sono imposte sotto forma di sanzioni pecuniarie.

2. Come tutte le misure correttive scelte dalle autorità di controllo, le sanzioni amministrative pecuniarie dovrebbero essere "effettive, proporzionate e dissuasive".

Come tutte le misure correttive in generale, le sanzioni amministrative pecuniarie dovrebbero rispondere adeguatamente alla natura, alla gravità e alle conseguenze della violazione, e le autorità di controllo devono valutare tutte le circostanze del caso in maniera coerente e oggettivamente giustificata. La valutazione di quanto sia effettivo, proporzionato e dissuasivo in ciascun caso dovrà anche riflettere l'obiettivo perseguito dalla misura correttiva prescelta, che è quello di ripristinare la conformità alle norme oppure di punire un comportamento illecito (o entrambi).

Le autorità di controllo dovrebbero individuare misure correttive che siano "*effettive, proporzionate e dissuasive*" (articolo 83, paragrafo 1), sia nei casi nazionali (articolo 55) che nei casi che comportano il trattamento transfrontaliero dei dati (secondo la definizione di cui all'articolo 4, punto 23).

Le presenti linee guida riconoscono che la legislazione nazionale può stabilire requisiti aggiuntivi per la procedura che le autorità di controllo devono seguire per far rispettare le norme. Essi possono consistere ad esempio in notifiche di indirizzo, moduli, termini per presentare osservazioni, appello, esecuzione, pagamento[4].

Tali requisiti non dovrebbero tuttavia ostacolare in pratica il conseguimento degli obiettivi di efficacia, proporzionalità e dissuasività.

Una determinazione più precisa dell'efficacia, della proporzionalità e della dissuasività scaturirà dalla pratica che emergerà in seno alle autorità di controllo (in materia di protezione dei dati e grazie alle esperienze acquisite in altri settori normativi) e dalla giurisprudenza relativa all'interpretazione di tali principi.

Al fine di irrogare sanzioni amministrative che siano effettive, proporzionate e dissuasive, l'autorità di controllo deve rifarsi alla definizione della nozione di impresa fornita dalla Corte di giustizia dell'Unione europea (CGUE) ai fini dell'applicazione degli articoli 101 e 102 TFUE, secondo cui il concetto di impresa **va inteso come** un'unità economica che può essere composta dall'impresa madre e da tutte le filiali coinvolte. Conformemente al diritto e alla giurisprudenza dell'UE[5], un'impresa deve essere intesa quale unità economica che intraprende attività economiche/commerciali, a prescindere dalla persona giuridica implicata (considerando 150).

[4] Ad esempio, il quadro costituzionale e la proposta legislativa in materia di protezione dei dati dell'Irlanda prevedono che, prima di valutare la portata della o delle sanzioni, si giunga a una decisione formale in merito alla violazione stessa e la si comunichi alle parti interessate. La decisione sulla violazione non può essere rivista durante la valutazione della portata della o delle sanzioni.

[5] La definizione della giurisprudenza della Corte di giustizia è la seguente: "la nozione di impresa abbraccia qualsiasi entità che esercita un'attività economica, a prescindere dallo status giuridico di detta entità e dalle sue modalità di finanziamento" (causa Höfner e Elsner, punto 21, ECLI:EU:C:1991:161). Un'impresa "dev'essere intesa nel senso che essa si riferisce ad un'unità economica, anche qualora, sotto il profilo giuridico, questa unità economica sia costituita da più persone, fisiche o giuridiche" (causa Confederación Española de Empresarios de Estaciones de Servicio, punto 40, ECLI:EU:C:2006:784).

3. L'autorità di controllo competente effettuerà una valutazione "in ogni singolo caso".

È possibile imporre sanzioni amministrative pecuniarie in risposta a una vasta serie di violazioni. L'articolo 83 del regolamento prevede un approccio armonizzato nei confronti delle violazioni di obblighi espressamente elencate nei paragrafi da 4 a 6. Il diritto di uno Stato membro può estendere l'applicazione dell'articolo 83 alle autorità e agli organismi pubblici istituiti in tale Stato membro. Inoltre, il diritto di uno Stato membro può consentire o addirittura imporre l'irrogazione di una sanzione pecuniaria in caso di violazione di disposizioni diverse da quelle citate all'articolo 83, paragrafi da 4 a 6.

