Accorgimenti

PER LA SICUREZZA ED IL CORRETTO TRATTAMENTO DEI **DATI PERSONALI**

TRATTAMENTO DEI DATI NELLE PUBBLICHE AMMINISTRAZIONI

- **il trattamento dei dati sensibili e giudiziari** se autorizzato da espressa disposizione di legge nella quale si specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Nei casi in cui una disposizione di legge specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, le amministrazioni sono tenute ad adottare un apposito regolamento con il quale identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dal Codice.

In ogni caso, il trattamento dei dati sensibili e giudiziari da parte delle Pubbliche Amministrazioni è retto dal principio di indispensabilità, ossia possono essere trattati soltanto i dati sensibili e giudiziari indispensabili allo svolgimento di funzioni istituzionali che non potrebbero essere adempiute altrimenti (mediante il ricorso a dati anonimi o personali di diversa natura).

la comunicazione di dati personali

- a privati o enti pubblici economici soltanto se prevista da una norma di legge o di regolamento
- ad altri soggetti pubblici se prevista da una norma di legge o di regolamento ovvero, in mancanza, se necessaria per il perseguimento dei fini istituzionali previa apposita comunicazione al Garante per la protezione dei dati personali.

Non è in ogni caso consentita la diffusione dei dati idonei a rilevare lo stato di salute.

Misure di sicurezza da adottare vengono distinte in:

- **misure idonee e preventive** volte a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
- **misure minime**, indicate negli articoli 34 e 35 e analiticamente specificate nel Disciplinare Tecnico e diversificate a seconda che il trattamento sia effettuato o meno con strumenti elettronici.

Con l'approvazione del Codice i titolari di trattamento di dati sono tenuti ad adottare, quanto meno, le cd "misure minime di sicurezza", ossia gli accorgimenti, individuati negli artt. 34-35 e nel Disciplinare Tecnico del Codice, tesi ad assicurare un livello minimo di protezione dei dati personali.

La mancata osservanza di quanto stabilito in materia di misure minime di sicurezza è sanzionata penalmente

L'adozione delle misure minime di sicurezza non esonera tuttavia da responsabilità civile qualora l'eventuale danneggiato dimostri che, in base all'evoluzione tecnologica raggiunta, era possibile e raccomandabile l'utlizzo di misure di sicurezza ulteriori (le cd misure "idonee").

PRECAUZIONI GENERALI DA ADOTTARE NEL TRATTAMENTO DI DATI PERSONALI CONTENUTI IN ARCHIVI E DOCUMENTI CARTACEI

Trattamento di documenti contenenti dati personali

1. Gli incaricati sono tenuti a custodire e controllare gli atti e i documenti contenenti dati personali, in modo da evitare che persone prive di autorizzazione possano accedere ai dati.
2. I documenti contenenti dati personali devono essere conservati in archivi ad accesso controllato e con possibilità di chiusura, solo il personale autorizzato, secondo le modalità specificate nella lettera d'incarico, avrà la possibilità di averne accesso.
3. Tutta la documentazione e le pratiche trattate o da trattare devono essere riposte in armadi chiusi a chiave nel periodo di intervallo meridiano o al termine della giornata lavorativa.
4. La protezione dei dati deve essere compiuta dalla loro acquisizione fino all'eventuale distruzione degli stessi e per tutto il ciclo di loro trattamento e conservazione.
5. Gli incaricati **devono** evitare che terzi (non incaricati), possano accedere ai luoghi in cui sono custoditi i dati, quindi devono adottare misure idonee per evitare la visibilità dei dati a terzi.
6. Non è possibile effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile della **sicurezza dei dati personali** di dati oggetto del trattamento.
7. Non è possibile effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personali,** di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
8. Non è possibile sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personali,** stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento
9. Sarà cura di ogni incaricato adottare ogni misura possibile al fine di garantire quanto sopra.

LE MISURE MINIME DI SICUREZZA

Trattamenti effettuati con strumenti elettronici TRATTAMENTO DATI COMUNI

Sono obbligatorie le seguenti misure:

A) AUTENTICAZIONE INFORMATICA.

Il sistema informatico deve essere dotato di mezzi (le cd. credenziali di autenticazione) deputati alla verifica ed alla convalidazione dell'identità del soggetto che vi accede Le credenziali di autenticazione consistono in un codice per l'identificazione (user id) dell'incaricato associato a una parola chiave riservata (password), conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

B) ADOZIONE DI PROCEDURE DI GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE;

Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri

oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali

C) UTILIZZAZIONE DI UN SISTEMA DI AUTORIZZAZIONE;

E' il sistema che, dopo l'autenticazione, permette agli incaricati di trattare effettivamente i dati.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione

D) AGGIORNAMENTO PERIODICO DELL'INDIVIDUAZIONE DELL'AMBITO DEL TRATTAMENTO CONSENTITO AI SINGOLI INCARICATI E ADDETTI ALLA GESTIONE O ALLA MANUTENZIONE DEGLI STRUMENTI ELETTRONICI;

E' effettuata tramite l'aggiornamento, almeno annuale, dell'anagrafe del trattamento dei dati personali.

E) PROTEZIONE DEGLI STRUMENTI ELETTRONICI E DEI DATI RISPETTO A TRATTAMENTI ILLECITI DI DATI, AD ACCESSI NON CONSENTITI E A DETERMINATI PROGRAMMI INFORMATICI;

Utilizzo di antivirus aggiornati almeno semestralmente (giornalmente) e adozione di misure atte alla protezione dagli accessi dalla rete (firewall etc)

F) ADOZIONE DI PROCEDURE PER LA CUSTODIA DI COPIE DI SICUREZZA, IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI E DEI SISTEMI;

Utilizzo di back up e strategie di disaster recovery

TRATTAMENTO DATI SENSIBILI O GIUDIZIARI

Ulteriori misure:

H) ADOZIONE DI IDONEE MISURE PER GARANTIRE IL RIPRISTINO DELL'ACCESSO AI DATI IN CASO DI DANNEGGIAMENTO DEGLI STESSI O DEGLI STRUMENTI ELETTRONICI, IN TEMPI CERTI COMPATIBILI CON I DIRITTI DEGLI INTERESSATI E NON SUPERIORI A SETTE GIORNI

i) Devono essere concordate con il titolare del trattamento o gli amministratori di sistema le misure organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati

sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI (DATI SU SUPPORTO CARTACEO)

Trattamento dati comuni
Sono **obbligatorie** le seguenti misure:

a) L'aggiornamento periodico dei dati il cui trattamento è consentito agli incaricati (tramite l'aggiornamento dell'anagrafe dei trattamenti)
b) Istruzioni circa un'idonea custodia degli atti e dei documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

E' compito di ciascun responsabile fornire istruzioni agli incaricati del trattamento affinché ai documenti contenenti dati personali non accedano persone prive di autorizzazione, dando idonea divulgazione presso gli stessi del presente Manuale per la sicurezza, per quanto riguarda le prescrizioni di carattere generale, nonché impartendo le istruzioni del caso relativamente alla specificità del trattamento dei dati personali effettuato nell'Unità Organizzativa medesima.

TRATTAMENTO DATI SENSIBILI O GIUDIZIARI

Ulteriori misure:
L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, possibilmente utilizzando armadi o contenitori chiusi a chiave Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

1. Tali dati dovranno essere custoditi in appositi armadi muniti di serratura, solo in personale specificatamente autorizzato preposto al trattamento di questi dati, secondo le modalità specificate nella lettera d'incarico, avrà la possibilità di averne accesso. Tali armadi dovranno sempre rimanere chiusi, e solo il personale o l'incaricato potrà avere la chiave per poter effettuare l'apertura degli stessi. È assolutamente ***VIETATO*** lasciare incustodito e aperti, anche solo temporaneamente tali archivi;

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

1. UTILIZZATE LE CHIAVI!
Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio quando l'ultima unità di personale lascia il locale e, comunque, alla fine della giornata e chiudete i documenti a chiave negli armadi ogni volta che potete.

2. NON COMUNICATE DATI PERSONALI A SOGGETTI NON LEGITTIMATI
L'utilizzo dei dati personali deve avvenire in base al cd "principio di necessità", è cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative.
I dati non devono essere comunicati all'esterno dell'Università e comunque a soggetti terzi, se non previa autorizzazione del Responsabile nelle ipotesi consentite dalla normativa vigente.

3. FATE ATTENZIONE A COME DISTRUGGETE I DOCUMENTI

Qualora sia necessario distruggere i documenti contenenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.

I documenti originali non possono in alcun caso essere distrutti senza la previa autorizzazione della Soprintendenza Archivistica.

4. RADDOPPIATE LE ATTENZIONI SE I DOCUMENTI CONTENGONO DATI SENSIBILI O GIUDIZIARI

I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi molto attentamente in modo che non vi accedano persone prive di autorizzazione.

Ad esempio, la consultazione di documenti o certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattia, ecc., deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati.

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando possibilmente armadi o contenitori chiusi a chiave Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori dall'orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

Riponete i documenti contenenti dati sensibili o giudiziari negli appositi contenitori o arma al termine delle operazioni affidate e comunque a fine giornata. In ogni caso di allontanamento dal proprio posto di lavoro, documenti devono essere riposti negli armadi o nei cassetti, possibilmente chiusi a chiave.

