Datore di lavoro **SCARPIELLO Racing**
Lì, 21/10/2026 – [Contr. 2714bis]
Via Zara, 57
60019 – Senigallia (AN)

Sig./sig.ra
Lorenzo Carbone
Via Giacomo Leopardi, 37
60033 - Chiaravalle (AN)

CONTRATTO DI ASSUNZIONE A TEMPO DETERMINATO PART-TIME

A seguito di accordi intercorsi sono a confermare la sua prosecuzione presso questo Team con decorrenza dal 01/11/2026. L'assunzione avviene alle seguenti condizioni:

QUALIFICA
Operatore di Revisione sito web di www.marcoscarpiello.it (*x2 volte al mese*)

DURATA
Il rapporto di lavoro è stipulato a **tempo determinato**, per la durata complessiva di **3 mesi**, con incarico di revisione del sito web. Il rapporto avrà pertanto termine in data **01/02/2027** e, alla scadenza prevista, si intenderà **automaticamente concluso**, senza necessità di preavviso o di ulteriore comunicazione da parte delle parti.

ORARIO
Giorni e orario di lavoro saranno scelti direttamente dal Dipendente, in quanto si tratta di una gestione lavorativa singola e autonoma.

LUOGO
L'attività lavorativa verrà svolta presso l'abitazione del dipendente.

FERIE/RIPOSI
Le ferie non sono previste.

CONTRIBUTO MENSILE
La paga mensile netta per l'incarico assegnato è pari a **13,69**€ che verrà automaticamente accreditato tramite l'IBAN «IT67T0538737320000004566526» di Lorenzo Carbone ogni 23 del mese ad accezione del sabato e domenica che lo stesso potrebbe essere anticipato o posticipato in base agli accordi contrattuali con la banca nazionale di Revolut (sede Italia – Milano MI).

COMPETENZE/STRAORDINARI
Gli incarichi extra e gli straordinari supplementari, che ricorreranno nel periodo contrattuale, verranno accreditati sul conto deposito pocket del sito web, associato al seguente link personale (https://www.marcoscarpiello.it/dipendenti/lorenzocarbone05122006-333309574474/). Al termine del rapporto lavorativo, sia in caso di cessione immediata che per scadenza naturale del contratto, l'importo complessivo maturato verrà manualmente trasferito sul conto corrente personale dell'interessato, utilizzando l'IBAN italiano indicato alla voce "*contributo mensile*", previa richiesta scritta di autentificazione di deposito e/o prelievo tramite portale web del sito ufficiale.

TABELLA COMPETENZE EXTRA

Si riporta, in allegato, la tabella extra delle Competenze autorizzati dal Team;

- servizio notturno +5,00€ al gg (*dalle ore 22.30 alle ore 06.30*)
- servizio news diurno +1,99 a news
- servizio di pubblicazione link news diurno +0,35€ a news
- revisione sito web +7,84€ al gg
- gestione contabilità del Team +89,42€ al gg
- gestione reparto Team in Autodromo nazionale +644,57€ al gg
- gestione reparto Team in Autodromo internazionale +1.894,93€ al gg

CLAUSOLE CONTRATTUALE (imposto dal Titolare)

1. Il Dipendente ha facoltà di recedere dal presente rapporto lavorativo in qualsiasi momento, con un preavviso minimo di 5 (cinque) giorni, mediante comunicazione scritta da inviarsi via email all'Uff. Amministrativo (amministrativo@scarpiellostaff.net); tale facoltà è esercitabile esclusivamente nel caso in cui il condizione che egli fornisce copia del contratto di assunzione o altra documentazione ufficiale che attesti l'avvenuta proposta lavorativa. Decorso il termine di preavviso, il rapporto si intenderà "*sospeso per causa di forza maggiore*" con la sospensione della retribuzione mensile. Altresì, è obbligatorio comunicare tempestivamente al Team l'eventuale decadenza della presente offerta lavorativa, al fine di consentire lo sblocco dello stato di servizio. In assenza di tale comunicazione, sarà applicata una sanzione amministrativa pari a 321,44€ come da Art. 2.014, 2.015 e 1.375 del Codice Civile.
2. Il Dipendente ha facoltà di recedere dal presente contratto entro e non oltre i primi 10 (dieci) giorni dalla data di decorrenza dello stesso, ovvero entro il 10 gennaio c.a. Tale periodo è da intendersi quale periodo di prova lavorativa, durante il quale ciascuna delle parti potrà recedere dal contratto senza obbligo di preavviso né di corresponsione di indennità.

TUTELA LEGGE – PRIVACY

La ***nuova normativa sulla protezione dei dati personali*** risulta dalle disposizioni del 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 (c.d. GDPR), nonché dalle disposizioni del Codice della privacy così come riformato, nella XVIII legislatura, dal d.lgs. n. 101/2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR. Ulteriori modifiche al Codice sono state successivamente apportate attraverso il decreto-legge n. 139 del 2021 convertito, con modificazioni, dalla legge n. 205 del 2021. Il decreto legislativo n. 101 del 2018 è andato ad aggiungersi al decreto legislativo n. 51 del 2018, con il quale l'ordinamento italiano ha attuato la direttiva 2016/680, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, completando il recepimento del c.d. pacchetto protezione dati dell'Unione europea.

(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 '3' 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.

Il Team Amm.vo

Marco Scarpiello



Per accettazione il Dipendente

FIRMATO il 22/10/2026, ore 15:03