Il regolamento stabilisce che ogni caso sia valutato singolarmente[6]. L'articolo 83, paragrafo 2, rappresenta il punto di partenza di tale valutazione individuale. Esso prevede che "*al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi*...". Di conseguenza, e alla luce del considerando 148[7], l'autorità di controllo ha la responsabilità di scegliere la o le misure più appropriate. Nei casi citati all'articolo 83, paragrafi da 4 a 6, tale scelta **deve** tenere conto di tutte le misure correttive, tra cui l'imposizione della sanzione amministrativa pecuniaria appropriata, sia che essa sia associata a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, oppure che sia autonoma.

Le sanzioni pecuniarie rappresentano un importante strumento che le autorità di controllo dovrebbero utilizzare nelle opportune circostanze. Le autorità di controllo sono incoraggiate a ricorrere alle misure correttive con un approccio ponderato ed equilibrato, al fine di reagire in maniera effettiva, dissuasiva e proporzionata alla violazione. Il punto non è qualificare le sanzioni pecuniarie come misure di ultima istanza, né evitare di irrogarle, bensì utilizzarle in un modo che non ne riduca l'efficacia come strumento.

---

[6] Oltre all'applicazione dei criteri di cui all'articolo 83, esistono altre disposizioni a sostegno di tale approccio quali:

- considerando 141: "*Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico*";
- considerando 129: "*È opportuno che i poteri delle autorità di controllo siano esercitati nel rispetto di garanzie procedurali adeguate previste dal diritto dell'Unione e degli Stati membri, 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 al presente regolamento, tenuto conto delle circostanze di ciascun singolo caso..."*;
- articolo 57, paragrafo 1, lettera f): *"tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 8, e svolge le indagini opportune sull'oggetto del reclamo"*.

[7] "*Per rafforzare il rispetto delle norme del presente regolamento, dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dall'autorità di controllo ai sensi del presente regolamento. In caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica, potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria. Si dovrebbe prestare tuttavia debita attenzione alla natura, alla gravità e alla durata della violazione, al carattere doloso della violazione e alle misure adottate per attenuare il danno subito, al grado di responsabilità o eventuali precedenti violazioni pertinenti, alla maniera in cui l'autorità di controllo ha preso conoscenza della violazione, al rispetto dei provvedimenti disposti nei confronti del titolare del trattamento o del responsabile del trattamento, all'adesione a un codice di condotta e eventuali altri fattori aggravanti o attenuanti. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta, inclusi l'effettiva tutela giurisdizionale e il giusto processo*".

Il comitato europeo per la protezione dei dati, negli ambiti di sua competenza ai sensi dell'articolo 65 del regolamento, adotterà una decisione vincolante sulle controversie tra le autorità, in particolare in merito alla determinazione dell'esistenza di una violazione. Se un'obiezione pertinente e motivata mette in discussione la conformità di una misura correttiva con il regolamento generale sulla protezione dei dati, la decisione del comitato europeo per la protezione dei dati esaminerà anche in che modo la sanzione amministrativa pecuniaria proposta nel progetto di decisione dell'autorità di controllo competente rispetta i principi di efficacia, proporzionalità e deterrenza. Seguiranno separatamente orientamenti del comitato europeo per la protezione dei dati sull'applicazione dell'articolo 65 del regolamento per ulteriori dettagli sul tipo di decisione che il comitato deve adottare.

---

4. Un approccio armonizzato alle sanzioni amministrative pecuniarie in materia di protezione dei dati richiede la partecipazione attiva delle autorità di controllo e lo scambio di informazioni tra le stesse.

Le presenti linee guida riconoscono che per alcune autorità di controllo nazionali i poteri sanzionatori rappresentano una novità nel settore della protezione dei dati e sollevano numerose questioni in termini di risorse, organizzazione e procedura. In particolare, le decisioni in cui le autorità di controllo esercitano i poteri sanzionatori saranno impugnabili dinanzi ai tribunali nazionali.

Le autorità di controllo collaborano tra loro e, ove necessario, con la Commissione europea tramite il meccanismo di cooperazione, come stabilito nel regolamento, al fine di sostenere scambi formali e informali di informazioni, ad esempio attraverso seminari periodici. Tale cooperazione si concentrerà sulla loro esperienza e pratica nell'applicazione dei poteri sanzionatori al fine di raggiungere una maggiore coerenza.

Questa condivisione attiva di informazioni, insieme alla giurisprudenza emergente sul ricorso a tali poteri, potrebbe condurre a una rivisitazione dei principi o dei dettagli particolari delle presenti linee guida.