Particolare attenzione dovrà essere rivolta ai documenti contenenti dati sensibili o giudiziari con particolare attenzione alla documentazione sanitaria contenuta nelle schede. A tal fine è necessario che tali documenti, quando sono al di fuori dei loro archivi durante l'utilizzo quotidiano, siano tenuti sotto il controllo e la custodia degli incaricati, mentre al termine dell'impiego quotidiano, devono essere riposti in armadi, cassetti, archivi o contenitori chiusi a chiave. Non devono assolutamente essere lasciati sulle scrivanie o postazioni di lavoro a disposizione di chiunque entri nell'ufficio/locale. In caso di ingresso nel locale/ufficio di persone estranee è buona norma fare in modo di impedire l'accesso a tali documenti, ad esempio conservandoli temporaneamente in un cassetto o in una teca, sempre comunque sotto il controllo dell'incaricato. Si ricorda inoltre, di provvedere alla separazione dei dati sensibili (idonei a rilevare lo stato di salute e vita sessuale, da altri dati non necessari alle finalità del trattamento). Ad esempio, i certificati medici possono essere mantenuti nel faldone contenente la documentazione dell'interessato ma separandoli dagli altri documenti, ad esempio, utilizzando una busta chiusa.

TRATTAMENTI CON STRUMENTI ELETTRONICI

1. CONSERVATE I DATI IN UN LUOGO SICURO

Si applicano gli stessi criteri che per i documenti cartacei. Riponeteli negli armadi o nei cassetti non appena avete finito di usarli.

2. UTILIZZATE LE PASSWORD

Vi sono svariate categorie di password, ognuna con il proprio ruolo preciso:

a) La password di accesso al computer impedisce l'utilizzo improprio della vostra postazione, quando per un motivo o per l'altro non vi trovate in ufficio.
b) La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio.
c) La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.

d) La password del salvaschermo, infine, impedisce che una vostra assenza momentanea permetta a una persona non autorizzata di visualizzare il vostro lavoro.
e) Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta almeno quella di tipo *a*, che può dover essere resa nota, almeno temporaneamente, esclusivamente ai tecnici accreditati incaricati dell'assistenza. Scegliete le password secondo le indicazioni della sezione successiva.

3. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI
Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe.

4. PRESTATE ATTENZIONE ALL'UTILIZZO DEI PC PORTATILI
I PC portatili sono un facile bersaglio per i furti. Se avete necessità di gestire dati riservati su un portatile, fatevi installare un buon programma di cifratura del disco rigido, e utilizzate una procedura di backup periodico.

5. NON FATEVI SBIRCIARE QUANDO STATE DIGITANDO LE PASSWORD
Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattilo-scrittura.

6. CUSTODITE LE PASSWORD IN UN LUOGO SICURO
Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati.

7. NON UTILIZZATE APPARECCHI NON AUTORIZZATI
L'utilizzo di modem su postazioni di lavoro collegati alla rete di edificio offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata.

8. NON INSTALLATE PROGRAMMI NON AUTORIZZATI
Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con responsabile/amministratore di sistema.

9. APPLICATE CON CURA LE LINEE GUIDA PER LA PREVENZIONE DA INFEZIONI DI VIRUS
La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.
LINEE GUIDA PER LA PREVENZIONE DEI VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

COME SI TRASMETTE UN VIRUS:
1. Attraverso programmi provenienti da fonti non ufficiali;
2. Attraverso le macro dei programmi di automazione d'ufficio.

COME *NON* SI TRASMETTE UN VIRUS:
1. Attraverso file di dati non in grado di contenere macro (file di testo, html, pdf, ecc.);
2. Attraverso mail non contenenti allegati.

Guida ai primi accorgimenti per il Nuovo Regolamento Europeo 679/2016.

Principali accorgimenti utili all'immediata applicazione del nuovo Regolamento Ue.

Fonti: Rete – Garante Privacy – Agi – legaldesk.

Il GDPR si basa, infatti, sul principio di "responsabilizzazione" (in inglese accountability) di chiunque effettui operazioni di trattamento nell'ambito della propria attività (il cosiddetto "titolare del trattamento"). Significa, quindi, che ciascuno dovrà fare le valutazioni e le scelte adatte alla propria specifica realtà. E le sanzioni per l'inosservanza delle norme possono arrivare fino a 20 milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale. Particolare attenzione è dedicata alla tutela dei minori che - per accedere ai servizi della società dell'informazione (come i social network) - devono avere almeno 16 anni per poter prestare autonomamente il consenso al trattamento.
Il Regolamento è destinato ad abrogare la Direttiva 95/46 che ha portato l'Italia all'adozione dell'attuale Codice Privacy (il Decreto Legislativo n. 196/2003)
Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica.
Particolarmente:

1) Gli obblighi nei confronti degli utenti

Gli utenti devono essere informati in modo semplice e chiaro sulle finalità, modalità e ambito del trattamento. Le informative richieste agli utenti (dal form per una newsletter ai moduli per richiedere una fidelity card) devono quindi essere aggiornate, prevedendo alcune informazioni nuove (come la base giuridica del trattamento e il tempo di conservazione dei dati) e semplificando il testo in modo da renderle realmente comprensibili.

2)Le misure tecniche da adoperare

Ogni titolare del trattamento è tenuto ad adottare misure tecniche e organizzative sin dal momento della progettazione oltre che nell'esecuzione del trattamento, che tutelino i principi di protezione dei dati. Non esiste un elenco di misure di sicurezza "minime" uguali per tutti. Spetta a ciascuno decidere e assumersi le responsabilità di quali siano le contromisure adeguate alla propria realtà (crittografia, controllo degli accessi, sorveglianza degli archivi, ecc.).

3)Viene introdotto il diritto degli interessati di venire a conoscenza delle violazioni dei propri dati personali ("data breach"). Questo significa che - nel caso di incidenti di sicurezza relativi ai sistemi utilizzati per il trattamento (come lo smarrimento di una chiavetta Usb, il furto di un fascicolo oppure un attacco informatico) - il titolare del trattamento dovrà organizzarsi per procedere alla notificazione al Garante Privacy senza ritardo (e comunque, entro le 72 ore).

4)Le sanzioni

Il sistema sanzionatorio previsto del GDPR è molto più severo rispetto a quello del Codice Privacy. Le sanzioni amministrative - che saranno inflitte dal Garante Privacy - possono arrivare fino a 20 milioni di euro o, se superiore, fino al 4% del fatturato mondiale totale. Le sanzioni non sono però l'unico spauracchio. In attesa di vedere se e quali saranno gli illeciti penalmente rilevanti previsti dal Decreto che il governo italiano si appresta ad adottare, è importante tenere a mente che chiunque subisca un danno da una violazione del GDPR ha il diritto di ottenerne il risarcimento dal titolare, a meno che quest'ultimo non dimostri che il danno non gli è alcun modo imputabile. E forse questa è alla fine la prova più difficile da dare se non sono state affrontate tutte le novità del GDPR.

QUINDI

IL CONSENSO

- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso deve essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22).

Si segnalano, al riguardo, le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy.it/regolamentoue/profilazione.

- Non deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a

configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

Contenutidell'informativa

- I contenuti dell'informativa sono elencati in modo tassativo negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare deve sempre specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ul- timo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).
- Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.
- Se il trattamento comporta processi decisionali automatizzati (anche la profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi dell'informativa

- Nel caso di dati personali non raccolti direttamente presso l'interessa- to (art. 14 del regolamento), l'informativa deve essere fornita entro un

termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa

- Il regolamento specifi molto più in dettaglio rispetto al Codice le ca- ratteristiche dell'informativa, che deve avere forma concisa, trasparente, intelligibileperl'interessatoefacilmente accessibile;occorreutilizzareun linguaggio chiaro e semplice, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).
- L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di icone per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno defi e prossimamente dalla Commissione europea.
- Sono inoltre parzialmente diversi i requisiti che il regolamento fi sa per l'esonero dall'informativa (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che spetta al titolare.

Registro dei trattamenti

• Tutti i titolari e i responsabili di trattamento devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno strumento fondamentale non soltanto ai fni dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Notifca delle violazioni di dati personali

• A partire dal 25 maggio 2018, tutti i titolari – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notifcare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustifcato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, la notifca all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustifcato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifca all'Autorità e della

comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento. Si segnalano, al riguardo, le linee-guida in materia di notifca delle violazioni di dati personali del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/regolamentoue/databreach.

Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

• Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese, estendibile fno a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

• Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

• La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Titolare, responsabile, incaricato del trattamento

Il regolamento

- disciplina la contitolarità del trattamento (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

- fissa più dettagliatamente (rispetto al Codice) le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28 al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

- consente la nomina di sub-responsabili del trattamento da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3);

- prevede obblighi specifici in capo ai responsabili del trattamento, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del registro dei trattamenti svolti (ex art. 30, paragrafo 2); l'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti (ex art. 32 regolamento); la designazione di un RPD-DPO (si segnalano, al riguardo, le linee-guida in materia di responsabili della protezione dei dati recente-mente adottate dal Gruppo "Articolo 29", qui disponibili: www.garante-privacy.it/regolamentoue/rpd), nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che anche il responsabile non stabilito nell'Ue dovrà designare un rappresentante in Italia quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevedeva l'art. 5, comma 2, del Codice.

Responsabile della protezione dei dati

Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/responsabile. Non è un caso, infatti, che fra i compiti del RPD la sor-veglianza sull'ossrvazione del regolamento, informazione e dello svolgimento della valutazione di impatto di cui all'art. 35. La sua designazione è obbligatoria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali).