III. Criteri di valutazione di cui all'articolo 83, paragrafo 2

L'articolo 83, paragrafo 2, contiene un elenco di criteri che le autorità di controllo devono usare per valutare sia l'opportunità di irrogare una sanzione amministrativa che l'importo della sanzione. Ciò non significa che occorre ripetere la valutazione usando gli stessi criteri, bensì che si deve procedere a una valutazione che tenga conto di tutte le circostanze di ogni singolo caso, conformemente all'articolo 83[8].

Le conclusioni raggiunte nella prima fase della valutazione possono essere impiegate nella seconda parte relativa all'importo della sanzione, evitando così di dover eseguire la valutazione utilizzando gli stessi criteri due volte.

La presente sezione fornisce orientamenti alle autorità di controllo su come interpretare le singole circostanze del caso alla luce dei criteri di cui all'articolo 83, paragrafo 2.

a) la natura, la gravità e la durata della violazione

Quasi tutti gli obblighi dei titolari del trattamento e dei responsabili del trattamento previsti dal regolamento sono classificati in base alla loro **natura** nelle disposizioni di cui all'articolo 83, paragrafi da 4 a 6. Il regolamento, fissando due diversi massimali per le sanzioni amministrative pecuniarie (10/20 milioni di EUR), fornisce già un'indicazione del fatto che la violazione di alcune disposizioni del regolamento può essere più grave della violazione di altre disposizioni. Tuttavia l'autorità di controllo competente, valutando le circostanze del caso alla luce dei criteri generali di cui all'articolo 83, paragrafo 2, può decidere che in quel particolare caso vi sia una necessità maggiore o minore di reagire con una misura correttiva sotto forma di sanzione pecuniaria. Quando è scelta una sanzione pecuniaria quale misura correttiva appropriata, da sola o in aggiunta ad altre misure, si applicherà il sistema a livelli del regolamento (articolo 83, paragrafi da 4 a 6) per individuare la sanzione massima imponibile a seconda della natura della violazione in questione.

Il considerando 148 introduce la nozione di "violazioni minori". Tali violazioni possono consistere nella violazione di una o più disposizioni del regolamento elencate all'articolo 83, paragrafo 4 o 5. La valutazione dei criteri di cui all'articolo 83, paragrafo 2, può tuttavia spingere l'autorità di controllo a ritenere che nelle circostanze concrete del caso la violazione, ad esempio, non crei un rischio significativo per i diritti degli interessati in questione e non incida sull'essenza dell'obbligo in questione. In tali casi, la sanzione può essere sostituita (ma non sempre) da un ammonimento.

Il considerando 148 non prevede l'obbligo per l'autorità di controllo di sostituire sempre una sanzione con un ammonimento in caso di violazione minore ("*potrebbe essere rivolto un ammonimento anziché imposta una sanzione pecuniaria*"), ma piuttosto una possibilità, dopo la valutazione concreta di tutte le circostanze del caso.

Il considerando 148 offre la stessa possibilità di sostituire una sanzione pecuniaria con un ammonimento qualora il titolare del trattamento sia una persona fisica e la sanzione pecuniaria che dovrebbe essere imposta costituisca un onere sproporzionato. L'autorità di controllo deve innanzitutto decidere, valutando le circostanze del caso, in merito alla necessità di irrogare una sanzione. Qualora sia favorevole a imporre una sanzione pecuniaria, l'autorità di controllo deve altresì valutare se la sanzione che dovrebbe essere imposta costituisca un onere sproporzionato per una persona fisica.

Il regolamento non fissa un importo specifico per violazioni specifiche, ma solo un massimale. Da ciò si può desumere la gravità relativamente minore delle violazioni di cui all'articolo 83, paragrafo 4,

[8] In alcuni paesi, in applicazione delle norme procedurali nazionali derivanti dai requisiti costituzionali, la valutazione della sanzione da infliggere può avvenire separatamente, in un momento successivo alla valutazione dell'esistenza della violazione. Ciò può limitare il contenuto e la quantità di dettagli di un progetto di decisione presentato dall'autorità di controllo capofila di tali paesi.

rispetto a quelle di cui all'articolo 83, paragrafo 5. La reazione effettiva, proporzionata e dissuasiva a una violazione dell'articolo 83, paragrafo 5, dipenderà tuttavia dalle circostanze del caso.