Decalogo del Garante

- **Cellulari, tablet e smartphone**: il loro utilizzo deve ritenersi consentito **per uso personale e nel rispetto delle persone**.
- Si possono **registrare le lezioni** (spetta agli studi scolastici decidere come regolamentare l'utilizzo di questi strumenti elettronici compresa la possibilità di vietare del tutto l'uso di essi).
- Si possono **consultare** in classe libri elettronici e testi on line.
- **Divieto di diffondere immagini e video sul Web senza il consenso** delle persone eventualmente riprese. (Si ricorda che la diffusione di immagini che ledono la riservatezza e la dignità delle persone può far incorrere in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati).
- **Temi in classe**: l'insegnante può liberamente assegnare gli alunni temi che riguardano il loro mondo personale senza che ciò possa costituire una violazione della privacy. L'insegnante deve però trovare il giusto equilibrio (in caso di lettura dei temi in classe) tra le esigenze dell'insegnamento e il rispetto della privacy quando nei temi vengono trattati argomenti delicati.
- **Gite scolastiche, saggi e recite**: Non c'è violazione della privacy per le riprese fotografiche e per i video fatti dai genitori durante recite, saggi e gite scolastiche, ma queste immagini possono essere usate solo in ambito familiare. Se si intende pubblicarle nel Web, occorre il **consenso delle persone presenti nei video e nelle foto**.
- E' vietato pubblicare nel **sito della scuola** le generalità di chi è in ritardo nel pagamento della retta del servizio mensa.
- È vietato pubblicare i nominativi di chi **usufruisce gratuitamente della mensa**.
- Nel sito della scuola **gli avvisi devono avere carattere generale** giacché ogni altra comunicazione di carattere personale deve essere trasmessa individualmente.
- **Utilizzo di telecamere:** Pur non essendo vietata l'istallazione all'interno degli istituti, la loro presenza deve essere segnalata con cartelli e, in ogni caso, il funzionamento delle telecamere deve avvenire solo negli orari di chiusura. Se poi le telecamere sono collocate all'esterno della scuola è necessario delimitarne l'angolo visuale. In ogni caso le immagini registrate vanno cancellate dopo 24 ore.
- **Iscrizione on-line:** particolare attenzione deve essere prestata inoltre all'eventuale raccolta di dati sensibili. Il trattamento di questi dati, oltre a dover essere espressamente previsto dalla normativa, richiede infatti speciali cautele e può essere effettuato solo se i dati sensibili sono indispensabili per l'attività istituzionale svolta
- **Voti ed esami:** gli esiti degli scrutini o degli esami di Stato sono pubblici. Le informazioni sul rendimento scolastico sono soggette ad un regime di conoscibilità stabilito dal Ministero dell'Istruzione dell'Università e della Ricerca. È necessario però che, nel pubblicare i voti degli scrutini e degli esami nei tabelloni, l'istituto scolastico eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o altri dati personali.
- **Attività di ricerca:** se prevedono l'utilizzo di questionari con raccolta di informazioni personali, è necessaria una preventiva informativa ad alunni e genitori sugli scopi della ricerca, le modalità del trattamento e le misure di sicurezza che vengono adottate.

.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI

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

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

del 27 aprile 2016

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

(Testo rilevante ai fini del SEE)

Indice

NOTA PER LA LETTURA DEL TESTO

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

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

del 27 aprile 2016

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

(Testo rilevante ai fini del SEE)

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,
visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16,
vista la proposta della Commissione europea,
previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,
visto il parere del Comitato economico e sociale europeo ([1]),
visto il parere del Comitato delle regioni ([2]),
deliberando secondo la procedura legislativa ordinaria ([3]),
considerando quanto segue:

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

(2) I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o

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

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

(4) Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

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

(6) La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazio-

ni personali che li 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 li 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 livel-

lo di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio 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 riguar-

danti 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'intenzio-

ne 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 all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, 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 all'interno 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, a marcatori temporanei (cookies) o a identificativi di altro tipo, come 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 destinata-

ri 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 espresso 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 ribonu-

cleico (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 li 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 li 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 legislati-

vo 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 esprimere 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 espresso 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 espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto 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 espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere 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 legale 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 pubbli-

che, 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 sotto-

porre 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 saranno 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 con-

senso 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 con-

nesse 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 infor-

mazioni 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 del contesto specifici in cui i dati personali sono trattati. Inoltre l'interessa-

to 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 informazio-

ni 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 la 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 ritirato 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 trattamen-

to 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, sia con riguardo a quello iniziale o ulteriore, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto. Tale diritto dovrebbe esse-

re 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 fatto-

ri 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 che 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 che comportano 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 le basi giuridiche 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 di default. 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 di default 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 monitoraggio 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 tito-

lare 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 monitorare 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 ter-

mine 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, segnata-

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

(112) Tali deroghe dovrebbero in particolare valere per i trasferimenti di dati richiesti e necessari per importanti motivi di interesse pubblico, ad esempio nel caso di scambio internazionale di dati tra autorità garanti della concorrenza, amministrazioni fiscali o doganali, autorità di controllo finanziario, servizi competenti in materia di

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

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

(114) In ogni caso, se la Commissione non ha adottato alcuna decisione circa il livello adeguato di protezione dei dati di un paese terzo, il titolare del trattamento o il

responsabile del trattamento dovrebbe ricorrere a soluzioni che diano all'interessato diritti effettivi e azionabili in relazione al trattamento dei suoi dati personali nell'Unione, dopo il trasferimento, così da continuare a beneficiare dei diritti fondamentali e delle garanzie.

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

(116) Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati dall'insufficienza di poteri per prevenire e correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. Pertanto vi è la necessità di promuovere una più stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni e condurre indagini di concerto con le loro controparti internazionali. Al fine di sviluppare meccanismi di cooperazione internazionale per agevolare e prestare mutua assistenza a livello internazionale nell'applicazione della legislazio-

ne sulla protezione dei dati personali, la Commissione e le autorità di controllo dovrebbero scambiare informazioni e cooperare, nell'ambito di attività connesse con l'esercizio dei loro poteri, con le autorità competenti in paesi terzi, sulla base della reciprocità e in conformità del presente regolamento.

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

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

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

(120) Ciascuna autorità di controllo dovrebbe disporre delle risorse umane e finanziarie, dei locali e delle infrastrutture necessari per l'effettivo adempimento dei propri compiti, compresi quelli di assistenza reciproca e cooperazione con altre autorità di controllo in tutta l'Unione. Ciascuna autorità di controllo dovrebbe disporre di un bilancio annuale, separato e pubblico, che può far parte del bilancio generale statale o nazionale.

(121) Le condizioni generali applicabili al membro o ai membri dell'autorità di controllo dovrebbero essere stabilite per legge da ciascuno Stato membro e dovrebbero in particolare prevedere che tali membri devono essere nominati, attraverso una procedura trasparente, dal parlamento, dal governo o dal capo di Stato dello Stato membro, sulla base di una proposta del governo, di un membro del governo, del parlamento o di una sua camera, o da un organismo indipendente incaricato ai sensi del dirit-

to degli Stati membri. Al fine di assicurare l'indipendenza dell'autorità di controllo, è opportuno che il membro o i membri di tale autorità agiscano con integrità, si astengano da qualunque azione incompatibile con le loro funzioni e, per tutta la durata del mandato, non esercitino alcuna altra attività incompatibile, remunerata o meno. L'autorità di controllo dovrebbe disporre di proprio personale, scelto dalla stessa autorità di controllo o da un organismo indipendente istituito ai sensi del diritto degli Stati membri, che dovrebbe essere soggetto alla direzione esclusiva del membro o dei membri dell'autorità di controllo.

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

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

(124) Qualora il trattamento dei dati personali abbia luogo nell'ambito delle attività di uno stabilimento di un titolare del trattamento o di un responsabile del trattamento nell'Unione e il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro o qualora il trattamento effettuato nell'ambito

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

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

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

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

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

(129) Al fine di garantire un monitoraggio e un'applicazione coerenti del presente regolamento in tutta l'Unione, le autorità di controllo dovrebbero avere in ciascuno Stato membro gli stessi compiti e poteri effettivi, fra cui poteri di indagine, poteri correttivi e sanzionatori, e poteri autorizzativi e consultivi, segnatamente in caso di reclamo proposto da persone fisiche, e fatti salvi i poteri delle autorità preposte all'eser-

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

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

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

(132) Le attività di sensibilizzazione delle autorità di controllo nei confronti del pubblico dovrebbero comprendere misure specifiche per i titolari del trattamento e i responsabili del trattamento, comprese le micro, piccole e medie imprese, e le persone fisiche in particolare nel contesto educativo.

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

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

(135) È opportuno istituire un meccanismo di coerenza per la cooperazione tra le autorità di controllo, al fine di assicurare un'applicazione coerente del presente regola-

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

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

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

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

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

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

(141) Ciascun interessato dovrebbe avere il diritto di proporre reclamo a un'unica autorità di controllo, in particolare nello Stato membro in cui risiede abitualmente, e il diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento o se l'autorità di controllo non dà seguito a un reclamo, lo respinge in tutto o in parte o lo archivia o non agisce quando è necessario intervenire per proteggere i diritti dell'interessato. Successivamente al reclamo si dovrebbe condurre un'indagine, soggetta a controllo giurisdizionale, nella misura in cui ciò sia opportuno nel caso specifico. È opportuno che l'autorità di controllo informi gli interessati dello stato e dell'esito del reclamo entro un termine ragionevole. Se il caso richiede un'ulteriore indagine o il coordinamento con un'altra autorità di controllo, l'interessato dovrebbe ricevere informazioni interlocutorie. Per agevolare la proposizione di reclami, ogni autorità di controllo dovrebbe adottare misure quali la messa a dispo-

sizione di un modulo per la proposizione dei reclami compilabile anche elettronicamente, senza escludere altri mezzi di comunicazione.

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

(143) Qualsiasi persona fisica o giuridica ha diritto di proporre un ricorso per l'annullamento delle decisioni del comitato dinanzi alla Corte di giustizia, alle condizioni previste all'articolo 263 TFUE. In quanto destinatari di tali decisioni, le autorità di controllo interessate che intendono impugnarle, devono proporre ricorso entro due mesi dalla loro notifica, conformemente all'articolo 263 TFUE. Ove le decisioni del comitato si riferiscano direttamente e individualmente a un titolare del trattamento, a un responsabile del trattamento o al reclamante, quest'ultimo può proporre un ricorso per l'annullamento di tali decisioni e dovrebbe farlo entro due mesi dalla loro pubblicazione sul sito web del comitato, conformemente all'articolo 263 TFUE. Fatto salvo tale diritto ai sensi dell'articolo 263 TFUE, ogni persona fisica o giuridica dovrebbe poter proporre un ricorso giurisdizionale effettivo dinanzi alle competenti autorità giurisdizionali nazionali contro una decisione dell'autorità di controllo che produce effetti giuridici nei confronti di detta persona. Tale decisione riguarda in particolare l'esercizio di poteri di indagine, correttivi e autorizzativi da parte dell'autorità di controllo o l'archiviazione o il rigetto dei reclami. Tuttavia,

tale diritto a un ricorso giurisdizionale effettivo non comprende altre misure adottate dalle autorità di controllo che non sono giuridicamente vincolanti, come pareri o consulenza forniti dall'autorità di controllo. Le azioni contro l'autorità di controllo dovrebbero essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita e dovrebbero essere effettuate in conformità del diritto processuale dello Stato membro in questione. Tali autorità giurisdizionali dovrebbero esercitare i loro pieni poteri giurisdizionali, ivi compreso quello di esaminare tutte le questioni di fatto e di diritto che abbiano rilevanza per la controversia dinanzi a esse pendente.

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

(144) Qualora un'autorità giurisdizionale adita per un'azione contro una decisione di un'autorità di controllo abbia motivo di ritenere che le azioni riguardanti lo stesso trattamento, quale lo stesso oggetto relativamente al trattamento da parte dello stesso titolare del trattamento o dello stesso responsabile del trattamento, o lo stesso titolo, siano sottoposte a un'autorità giurisdizionale competente in un altro Stato membro, l'autorità giurisdizionale adita dovrebbe contattare tale autorità giurisdi-

zionale al fine di confermare l'esistenza di tali azioni connesse. Se le azioni connesse sono pendenti dinanzi a un'autorità giurisdizionale in un altro Stato membro, qualsiasi autorità giurisdizionale successivamente adita può sospendere l'azione proposta dinanzi a essa o, su richiesta di una delle parti, può dichiarare la propria incompetenza a favore della prima autorità giurisdizionale adita se tale autorità giurisdizionale è competente a conoscere delle azioni in questione e la sua legge consente la riunione delle azioni. Le azioni sono considerate connesse quando hanno tra loro un legame così stretto da rendere opportuno trattarle e decidere in merito contestualmente, per evitare il rischio di sentenze incompatibili risultanti da azioni separate.

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

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

bilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento.

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

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

(149) Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali

adottate in virtù ed entro i limiti del presente regolamento. Tali sanzioni penali possono altresì autorizzare la sottrazione dei profitti ottenuti attraverso violazioni del presente regolamento. Tuttavia, l'imposizione di sanzioni penali per violazioni di tali norme nazionali e di sanzioni amministrative non dovrebbe essere in contrasto con il principio del ne bis in idem quale interpretato dalla Corte di giustizia.

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

(151) I sistemi giudiziari di Danimarca ed Estonia non consentono l'irrogazione di sanzioni amministrative pecuniarie come previsto dal presente regolamento. Le norme relative alle sanzioni amministrative pecuniarie possono essere applicate in maniera tale che in Danimarca la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali quale sanzione penale e in Estonia la sanzione pecuniaria sia imposta dall'autorità di controllo nel quadro di una procedura d'infrazione, purché l'applicazione di tali norme in detti Stati membri abbia effetto equi-

valente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. Le competenti autorità giurisdizionali nazionali dovrebbero pertanto tener conto della raccomandazione dell'autorità di controllo che avvia l'azione sanzionatoria. In ogni caso, le sanzioni pecuniarie irrogate dovrebbero essere effettive, proporzionate e dissuasive.

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

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

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

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

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

(157) Combinando informazioni provenienti dai registri, i ricercatori possono ottenere nuove conoscenze di grande utilità relativamente a patologie diffuse come le malattie cardiovascolari, il cancro e la depressione. Avvalendosi dei registri, i risultati delle ricerche possono acquistare maggiore rilevanza, dal momento che si basano su una popolazione più ampia. Nell'ambito delle scienze sociali, la ricerca basata sui registri consente ai ricercatori di ottenere conoscenze essenziali sulla correlazione a lungo termine tra numerose condizioni sociali, quali la disoccupazione e il livello di istruzione, e altre condizioni di vita. I risultati delle ricerche ottenuti dai registri for-

niscono conoscenze solide e di alta qualità, che possono costituire la base per l'elaborazione e l'attuazione di politiche basate sulla conoscenza, migliorare la qualità della vita per molte persone, migliorare l'efficienza dei servizi sociali. Al fine di facilitare la ricerca scientifica, i dati personali possono essere trattati per finalità di ricerca scientifica fatte salve condizioni e garanzie adeguate previste dal diritto dell'Unione o degli Stati membri.

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

(159) Qualora i dati personali siano trattati per finalità di ricerca scientifica, il presente regolamento dovrebbe applicarsi anche a tale trattamento. Nell'ambito del presente regolamento, il trattamento di dati personali per finalità di ricerca scientifica dovrebbe essere interpretato in senso lato e includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica. Per rispondere alle specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica. Se il risultato della ricerca scientifica, in particolare nel contesto sanitario, costituisce motivo per ulteriori misure nell'interesse dell'interessato, le norme generali del presente regolamento dovrebbero applicarsi in vista di tali misure.

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

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

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

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

(164) Per quanto riguarda il potere delle autorità di controllo di ottenere, dal titolare del trattamento o dal responsabile del trattamento, accesso ai dati personali e accesso ai loro locali, gli Stati membri possono stabilire per legge, nei limiti del presente regolamento, norme specifiche per tutelare il segreto professionale o altri obblighi equi-

valenti di segretezza, qualora si rendano necessarie per conciliare il diritto alla protezione dei dati personali con il segreto professionale. Ciò non pregiudica gli obblighi esistenti degli Stati membri di adottare norme relative al segreto professionale laddove richiesto dal diritto dell'Unione.

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

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

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

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

di informazioni per via elettronica tra i titolari del trattamento, i responsabili del trattamento e le autorità di controllo per norme vincolanti d'impresa; assistenza reciproca; e modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato.

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

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

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

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

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

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I
Disposizioni generali

Articolo 1

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

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

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

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

Articolo 2

Ambito di applicazione materiale (C 15-21)

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

2. Il presente regolamento non si applica ai trattamenti di dati personali:

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

b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE;

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

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

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

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

Articolo 3

Ambito di applicazione territoriale

1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. (**C22**)

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

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

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

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

Articolo 4

Definizioni

Ai fini del presente regolamento s'intende per:

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

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

3) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro; (**C67**)

4) «**profilazione**»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica; (**C24, C30, C71-C72**)

5) «**pseudonimizzazione**»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di

informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; (**C26, C28-C29**)

6) «**archivio**»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico; (**C15**)

7) «**titolare del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri; (**C74**)

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

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

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

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

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati; (**C85**)

13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; (**C34**)

14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; (**C51**)

15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; (**C35**)

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

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

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

17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'artico-

lo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento; (**C80**)

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

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

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

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

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

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

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

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

23) «**trattamento transfrontaliero**»:

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

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

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

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

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

CAPO II
Principi

Articolo 5

Principi applicabili al trattamento di dati personali

1. I dati personali sono: (**C39**)

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

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

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

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

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

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non

autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

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

Articolo 6

Liceità del trattamento

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

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

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

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

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

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

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

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

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

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

a) dal diritto dell'Unione; o

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

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

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

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

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

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

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

Articolo 7

Condizioni per il consenso (C42, C43)

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

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

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

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

Articolo 8

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

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

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

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

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

Articolo 9

Trattamento di categorie particolari di dati personali

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. (**C51**)

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

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

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

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

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

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

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

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

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

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

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

3. I dati personali di cui al paragrafo 1 possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti. (**C53**)

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

Articolo 10

Trattamento dei dati personali relativi a condanne penali e reati

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

Articolo 11

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

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

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

CAPO III
Diritti dell'interessato

Sezione 1

Trasparenza e modalità

Articolo 12

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

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

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

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

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

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

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

b) rifiutare di soddisfare la richiesta.Incombe al titolare del trattamento l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

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

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

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

Sezione 2

Informazione e accesso ai dati personali

Articolo 13

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Articolo 14

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

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

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

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

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

d) le categorie di dati personali in questione;

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

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

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

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

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

c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamen-

to dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

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

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

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

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

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

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

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

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

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

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

a) l'interessato dispone già delle informazioni;

b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse,

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

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

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

Articolo 15

Diritto di accesso dell'interessato (C63, C64)

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

a) le finalità del trattamento;

b) le categorie di dati personali in questione;

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

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

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

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

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

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

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

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

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

Sezione 3

Rettifica e cancellazione

Articolo 16

Diritto di rettifica (C65)

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

Articolo 17

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

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

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

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

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

d) i dati personali sono stati trattati illecitamente;

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

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

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

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

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

b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'ese-

cuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

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

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

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

Articolo 18

Diritto di limitazione di trattamento (C67)

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

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

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

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

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

2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamen-

to, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

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

Articolo 19

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

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

Articolo 20

Diritto alla portabilità dei dati (C68)

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

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

b) il trattamento sia effettuato con mezzi automatizzati.