Occorre notare che, in determinate circostanze, le violazioni del regolamento che per natura dovrebbero rientrare nella categoria *"fino a 10 000 000 EUR o […] fino al 2 % del fatturato mondiale totale annuo"* conformemente all'articolo 83, paragrafo 4, potrebbero essere classificate in una categoria superiore (20 milioni di EUR). È il caso, ad esempio, di una violazione che sia stata precedentemente oggetto di un ordine[9] dell'autorità di controllo che il titolare o il responsabile del trattamento non ha rispettato[10] (articolo 83, paragrafo 6). Le disposizioni del diritto nazionale possono nella pratica ripercuotersi sulla valutazione[11]. La natura della violazione e "*l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito*" forniranno un'indicazione della **gravità** della violazione. Qualora nell'ambito di un singolo caso siano state commesse congiuntamente più violazioni diverse, l'autorità di controllo può applicare le sanzioni amministrative pecuniarie a un livello che risulti effettivo, proporzionato e dissuasivo entro i limiti della violazione più grave. Ad esempio, qualora siano stati violati l'articolo 8 e l'articolo 12, l'autorità di controllo può applicare le misure correttive di cui all'articolo 83, paragrafo 5, che corrispondono alla categoria della violazione più grave, ossia quella dell'articolo 12. Precisare ulteriori dettagli in questa fase esula dall'ambito delle presenti linee guida (un calcolo più dettagliato costituirebbe l'oggetto di un'eventuale fase successiva delle presenti linee guida).

I fattori presentati di seguito devono essere valutati combinatamente, ad esempio il numero di interessati va valutato in combinazione con le possibili ripercussioni nei loro confronti.

Occorre valutare **il numero** di interessati coinvolti, al fine di stabilire se si tratta di un evento isolato oppure del sintomo di una violazione sistemica oppure dell'assenza di prassi adeguate. Ciò non vuol dire che gli eventi isolati non debbano essere punibili, in quanto un evento isolato potrebbe pur sempre ripercuotersi su molti interessati. A seconda delle circostanze del caso, ciò dipenderà, ad esempio, dal numero totale di soggetti registrati nella banca dati in questione, dal numero di utenti di un servizio, dal numero di clienti, oppure dalla popolazione del paese, ove opportuno.

---

[9] Gli ordini, di cui all'articolo 58, paragrafo 2, sono i seguenti:

- ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal regolamento;
- ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del regolamento, se del caso, in una determinata maniera ed entro un determinato termine;
- ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;
- imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;
- ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;
- revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;
- ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

[10] L'applicazione dell'articolo 83, paragrafo 6, deve necessariamente tenere conto del diritto procedurale nazionale. Il diritto nazionale determina le modalità di emissione e di notifica di un ordine, il momento di entrata in vigore e l'eventuale periodo di tolleranza per conformarvisi. In particolare, occorre tenere conto dell'effetto di un appello sull'esecuzione di un ordine.

[11] Le disposizioni di legge che pongono limitazioni potrebbero far sì che un ordine precedente dell'autorità di controllo non possa più essere preso in considerazione dopo un determinato periodo dalla sua emissione. Le norme di alcune giurisdizioni prevedono che al termine del periodo di prescrizione di un ordine non possa essere imposta alcuna sanzione pecuniaria per l'inosservanza di tale ordine a norma dell'articolo 83, paragrafo 6. Spetta all'autorità di controllo di ciascuna giurisdizione determinare le ripercussioni di tali impatti.

Occorre altresì valutare **la finalità** del trattamento. Il parere del Gruppo di lavoro sulla "limitazione delle finalità"[12] ha analizzato i due elementi fondamentali di tale principio della normativa sulla protezione dei dati: indicazione specifica della finalità e utilizzo compatibile. Nel valutare la finalità del trattamento nel contesto dell'articolo 83, paragrafo 2, le autorità di controllo dovrebbero valutare la misura in cui il trattamento rispetta i due elementi fondamentali del suddetto principio[13]. In alcuni casi, l'autorità di controllo potrebbe ritenere necessario inserire un'analisi più approfondita della finalità del trattamento stesso nell'analisi dell'articolo 83, paragrafo 2.

Se gli interessati hanno subito un **danno**, occorre considerarne l'entità. Il trattamento dei dati personali può generare rischi per i diritti e le libertà personali, come esposto al considerando 75:

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

Se dalla violazione del regolamento sono sorti o potrebbero sorgere danni, l'autorità di controllo dovrebbe tenerne conto nella scelta della misura correttiva, sebbene non abbia la facoltà di corrispondere il risarcimento specifico del danno.

L'irrogazione di una sanzione pecuniaria non dipende dalla capacità dell'autorità di controllo di stabilire un nesso causale tra la violazione e il danno materiale (si veda ad esempio l'articolo 83, paragrafo 6).