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

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

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

Sezione 4

Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche

Articolo 21

Diritto di opposizione (C69, C70)

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

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

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

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

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

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

Articolo 22

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

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

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

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

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

c) si basi sul consenso esplicito dell'interessato.

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

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9,

paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Sezione 5

Limitazioni

Articolo 23

Limitazioni (C73)

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

a) la sicurezza nazionale;

b) la difesa;

c) la sicurezza pubblica;

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

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

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

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

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

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

j) l'esecuzione delle azioni civili.

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

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

b) le categorie di dati personali;

c) la portata delle limitazioni introdotte;

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

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

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

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

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

CAPO IV
Titolare del trattamento e responsabile del trattamento

Sezione 1
Obblighi generali

Articolo 24

Responsabilità del titolare del trattamento (C74-C78)

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

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

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

Articolo 25

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

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costi-

tuiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.

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

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

Articolo 26

Contitolari del trattamento (C79)

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

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

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

Articolo 27

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

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

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

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

b) alle autorità pubbliche o agli organismi pubblici.

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

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

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

Articolo 28

Responsabile del trattamento (C81)

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

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

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

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

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

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

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

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

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

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

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.Con riguardo alla lettera h) del primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

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

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

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

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

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

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

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

Articolo 29

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

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

Articolo 30

Registri delle attività di trattamento (C82)

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

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

b) le finalità del trattamento;

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

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

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

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

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

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

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

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

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

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

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

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

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

Articolo 31

Cooperazione con l'autorità di controllo (C82)

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

Sezione 2

Sicurezza dei dati personali

Articolo 32

Sicurezza del trattamento (C83)

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

a) la pseudonimizzazione e la cifratura dei dati personali;

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

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

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

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

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

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è

istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo (C85, C87, C88)

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

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

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

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

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

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

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

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

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

Articolo 34

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

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

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

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

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

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

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

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

Sezione 3

Valutazione d'impatto sulla protezione dei dati e consultazione preventiva

Articolo 35

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

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

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

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

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

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

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

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

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipolo-

gie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

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

7. La valutazione contiene almeno:

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

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

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

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

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

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

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del tratta-

mento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

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

Articolo 36

Consultazione preventiva (C94-C96)

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

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

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

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

b) le finalità e i mezzi del trattamento previsto;

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

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

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

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

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

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

Sezione 4

Responsabile della protezione dei dati

Articolo 37

Designazione del responsabile della protezione dei dati (C97)

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

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

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

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

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

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

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

5. Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

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

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

Articolo 38

Posizione del responsabile della protezione dei dati (C97)

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

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

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

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

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in meri-

to all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

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

Articolo 39

Compiti del responsabile della protezione dei dati (C97)

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

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

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

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

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

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

Sezione 5

Codici di condotta e certificazione

Articolo 40

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

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

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

a) il trattamento corretto e trasparente dei dati;

b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;

c) la raccolta dei dati personali;

d) la pseudonimizzazione dei dati personali;

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

f) l'esercizio dei diritti degli interessati;

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

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

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

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

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

3. Oltre all'adesione ai codici di condotta approvati ai sensi del paragrafo 5 del presente articolo e aventi validità generale a norma del paragrafo 9 del presente articolo da parte di titolari o responsabili soggetti al presente regolamento, possono aderire a tali codici di condotta anche i titolari del trattamento o i responsabili del trattamento che non sono soggetti al presente regolamento ai sensi dell'articolo 3, al fine di fornire adeguate garanzie nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera e). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante e azionabile, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati.

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

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

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

7. Qualora il progetto di codice di condotta si riferisca alle attività di trattamento in vari Stati membri, prima di approvare il progetto, la modifica o la proroga, l'autorità di con-

trollo che è competente ai sensi dell'articolo 55 lo sottopone, tramite la procedura di cui all'articolo 63, al comitato, il quale formula un parere sulla conformità al presente regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 del presente articolo, sulla previsione di adeguate garanzie.

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

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

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

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

Articolo 41

Monitoraggio dei codici di condotta approvati

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

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

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

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

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

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

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

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

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

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

Articolo 42

Certificazione (C100)

1. Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della prote-

zione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

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

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

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

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

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

7. La certificazione è rilasciata al titolare del trattamento o responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché

continuino a essere soddisfatti i requisiti pertinenti. La certificazione è revocata, se del caso, dagli organismi di certificazione di cui all'articolo 43 o dall'autorità di controllo competente, a seconda dei casi, qualora non siano o non siano più soddisfatti i requisiti per la certificazione.

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

Articolo 43

Organismi di certificazione (C166-C168)

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

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

b) dall'organismo nazionale di accreditamento designato in virtù del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio ([20]) conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56.2.

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

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

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

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

d) hanno istituito procedure e strutture atte a gestire i reclami relativi a violazioni della certificazione o il modo in cui la certificazione è stata o è attuata dal titolare del trattamento o dal responsabile del trattamento e a rendere dette procedure e strutture trasparenti per gli interessati e il pubblico; e

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

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

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

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

6. I requisiti di cui al paragrafo 3 del presente articolo e i criteri di cui all'articolo 42, paragrafo 5, sono resi pubblici dall'autorità di controllo in forma facilmente accessibile. Le autorità di controllo provvedono a trasmetterli anche al comitato. Il comitato raccoglie in un registro tutti i meccanismi di certificazione e i sigilli di protezione dei dati e li rende pubblici con qualsiasi mezzo appropriato.

7. Fatto salvo il capo VIII, l'autorità di controllo competente o l'organismo nazionale di accreditamento revoca l'accreditamento di un organismo di certificazione di cui al para-

grafo 1 del presente articolo, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il presente regolamento.

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

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

CAPO V

Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali

Articolo 44

Principio generale per il trasferimento (C101, C102)

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato.

Articolo 45

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

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

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

a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza

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

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

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

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

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

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

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

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

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

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

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

Articolo 46

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

1. In mancanza di una decisione ai sensi dell'articolo 45, paragrafo 3, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo

o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

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

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

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

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

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

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

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

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

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

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

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

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

Articolo 47

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

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

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

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

c) soddisfino i requisiti di cui al paragrafo 2.

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

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

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

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

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

e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;

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

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

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

i) le procedure di reclamo;

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

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

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

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

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

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

Articolo 48

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

Le sentenze di un'autorità giurisdizionale e le decisioni di un'autorità amministrativa di un paese terzo che dispongono il trasferimento o la comunicazione di dati personali da

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

Articolo 49

Deroghe in specifiche situazioni (C111-C114)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Articolo 50

Cooperazione internazionale per la protezione dei dati personali (C116)

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

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

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

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

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

CAPO VI

Autorità di controllo indipendenti

Sezione 1

Indipendenza

Articolo 51

Autorità di controllo (C117)

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

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

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

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

Articolo 52

Indipendenza (C118-C120)

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

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

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

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

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

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

Articolo 53

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

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

— dal rispettivo parlamento;

— dal rispettivo governo;

— dal rispettivo capo di Stato; oppure

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

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

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

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

Articolo 54

Norme sull'istituzione dell'autorità di controllo

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

a) l'istituzione di ogni autorità di controllo;

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

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

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

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

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

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

Sezione 2

Competenza, compiti e poteri

Articolo 55

Competenza (C122, C123, C128)

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

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

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

Articolo 56

Competenza dell'autorità di controllo capofila (C124, C125, C127, C128, C131)

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

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

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

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

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

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

Articolo 57

Compiti (C122, C129, C132)

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

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

b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai

rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

t) contribuisce alle attività del comitato;

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

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

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

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

4. Qualora le richieste siano manifestamente infondate o eccessive, in particolare per il carattere ripetitivo, l'autorità di controllo può addebitare un contributo spese ragionevole basato sui costi amministrativi o rifiutarsi di soddisfare la richiesta. Incombe all'autorità di controllo dimostrare il carattere manifestamente infondato o eccessivo della richiesta.

Articolo 58

Poteri (C122, C129)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Articolo 59

Relazioni di attività

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

CAPO VII
Cooperazione e coerenza

Sezione 1

Cooperazione

Articolo 60

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

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

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

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

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

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

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

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

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

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

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

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

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

Articolo 61

Assistenza reciproca (C123, C133, C167-C168)

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

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

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

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

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

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

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

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

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

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

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

Articolo 62

Operazioni congiunte delle autorità di controllo (C134)

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

2. Qualora il titolare del trattamento o responsabile del trattamento abbia stabilimenti in vari Stati membri o qualora esista la probabilità che il trattamento abbia su un numero significativo di interessati in più di uno Stato membro un impatto negativo sostanziale,

un'autorità di controllo di ogni Stato membro in questione ha il diritto di partecipare alle operazioni congiunte. L'autorità di controllo che è competente conformemente all'articolo 56, paragrafo 1, o all'articolo 56 paragrafo 4, invita l'autorità di controllo di ogni Stato membro interessato a partecipare all'operazione congiunta in questione e risponde senza ritardo alle richieste di partecipazione delle autorità di controllo.

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

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

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

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

7. Qualora sia prevista un'operazione congiunta e un'autorità di controllo non si conformi entro un mese all'obbligo di cui al paragrafo 2, seconda frase, del presente articolo, le altre autorità di controllo possono adottare misure provvisorie nel territorio del loro Stato

membro ai sensi dell'articolo 55. Si considera, in tal caso, che urga intervenire ai sensi dell'articolo 66, paragrafo 1, e che siano necessari un parere o una decisione vincolante d'urgenza da parte del comitato a norma dell'articolo 66, paragrafo 2.