La durata dell'infrazione può fornire un'indicazione, ad esempio, dei seguenti elementi:

a) condotta intenzionale da parte del titolare del trattamento, oppure

b) mancata adozione di misure preventive appropriate, oppure

c) incapacità di attuare le misure tecniche e organizzative richieste.

b) il carattere doloso o colposo della violazione

In generale, il "dolo" comprende sia la consapevolezza che l'intenzionalità in relazione alle caratteristiche di un reato, mentre per "colposo" si intende che non vi era l'intenzione di causare la

[12] WP 203, parere 03/2013 sulla limitazione delle finalità, disponibile (in inglese) al seguente indirizzo: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[13] Vedasi anche WP 217, parere 6/2014 sul concetto di legittimo interesse del titolare del trattamento ai sensi dell'articolo 7, pagina 24, sulla questione: "Cosa rende un interesse "legittimo" o "illegittimo"?"

violazione nonostante il titolare/responsabile del trattamento abbia violato l'obbligo di diligenza previsto per legge.

È generalmente riconosciuto che le violazioni dolose, da cui emerge il disprezzo per le disposizioni di legge, sono più gravi di quelle colpose e pertanto possono verosimilmente giustificare l'applicazione di una sanzione amministrativa pecuniaria. Le conclusioni circa il dolo o la colpa dipenderanno dagli elementi oggettivi di condotta rilevati dalle circostanze del caso. Inoltre, la giurisprudenza emergente e la pratica in materia di protezione dei dati nell'ambito dell'applicazione del regolamento chiariranno le circostanze fornendo linee di demarcazione più chiare per valutare il carattere doloso di una violazione.

Tra le circostanze indicanti il carattere doloso di una violazione figura il trattamento illecito autorizzato esplicitamente dall'alta dirigenza del titolare del trattamento oppure effettuato nonostante i pareri del responsabile della protezione dei dati o ignorando le politiche esistenti, ad esempio ottenendo e trattando dati relativi ai dipendenti di un concorrente con l'intento di screditare tale concorrente sul mercato.

Altri esempi sono:

- modifica di dati personali per dare un'impressione fuorviante (positiva) circa il conseguimento degli obiettivi – episodio riscontrato nel contesto degli obiettivi relativi ai tempi d'attesa ospedalieri;
- scambio di dati personali con finalità di marketing, ossia vendita di dati come "approvati" senza verificare/ignorando il parere degli interessati circa le modalità di utilizzo dei propri dati.

Altre circostanze, quali mancata lettura e non rispetto delle politiche esistenti, errore umano, mancata verifica dei dati personali nelle informazioni pubblicate, incapacità di apportare aggiornamenti tecnici in maniera puntuale, mancata adozione delle politiche (piuttosto che la semplice mancata applicazione) possono essere sintomo di negligenza.

Le imprese dovrebbero essere responsabili dell'adozione di strutture e risorse idonee alla natura e alla complessità della propria attività. Pertanto, i titolari del trattamento e i responsabili del trattamento non possono legittimare violazioni della normativa sulla protezione dei dati appellandosi a una carenza di risorse. Le prassi e la documentazione delle attività di trattamento seguono un approccio basato sul rischio ai sensi del regolamento.

Esistono zone grigie che influenzano il processo decisionale circa la necessità di imporre o meno una misura correttiva e l'autorità potrebbe dover condurre indagini più approfondite per accertare le circostanze del caso e per garantire che tutte le circostanze specifiche di ciascun caso siano state adeguatamente considerate.

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

I titolari del trattamento e i responsabili del trattamento hanno l'obbligo di attuare misure tecniche e organizzative volte a garantire un livello di sicurezza adeguato al rischio, di condurre valutazioni di impatto sulla protezione dei dati e di mitigare i rischi arrecati ai diritti e alle libertà personali dal trattamento dei dati personali. Tuttavia, quando si verifica una violazione e l'interessato ne subisce i danni, la parte responsabile dovrebbe fare quanto in suo potere per ridurre le conseguenze della violazione per il o i soggetti coinvolti. Tale comportamento responsabile (o la sua assenza) sarà preso in considerazione dall'autorità di controllo nella scelta della o delle misure correttive e nel calcolo della sanzione da imporre nel caso specifico.

Sebbene i fattori attenuanti o aggravanti siano particolarmente utili per adeguare l'importo della sanzione amministrativa pecuniaria alle particolari circostanze del caso, il loro ruolo nella scelta della misura correttiva appropriata non dovrebbe essere sottovalutato. Nei casi in cui la valutazione fondata su altri criteri lascia l'autorità di controllo nel dubbio circa l'appropriatezza di una sanzione amministrativa pecuniaria, come misura correttiva a sé stante oppure in combinazione con altre misure di cui all'articolo 58, le circostanze aggravanti o attenuanti possono aiutare a scegliere le misure appropriate spostando l'ago della bilancia in favore di quella che sembra essere la misura più effettiva, proporzionata e dissuasiva nel caso in questione.