Sezione 2

Coerenza

Articolo 63

Meccanismo di coerenza (C135, C138)

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

Articolo 64

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

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

a) è finalizzata a stabilire un elenco di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;

b) riguarda una questione di cui all'articolo 40, paragrafo 7, relativa alla conformità al presente regolamento di un progetto di codice di condotta o una modifica o proroga di un codice di condotta;

c) è finalizzata ad approvare i criteri per l'accreditamento di un organismo ai sensi dell'articolo 41, paragrafo 3, o di un organismo di certificazione ai sensi dell'articolo 43, paragrafo 3;

d) è finalizzata a determinare clausole tipo di protezione dei dati di cui all'articolo 46, paragrafo 2, lettera d), e all'articolo 28, paragrafo 8;

e) è finalizzata ad autorizzare clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a); oppure

f) è finalizzata ad approvare norme vincolanti d'impresa ai sensi dell'articolo 47.

2. Qualsiasi autorità di controllo, il presidente del comitato o la Commissione può richiedere che le questioni di applicazione generale o che producono effetti in più di uno Stato membro siano esaminate dal comitato al fine di ottenere un parere, in particolare se un'autorità di controllo competente non si conforma agli obblighi relativi all'assistenza reciproca ai sensi dell'articolo 61 o alle operazioni congiunte ai sensi dell'articolo 62.

3. Nei casi di cui ai paragrafi 1 e 2, il comitato emette un parere sulla questione che gli è stata presentata, purché non abbia già emesso un parere sulla medesima questione. Tale parere è adottato entro un termine di otto settimane a maggioranza semplice dei membri del comitato. Tale termine può essere prorogato di sei settimane, tenendo conto della complessità della questione. Per quanto riguarda il progetto di decisione di cui al paragrafo 1 trasmesso ai membri del comitato conformemente al paragrafo 5, il membro che non abbia sollevato obiezioni entro un termine ragionevole indicato dal presidente è considerato assentire al progetto di decisione.

4. Senza ingiustificato ritardo, le autorità di controllo e la Commissione comunicano per via elettronica, usando un modulo standard, al comitato tutte le informazioni utili, in particolare, a seconda del caso, una sintesi dei fatti, il progetto di decisione, i motivi che rendono necessaria l'attuazione di tale misura e i pareri delle altre autorità di controllo interessate.

5. Il presidente del comitato informa, senza ingiustificato ritardo, con mezzi elettronici:

a) i membri del comitato e la Commissione di tutte le informazioni utili che sono state comunicate al comitato con modulo standard. Se necessario, il segretariato del comitato fornisce una traduzione delle informazioni utili; e

b) l'autorità di controllo di cui, secondo i casi, ai paragrafi 1 e 2, e la Commissione in merito al parere, che rende pubblico.

6. L'autorità di controllo competente si astiene dall'adottare il suo progetto di decisione di cui al paragrafo 1 entro il termine di cui al paragrafo 3.

7. L'autorità di controllo di cui al paragrafo 1 tiene nella massima considerazione il parere del comitato e, entro due settimane dal ricevimento del parere, comunica per via elettronica, usando un modulo standard, al presidente del comitato se intende mantenere o modificare il progetto di decisione e, se del caso, il progetto di decisione modificato.

8. Se entro il termine di cui al paragrafo 7 del presente articolo l'autorità di controllo interessata informa il presidente del comitato, fornendo le pertinenti motivazioni, che non intende conformarsi al parere del comitato, in tutto o in parte, si applica l'articolo 65, paragrafo 1.

Articolo 65

Composizione delle controversie da parte del comitato (C136, C138, C143)

1. Al fine di assicurare l'applicazione corretta e coerente del presente regolamento nei singoli casi, il comitato adotta una decisione vincolante nei seguenti casi:

a) se, in un caso di cui all'articolo 60, paragrafo 4, un'autorità di controllo interessata ha sollevato un'obiezione pertinente e motivata a un progetto di decisione dell'autorità capofila o l'autorità capofila ha rigettato tale obiezione in quanto non pertinente o non motivata. La decisione vincolante riguarda tutte le questioni oggetto dell'obiezione pertinente e motivata, in particolare se sussista una violazione del presente regolamento;

b) se vi sono opinioni contrastanti in merito alla competenza delle autorità di controllo interessate per lo stabilimento principale;

c) se un'autorità di controllo competente non richiede il parere del comitato nei casi di cui all'articolo 64, paragrafo 1, o non si conforma al parere del comitato emesso a norma dell'articolo 64. In tal caso qualsiasi autorità di controllo interessata o la Commissione può comunicare la questione al comitato.

2. La decisione di cui al paragrafo 1 è adottata entro un mese dal deferimento della questione da parte di una maggioranza di due terzi dei membri del comitato. Tale termine può essere prorogato di un mese, in considerazione della complessità della questione. La

decisione di cui al paragrafo 1 è motivata e trasmessa all'autorità di controllo capofila e a tutte le autorità di controllo interessate ed è per esse vincolante.

3. Qualora non sia stato in grado di adottare una decisione entro i termini di cui al paragrafo 2, il comitato adotta la sua decisione entro due settimane dalla scadenza del secondo mese di cui al paragrafo 2, a maggioranza semplice dei membri del comitato. In caso di parità di voti dei membri del comitato, prevale il voto del presidente.

4. Le autorità di controllo interessate non adottano una decisione sulla questione sottoposta al comitato a norma del paragrafo 1 entro i termini di cui ai paragrafi 2 e 3.

5. Il presidente del comitato notifica senza ingiustificato ritardo alle autorità di controllo interessate la decisione di cui al paragrafo 1 e ne informa la Commissione. La decisione è pubblicata senza ritardo sul sito web del comitato dopo che l'autorità di controllo ha notificato la decisione definitiva di cui al paragrafo 6.

6. L'autorità di controllo capofila o, se del caso, l'autorità di controllo a cui è stato proposto il reclamo adotta la sua decisione definitiva in base alla decisione di cui al paragrafo 1 del presente articolo senza ingiustificato ritardo e al più tardi entro un mese dalla notifica della decisione da parte del comitato. L'autorità di controllo capofila o, se del caso, l'autorità di controllo a cui è stato proposto il reclamo, informa il comitato circa la data in cui la decisione definitiva è notificata rispettivamente al titolare del trattamento o al responsabile del trattamento e all'interessato. La decisione definitiva delle autorità di controllo interessate è adottata ai sensi dell'articolo 60, paragrafi 7, 8 e 9. La decisione finale fa riferimento alla decisione di cui al paragrafo 1 del presente articolo e precisa che la decisione di cui a tale paragrafo sarà pubblicata sul sito web del comitato conformemente al paragrafo 5 del presente articolo. La decisione finale deve accludere la decisione di cui al paragrafo 1 del presente articolo.

Articolo 66

Procedura d'urgenza (C137)

1. In circostanze eccezionali, qualora ritenga che urga intervenire per proteggere i diritti e le libertà degli interessati, un'autorità di controllo interessata può, in deroga al meccanismo di coerenza di cui agli articoli 63, 64 e 65, o alla procedura di cui all'articolo 60, adot-

tare immediatamente misure provvisorie intese a produrre effetti giuridici nel proprio territorio, con un periodo di validità determinato che non supera i tre mesi. L'autorità di controllo comunica senza ritardo tali misure e la motivazione della loro adozione alle altre autorità di controllo interessate, al comitato e alla Commissione.

2. Qualora abbia adottato una misura ai sensi del paragrafo 1 e ritenga che urga adottare misure definitive, l'autorità di controllo può chiedere un parere d'urgenza o una decisione vincolante d'urgenza del comitato, motivando tale richiesta.

3. Qualsiasi autorità di controllo può chiedere un parere d'urgenza o una decisione vincolante d'urgenza, a seconda dei casi, del comitato qualora un'autorità di controllo competente non abbia adottato misure adeguate in una situazione in cui urge intervenire per proteggere i diritti e le libertà degli interessati, motivando la richiesta di tale parere o decisione, in particolare l'urgenza dell'intervento.

4. In deroga all'articolo 64, paragrafo 3, e all'articolo 65, paragrafo 2, il parere d'urgenza o la decisione vincolante d'urgenza di cui ai paragrafi 2 e 3 del presente articolo sono adottati entro due settimane a maggioranza semplice dei membri del comitato.

Articolo 67

Scambio di informazioni (C167-C168)

La Commissione può adottare atti di esecuzione di portata generale per specificare le modalità per lo scambio di informazioni per via elettronica tra autorità di controllo e tra le autorità di controllo e il comitato, in particolare il modulo standard di cui all'articolo 64.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.

Sezione 3

Comitato europeo per la protezione dei dati

Articolo 68

Comitato europeo per la protezione dei dati (C139)

1. Il comitato europeo per la protezione dei dati («comitato») è istituito quale organismo dell'Unione ed è dotato di personalità giuridica.

2. Il comitato è rappresentato dal suo presidente.

3. Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.

4. Qualora, in uno Stato membro, più autorità di controllo siano incaricate di sorvegliare l'applicazione delle disposizioni del presente regolamento, è designato un rappresentante comune conformemente al diritto di tale Stato membro.

5. La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato comunica alla Commissione le attività del comitato.

6. Nei casi di cui all'articolo 65, il garante europeo della protezione dei dati ha diritto di voto solo per decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione che corrispondono nella sostanza a quelli del presente regolamento.