Tale disposizione serve per valutare il grado di responsabilità del titolare del trattamento in seguito al verificarsi di una violazione. Può riguardare casi in cui è indubbio che il titolare/responsabile del trattamento non ha adottato un approccio imprudente/negligente e ha fatto quanto in suo potere per correggere le proprie azioni quando si è reso conto della violazione.

In passato, l'esperienza disciplinare delle autorità di controllo nell'ambito della direttiva 95/46/CE ha dimostrato che può essere opportuno mostrare un certo livello di flessibilità nei confronti di quei titolari/responsabili del trattamento che hanno ammesso la violazione e che si sono assunti la responsabilità di correggere o limitare l'impatto delle loro azioni. Alcuni esempi potrebbero essere i seguenti (anche se non porterebbero in tutti i casi a un approccio più flessibile):

- aver contattato altri titolari/responsabili del trattamento che potrebbero essere stati coinvolti in un'estensione del trattamento, ad esempio nel caso in cui alcuni dati sono stati erroneamente condivisi con terze parti;
- azione tempestiva adottata dal titolare/responsabile del trattamento per impedire la prosecuzione o l'espansione della violazione a un livello o a una fase che avrebbe determinato ripercussioni ben più gravi.

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

Il regolamento ha introdotto un livello ben superiore di responsabilità del titolare del trattamento rispetto alla direttiva 95/46/CE sulla protezione dei dati.

Il grado di responsabilità del titolare del trattamento o del responsabile del trattamento valutato sulla base dell'adozione di una misura correttiva appropriata può dipendere dai seguenti aspetti:

- Il titolare del trattamento ha attuato misure tecniche che seguono i principi della protezione dei dati fin dalla progettazione o per impostazione predefinita (articolo 25)?
- Il titolare del trattamento ha attuato misure organizzative che attuano i principi della protezione dei dati fin dalla progettazione e per impostazione predefinita (articolo 25) a tutti i livelli dell'organizzazione?
- Il titolare/responsabile del trattamento ha messo in atto un livello di sicurezza adeguato (articolo 32)?
- Le prassi/politiche pertinenti in materia di protezione dei dati sono conosciute e applicate al livello adeguato di gestione dell'organizzazione? (articolo 24).

L'articolo 25 e l'articolo 32 del regolamento prevedono che i titolari del trattamento tengano conto "*della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*". Anziché imporre un obbligo di risultato, tali disposizioni introducono obblighi di mezzi, il che significa che il titolare del trattamento deve condurre le valutazioni necessarie e giungere alle opportune conclusioni. La domanda cui l'autorità di controllo deve quindi rispondere è la seguente: in che misura il titolare del trattamento ha fatto quanto ci si aspettava facesse, considerando la natura, le finalità o l'entità del trattamento, alla luce degli obblighi imposti dal regolamento?

In tale valutazione, occorre tenere in debita considerazione qualsiasi procedura e metodo basati sulle migliori prassi, ove esistano e siano applicate. È importante tenere conto delle norme industriali e dei codici di condotta nel rispettivo campo o professione. I codici di condotta potrebbero fornire un'indicazione delle pratiche comuni nel settore e un'indicazione del livello di conoscenza dei diversi mezzi esistenti per affrontare le tipiche problematiche di sicurezza associate al trattamento.

Anche se le migliori prassi dovrebbero rappresentare l'ideale da perseguire in generale, nel valutare il grado di responsabilità occorre considerare le circostanze specifiche del singolo caso.

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

Tale criterio serve per valutare i precedenti dell'entità che commette la violazione. Le autorità di controllo dovrebbero considerare che la valutazione può avere una portata piuttosto vasta poiché ogni tipo di violazione del regolamento, seppur di natura diversa da quella esaminata dall'autorità di controllo, potrebbe essere pertinente ai fini della valutazione, in quanto potrebbe fornire indicazioni su un livello generale di conoscenza insufficiente o di indifferenza nei confronti delle norme sulla protezione dei dati.

L'autorità di controllo dovrebbe valutare quanto segue:

- Il titolare/responsabile del trattamento ha già commesso la stessa violazione in precedenza?
- Il titolare/responsabile del trattamento ha commesso una violazione del regolamento secondo le stesse modalità? (ad esempio a causa di una conoscenza insufficiente delle prassi esistenti nell'organizzazione, oppure in seguito a una valutazione del rischio inadeguata, non rispondendo alle richieste dell'interessato in maniera tempestiva o per un ritardo ingiustificato nel rispondere alle richieste, ecc.).