Articolo 69

Indipendenza (C139)

1. Nell'esecuzione dei suoi compiti o nell'esercizio dei suoi poteri ai sensi degli articoli 70 e 71, il comitato opera con indipendenza.

2. Fatte salve le richieste della Commissione di cui all'articolo 70, paragrafo 1, lettera b), e all'articolo 70, paragrafo 2, nell'esecuzione dei suoi compiti o nell'esercizio dei suoi poteri il comitato non sollecita né accetta istruzioni da alcuno.

Articolo 70

Compiti del comitato (C139)

1. Il comitato garantisce l'applicazione coerente del presente regolamento. A tal fine, il comitato, di propria iniziativa o, se del caso, su richiesta della Commissione, in particolare:

a) sorveglia il presente regolamento e ne assicura l'applicazione corretta nei casi previsti agli articoli 64 e 65 fatti salvi i compiti delle autorità nazionali di controllo;

b) fornisce consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, comprese eventuali proposte di modifica del presente regolamento;

c) fornisce consulenza alla Commissione sul formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa;

d) pubblica linee guida, raccomandazioni e migliori prassi in materia di procedure per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico di cui all'articolo 17, paragrafo 2;

e) esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del presente regolamento e pubblica linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del presente regolamento;

f) pubblica linee guida, raccomandazioni e migliori pratiche conformemente alla lettera e) del presente paragrafo, per specificare ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione ai sensi dell'articolo 22, paragrafo 2;

g) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, per accertare la violazione di dati personali e determinare l'ingiustificato ritardo di cui all'articolo 33, paragrafi 1 e 2, e le circostanze particolari in cui il titolare del trattamento o il responsabile del trattamento è tenuto a notificare la violazione dei dati personali;

h) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, relative alle circostanze in cui una violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche di cui all'articolo 34, paragrafo 1;

i) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, al fine di specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali basati sulle norme vincolanti d'impresa applicate, rispettivamente, dai titolari del trattamento e dai responsabili del trattamento, nonché gli ulteriori requisiti per assicurare la protezione dei dati personali degli interessati di cui all'articolo 47;

j) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, al fine di specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali sulla base dell'articolo 49, paragrafo 1;

k) elabora per le autorità di controllo linee guida riguardanti l'applicazione delle misure di cui all'articolo 58, paragrafi 1, 2 e 3, e la previsione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 83;

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

m) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, per stabilire procedure comuni per le segnalazioni da parte di persone fisiche di violazioni del presente regolamento ai sensi dell'articolo 54, paragrafo 2;

n) incoraggia l'elaborazione di codici di condotta e l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati ai sensi degli articoli 40 e 42;

o) effettua l'accreditamento di organismi di certificazione e il suo riesame periodico a norma dell'articolo 43 e tiene un registro pubblico di organismi accreditati a norma dell'articolo 43, paragrafo 6, e dei titolari o responsabili del trattamento accreditati, stabiliti in paesi terzi a norma dell'articolo 42, paragrafo 7;

p) specifica i requisiti di cui all'articolo 43, paragrafo 3, ai fini dell'accreditamento degli organismi di certificazione ai sensi dell'articolo 42;

q) fornisce alla Commissione un parere in merito ai requisiti di certificazione di cui all'articolo 43, paragrafo 8;

r) fornisce alla Commissione un parere in merito alle icone di cui all'articolo 12, paragrafo 7;

s) fornisce alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale, così come per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione. A tal fine, la Commissione fornisce al comitato tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, con riguardo a tale paese terzo, territorio o settore specifico, o con l'organizzazione internazionale;

t) emette pareri sui progetti di decisione delle autorità di controllo conformemente al meccanismo di coerenza di cui all'articolo 64, paragrafo 1, e sulle questioni presentate conformemente all'articolo 64, paragrafo 2, ed emette decisioni vincolanti ai sensi dell'articolo 65, anche nei casi di cui all'articolo 66;

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

v) promuove programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di organizzazioni internazionali;

w) promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo;

x) emette pareri sui codici di condotta redatti a livello di Unione a norma dell'articolo 40, paragrafo 9; e

y) tiene un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle auto-

rità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza.

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

3. Il comitato trasmette pareri, linee guida, raccomandazioni e migliori prassi alla Commissione e al comitato di cui all'articolo 93, e li pubblica.

4. Se del caso, il comitato consulta le parti interessate e offre loro la possibilità di esprimere commenti entro un termine ragionevole. Fatto salvo l'articolo 76, il comitato rende pubblici i risultati della procedura di consultazione.

Articolo 71

Relazioni

1. Il comitato redige una relazione annuale sulla protezione delle persone fisiche con riguardo al trattamento nell'Unione e, se del caso, nei paesi terzi e nelle organizzazioni internazionali. La relazione è pubblicata ed è trasmessa al Parlamento europeo, al Consiglio e alla Commissione.

2. La relazione annuale include la valutazione dell'applicazione pratica delle linee guida, raccomandazioni e migliori prassi di cui all'articolo 70, paragrafo 1, lettera l), nonché delle decisioni vincolanti di cui all'articolo 65.

Articolo 72

Procedura

1. Il comitato decide a maggioranza semplice dei suoi membri, salvo se diversamente previsto dal presente regolamento.

2. Il comitato adotta il proprio regolamento interno deliberando a maggioranza di due terzi dei suoi membri e stabilisce le modalità del proprio funzionamento.

Articolo 73

Presidente

1. Il comitato elegge un presidente e due vicepresidenti tra i suoi membri a maggioranza semplice.

2. Il presidente e i vicepresidenti hanno un mandato di cinque anni, rinnovabile una volta.

Articolo 74

Compiti del presidente (C139)

1. Il presidente ha il compito di:

a) convocare le riunioni del comitato e stabilirne l'ordine del giorno;

b) notificare le decisioni adottate dal comitato a norma dell'articolo 65 all'autorità di controllo capofila e alle autorità di controllo interessate;

c) assicurare l'esecuzione tempestiva dei compiti del comitato, in particolare in relazione al meccanismo di coerenza di cui all'articolo 63.

2. Il comitato europeo stabilisce nel proprio regolamento interno la ripartizione dei compiti tra presidente e vicepresidenti.

Articolo 75

Segreteria (C140)

1. Il comitato dispone di una segreteria messa a disposizione dal garante europeo della protezione dei dati.

2. La segreteria svolge i propri compiti seguendo esclusivamente le istruzioni del presidente del comitato.

3. Il personale del garante europeo della protezione dei dati coinvolto nell'assolvimento dei compiti attribuiti al comitato dal presente regolamento è soggetto a linee gerarchiche

separate rispetto al personale coinvolto nello svolgimento dei compiti attribuiti al garante europeo della protezione dei dati.

4. Se del caso, il comitato e il garante europeo della protezione dei dati stabiliscono e pubblicano un protocollo d'intesa che attua il presente articolo, stabilisce i termini della loro cooperazione e si applica al personale del garante europeo della protezione dei dati coinvolto nell'assolvimento dei compiti attribuiti al comitato dal presente regolamento.

5. La segreteria presta assistenza in materia di analisi, amministrativa e logistica al comitato.

6. La segreteria è incaricata in particolare:

a) della gestione ordinaria del comitato;

b) della comunicazione tra i membri del comitato, il suo presidente e la Commissione;

c) della comunicazione con le altre istituzioni e il pubblico;

d) dell'uso di mezzi elettronici per la comunicazione interna ed esterna;

e) della traduzione delle informazioni rilevanti;

f) della preparazione delle riunioni del comitato e del relativo seguito;

g) della preparazione, redazione e pubblicazione dei pareri, delle decisioni sulla composizione delle controversie tra le autorità di controllo e di altri testi adottati dal comitato.

Articolo 76

Riservatezza

1. Se il comitato europeo lo ritiene necessario, le sue deliberazioni hanno carattere riservato, come previsto dal suo regolamento interno.

2. L'accesso ai documenti trasmessi ai membri del comitato, agli esperti e ai rappresentanti di terzi è disciplinato dal regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio ([21]).

CAPO VIII
Mezzi di ricorso, responsabilità e sanzioni

Articolo 77

Diritto di proporre reclamo all'autorità di controllo (C141)

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.

2. L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78.

Articolo 78

Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo (C141, C143)

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

2. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, ciascun interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora l'autorità di controllo che sia competente ai sensi degli articoli 55 e 56 non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto ai sensi dell'articolo 77.

3. Le azioni nei confronti dell'autorità di controllo sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita.

4. Qualora siano promosse azioni avverso una decisione di un'autorità di controllo che era stata preceduta da un parere o da una decisione del comitato nell'ambito del mecca-

nismo di coerenza, l'autorità di controllo trasmette tale parere o decisione all'autorità giurisdizionale.

Articolo 79

Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento (C141, C145, C147)

1. Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.

2. Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.

Articolo 80

Rappresentanza degli interessati (C142)

1. L'interessato ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli articoli 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82.

2. Gli Stati membri possono prevedere che un organismo, organizzazione o associazione di cui al paragrafo 1 del presente articolo, indipendentemente dal mandato conferito dall'interessato, abbia il diritto di proporre, in tale Stato membro, un reclamo all'autorità di controllo competente, e di esercitare i diritti di cui agli articoli 78 e 79, qualora ritenga che i diritti di cui un interessato gode a norma del presente regolamento siano stati violati in seguito al trattamento.

Articolo 81

Sospensione delle azioni (C144, C147)

1. L'autorità giurisdizionale competente di uno Stato membro che venga a conoscenza di azioni riguardanti lo stesso oggetto relativamente al trattamento dello stesso titolare del trattamento o dello stesso responsabile del trattamento pendenti presso un'autorità giurisdizionale in un altro Stato membro, prende contatto con tale autorità giurisdizionale nell'altro Stato membro per confermare l'esistenza delle azioni.