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

L'articolo 83, paragrafo 2, prevede che il grado di cooperazione debba essere tenuto in "debito conto" al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa. Il regolamento non indica con precisione come tenere conto degli sforzi dei titolari del trattamento o dei responsabili del trattamento nel rimediare a una violazione già accertata dall'autorità di controllo. Inoltre, è chiaro che i criteri saranno solitamente applicati nel calcolo dell'importo della sanzione pecuniaria da imporre.

Tuttavia, nello scegliere la misura correttiva proporzionata al singolo caso si dovrebbe tener conto anche dell'eventuale l'intervento con cui il titolare del trattamento abbia limitato o addirittura azzerato le ripercussioni negative sui diritti delle persone che si sarebbero altrimenti verificate.

Un caso in cui la collaborazione con l'autorità di controllo potrebbe essere presa in debita considerazione è il seguente:

- L'entità ha risposto in modo particolare alle richieste dell'autorità di controllo durante la fase di indagine nel caso specifico limitando in tal modo in maniera significativa le ripercussioni sulle persone?

Detto ciò, non sarebbe opportuno tenere ulteriormente conto della collaborazione già prevista per legge: ad esempio, l'entità è in ogni caso tenuta a consentire all'autorità di controllo di accedere ai locali per controlli/ispezioni.

g) le categorie di dati personali interessate dalla violazione;

Alcuni esempi di domande chiave a cui l'autorità di controllo potrebbe ritenere necessario rispondere, ove opportuno, sono i seguenti:

- La violazione riguarda il trattamento di categorie particolari di dati di cui agli articoli 9 e 10 del regolamento?
- I dati sono direttamente/indirettamente identificabili?
- Il trattamento riguarda dati la cui diffusione causerebbe immediati danni/disagi alla persona (che non rientrano nelle categorie di cui agli articoli 9 e 10)?

- I dati sono direttamente disponibili senza protezioni tecniche oppure sono criptati[14]?

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

L'autorità di controllo potrebbe venire a conoscenza della violazione in seguito a indagini, reclami, articoli di giornale, suggerimenti anonimi oppure notifiche da parte del titolare del trattamento. Il titolare del trattamento ha l'obbligo a norma del regolamento di notificare all'autorità di controllo eventuali violazioni dei dati personali. Qualora il titolare del trattamento si limiti ad adempiere a tale obbligo, la conformità ad esso non può essere interpretata come fattore attenuante/mitigante. Analogamente, qualora il titolare/responsabile del trattamento abbia agito incautamente senza notificare la violazione, o perlomeno senza notificarne tutti i dettagli, in quanto non in grado di valutarne adeguatamente la portata, l'autorità di controllo potrebbe ritenere necessaria l'imposizione di una sanzione più grave, il che significa che risulterà improbabile la classificazione quale violazione minore.

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

Il titolare del trattamento o il responsabile del trattamento potrebbe già essere nel mirino dell'autorità di controllo per la verifica della conformità in seguito a una precedente violazione. In tal caso gli eventuali precedenti contatti con il responsabile della protezione dei dati saranno stati verosimilmente numerosi e l'autorità di controllo li terrà in considerazione.

A differenza dei criteri di cui alla lettera e), questo criterio di valutazione serve solo per ricordare alle autorità di controllo di fare riferimento alle misure precedentemente emesse nei confronti del medesimo titolare o responsabile del trattamento "*relativamente allo stesso oggetto*".

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;

Le autorità di controllo hanno il dovere di *"sorveglia[re] e assicura[re] l'applicazione del […] regolamento"* (articolo 57, paragrafo 1, lettera a)). L'adesione ai codici di condotta approvati può essere utilizzata dal titolare del trattamento o dal responsabile del trattamento per dimostrare la conformità, ai sensi dell'articolo 24, paragrafo 3, dell'articolo 28, paragrafo 5, o dell'articolo 32, paragrafo 3.

In caso di violazione di una delle disposizioni del regolamento, l'adesione a un codice di condotta approvato può fornire indicazioni circa la portata della necessità di intervenire con una sanzione amministrativa pecuniaria effettiva, proporzionata, dissuasiva o altra misura correttiva da parte dell'autorità di controllo. I codici di condotta approvati conterranno, ai sensi dell'articolo 40, paragrafo 4, "*i meccanismi che consentono all'organismo (di controllo) di effettuare il controllo obbligatorio del rispetto delle norme del codice*".

Qualora il titolare del trattamento o il responsabile del trattamento abbia aderito a un codice di condotta approvato, l'autorità di controllo potrebbe ritenere sufficiente che la comunità incaricata di gestire il codice intervenga adeguatamente in prima persona nei confronti del proprio membro, ad esempio tramite i regimi di monitoraggio e applicazione del codice di condotta stesso. Pertanto, l'autorità di controllo potrebbe ritenere che tali misure siano sufficientemente effettive, proporzionate

[14] Il fatto che la violazione riguardi solo dati indirettamente identificabili oppure pseudonimi/dati criptati non dovrebbe essere sempre considerato un fattore attenuante supplementare. Per tali violazioni una valutazione complessiva degli altri criteri potrebbe offrire una moderata o netta indicazione circa l'opportunità di imporre una sanzione amministrativa.

e dissuasive in quel particolare caso senza che l'autorità di controllo stessa debba imporre misure aggiuntive. Alcune forme di sanzionamento dei comportamenti non conformi possono avvenire tramite il regime di monitoraggio, ai sensi dell'articolo 41, paragrafo 2, lettera c), e dell'articolo 42, paragrafo 4), compresa la sospensione o l'esclusione del titolare del trattamento o del responsabile del trattamento dalla comunità incaricata di gestire il codice. Ciononostante, i poteri dell'organismo di controllo si espletano "*fatti salvi i compiti e i poteri dell'autorità di controllo competente*", il che significa che l'autorità di controllo non ha l'obbligo di tenere conto delle sanzioni precedentemente imposte relative al regime di autoregolamentazione.

La non conformità con le misure di autoregolamentazione potrebbe altresì rivelare la colpa o il dolo del titolare/responsabile del trattamento.

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

La disposizione stessa fornisce esempi di quali altri elementi potrebbero essere presi in considerazione nel decidere l'appropriatezza di una sanzione amministrativa pecuniaria per una violazione delle disposizioni di cui all'articolo 83, paragrafi da 4 a 6.

Le informazioni relative ai profitti derivanti da una violazione potrebbero risultare particolarmente importanti per le autorità di controllo in quanto il guadagno economico derivante dalla violazione non può essere compensato tramite misure che non abbiano una componente pecuniaria. Pertanto, il fatto che il titolare del trattamento abbia tratto profitto dalla violazione del regolamento può costituire una chiara indicazione della necessità di imporre una sanzione pecuniaria.

IV. Conclusioni

Le riflessioni sugli aspetti esposti nella sezione precedente aiuteranno le autorità di controllo a individuare, tra i fatti pertinenti del caso, i criteri più utili per valutare se sia necessario imporre una sanzione amministrativa pecuniaria appropriata in aggiunta o in sostituzione delle misure di cui all'articolo 58. Tenendo conto del contesto fornito dalla valutazione, l'autorità di controllo individuerà la misura correttiva più effettiva, proporzionata e dissuasiva per far fronte alla violazione.

L'articolo 58 fornisce alcuni orientamenti sulle misure tra cui un'autorità di controllo può scegliere, in quanto le misure correttive di per sé hanno natura diversa e sono destinate principalmente a finalità diverse. Alcune misure di cui all'articolo 58 possono anche essere cumulate, dando così luogo a un intervento che prevede più di una misura correttiva.

Non è sempre necessario integrare la misura con un'altra misura correttiva. Ad esempio, tenuto debito conto di cosa è proporzionato al caso specifico, l'efficacia e la dissuasività dell'intervento dell'autorità di controllo potrebbero essere garantite attraverso la sola sanzione pecuniaria.

In sintesi, le autorità devono ripristinare la conformità tramite tutte le misure correttive che hanno a disposizione. Le autorità di controllo dovranno altresì scegliere il canale più appropriato per portare avanti l'intervento (potendo ricorrere, ad esempio, a sanzioni penali - ove disponibili a livello nazionale).

La pratica di applicare sanzioni amministrative pecuniarie coerentemente all'interno dell'Unione europea è una pratica in via di evoluzione. Le autorità di controllo dovrebbero collaborare costantemente per aumentare tale coerenza, ad esempio tramite regolari scambi durante seminari sul trattamento dei casi o altri eventi che consentano di confrontare i casi a livello sub-nazionale, nazionale e transfrontaliero. Al fine di sostenere questa attività continuativa si raccomanda la creazione di un sottogruppo permanente annesso a una parte pertinente del comitato europeo per la protezione dei dati.