2. Qualora azioni riguardanti lo stesso oggetto relativamente al trattamento dello stesso titolare del trattamento o dello stesso responsabile del trattamento siano pendenti presso un'autorità giurisdizionale in un altro Stato membro, qualunque autorità giurisdizionale competente successivamente adita può sospendere le azioni.

3. Se tali azioni sono pendenti in primo grado, qualunque autorità giurisdizionale successivamente adita può parimenti dichiarare la propria incompetenza su richiesta di una delle parti a condizione che l'autorità giurisdizionale adita per prima sia competente a conoscere delle domande proposte e la sua legge consenta la riunione dei procedimenti.

Articolo 82

Diritto al risarcimento e responsabilità (C142, C146, C147)

1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.

4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.

6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2.

Articolo 83

Condizioni generali per infliggere sanzioni amministrative pecuniarie (C148, C150-C152)

1. Ogni autorità di controllo provvede affinché le sanzioni amministrative pecuniarie inflitte ai sensi del presente articolo in relazione alle violazioni del presente regolamento di cui ai paragrafi 4, 5 e 6 siano in ogni singolo caso effettive, proporzionate e dissuasive.

2. Le sanzioni amministrative pecuniarie sono inflitte, in funzione delle circostanze di ogni singolo caso, in aggiunta alle misure di cui all'articolo 58, paragrafo 2, lettere da a) a h) e j), o in luogo di tali misure. Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto dei seguenti elementi:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;

g) le categorie di dati personali interessate dalla violazione;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

3. Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento o un responsabile del trattamento viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave.

4. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 10 000 000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) gli obblighi del titolare del trattamento e del responsabile del trattamento a norma degli articoli 8, 11, da 25 a 39, 42 e 43;

b) gli obblighi dell'organismo di certificazione a norma degli articoli 42 e 43;

c) gli obblighi dell'organismo di controllo a norma dell'articolo 41, paragrafo 4;

5. In conformità del paragrafo 2, la violazione delle disposizioni seguenti è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore:

a) i principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;

b) i diritti degli interessati a norma degli articoli da 12 a 22;

c) i trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale a norma degli articoli da 44 a 49;

d) qualsiasi obbligo ai sensi delle legislazioni degli Stati membri adottate a norma del capo IX;

e) l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo ai sensi dell'articolo 58, paragrafo 2, o il negato accesso in violazione dell'articolo 58, paragrafo 1.

6. In conformità del paragrafo 2 del presente articolo, l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

7. Fatti salvi i poteri correttivi delle autorità di controllo a norma dell'articolo 58, paragrafo 2, ogni Stato membro può prevedere norme che dispongano se e in quale misura possono essere inflitte sanzioni amministrative pecuniarie ad autorità pubbliche e organismi pubblici istituiti in tale Stato membro.

8. L'esercizio da parte dell'autorità di controllo dei poteri attribuitile dal presente articolo è soggetto a garanzie procedurali adeguate in conformità del diritto dell'Unione e degli Stati membri, inclusi il ricorso giurisdizionale effettivo e il giusto processo.

9. Se l'ordinamento giuridico dello Stato membro non prevede sanzioni amministrative pecuniarie, il presente articolo può essere applicato in maniera tale che l'azione sanzionatoria sia avviata dall'autorità di controllo competente e la sanzione pecuniaria sia irrogata dalle competenti autorità giurisdizionali nazionali, garantendo nel contempo che i mezzi di ricorso siano effettivi e abbiano effetto equivalente alle sanzioni amministrative pecuniarie irrogate dalle autorità di controllo. In ogni caso, le sanzioni pecuniarie irrogate sono effettive, proporzionate e dissuasive. Tali Stati membri notificano alla Commissione le disposizioni di legge adottate a norma del presente paragrafo al più tardi entro 25 maggio 2018 e comunicano senza ritardo ogni successiva modifica.

Articolo 84

Sanzioni (C149, C152)

1. Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive.

2. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

CAPO IX
Disposizioni relative a specifiche situazioni di trattamento

Articolo 85

Trattamento e libertà d'espressione e di informazione (C153)

1. Il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria.

2. Ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono esenzioni o deroghe rispetto ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 2 e comunica senza ritardo ogni successiva modifica.

Articolo 86

Trattamento e accesso del pubblico ai documenti ufficiali (C154)

I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento.

Articolo 87

Trattamento del numero di identificazione nazionale

Gli Stati membri possono precisare ulteriormente le condizioni specifiche per il trattamento di un numero di identificazione nazionale o di qualsiasi altro mezzo d'identificazione d'uso generale. In tal caso, il numero di identificazione nazionale o qualsiasi altro mezzo d'identificazione d'uso generale sono utilizzati soltanto in presenza di garanzie adeguate per i diritti e le libertà dell'interessato conformemente al presente regolamento.

Articolo 88

Trattamento dei dati nell'ambito dei rapporti di lavoro (C155)

1. Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.

2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.

3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Articolo 89

Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (C33, C156-C163)

1. Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.

2. Se i dati personali sono trattati a fini di ricerca scientifica o storica o a fini statistici, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

3. Se i dati personali sono trattati per finalità di archiviazione nel pubblico interesse, il diritto dell'Unione o degli Stati membri può prevedere deroghe ai diritti di cui agli articoli 15, 16, 18, 19, 20 e 21, fatte salve le condizioni e le garanzie di cui al paragrafo 1 del presente articolo, nella misura in cui tali diritti rischiano di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità specifiche e tali deroghe sono necessarie al conseguimento di dette finalità.

4. Qualora il trattamento di cui ai paragrafi 2 e 3 funga allo stesso tempo a un altro scopo, le deroghe si applicano solo al trattamento per le finalità di cui ai medesimi paragrafi.

Articolo 90

Obblighi di segretezza (C164)

1. Gli Stati membri possono adottare norme specifiche per stabilire i poteri delle autorità di controllo di cui all'articolo 58, paragrafo 1, lettere e) e f), in relazione ai titolari del trattamen-

to o ai responsabili del trattamento che sono soggetti, ai sensi del diritto dell'Unione o degli Stati membri o di norme stabilite dagli organismi nazionali competenti, al segreto professionale o a un obbligo di segretezza equivalente, ove siano necessarie e proporzionate per conciliare il diritto alla protezione dei dati personali e l'obbligo di segretezza. Tali norme si applicano solo ai dati personali che il titolare del trattamento o il responsabile del trattamento ha ricevuto o ha ottenuto in seguito a un'attività protetta da tale segreto professionale.

2. Ogni Stato membro notifica alla Commissione le norme adottate ai sensi del paragrafo 1 al più tardi entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica.

Articolo 91

Norme di protezione dei dati vigenti presso chiese e associazioni religiose (C165)

1. Qualora in uno Stato membro chiese e associazioni o comunità religiose applichino, al momento dell'entrata in vigore del presente regolamento, corpus completi di norme a tutela delle persone fisiche con riguardo al trattamento, tali corpus possono continuare ad applicarsi purché siano resi conformi al presente regolamento.

2. Le chiese e le associazioni religiose che applicano i corpus completi di norme di cui al paragrafo 1 del presente articolo sono soggette al controllo di un'autorità di controllo indipendente che può essere specifica, purché soddisfi le condizioni di cui al capo VI del presente regolamento.

CAPO X
Atti delegati e atti di esecuzione

Articolo 92

Esercizio della delega (C166)

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. La delega di potere di cui all'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, è conferita alla Commissione per un periodo indeterminato a decorrere 24 maggio 2016.

3. La delega di potere di cui all'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella Gazzetta ufficiale dell'Unione europea o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

5. L'atto delegato adottato ai sensi dell'articolo 12, paragrafo 8, e all'articolo 43, paragrafo 8, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di tre mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di tre mesi su iniziativa del Parlamento europeo o del Consiglio.

Articolo 93

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

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

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

CAPO XI
Disposizioni finali

Articolo 94

Abrogazione della direttiva 95/46/CE (C171)

1. La direttiva 95/46/CE è abrogata a decorrere da 25 maggio 2018.

2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento.

Articolo 95

Rapporto con la direttiva 2002/58/CE (C173)

Il presente regolamento non impone obblighi supplementari alle persone fisiche o giuridiche in relazione al trattamento nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione nell'Unione, per quanto riguarda le materie per le quali sono soggette a obblighi specifici aventi lo stesso obiettivo fissati dalla direttiva 2002/58/CE.

Articolo 96

Rapporto con accordi precedentemente conclusi (C102)

Restano in vigore, fino alla loro modifica, sostituzione o revoca, gli accordi internazionali che comportano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali conclusi dagli Stati membri prima di 24 maggio 2016 e conformi al diritto dell'Unione applicabile prima di tale data.

Articolo 97

Relazioni della Commissione

1. Entro 25 maggio 2020 e, successivamente, ogni quattro anni, la Commissione trasmette al Parlamento europeo e al Consiglio relazioni di valutazione e sul riesame del presente regolamento.

2. Nel contesto delle valutazioni e del riesame del presente regolamento di cui al paragrafo 1, la Commissione esamina, in particolare, l'applicazione e il funzionamento:

a) del capo V sul trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, con particolare riguardo alle decisioni adottate ai sensi dell'articolo 45, paragrafo 3, del presente regolamento, e alle decisioni adottate sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46/CE;

b) del capo VII su cooperazione e coerenza.

3. Ai fini del paragrafo 1, la Commissione può richiedere informazioni agli Stati membri e alle autorità di controllo.

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

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

Articolo 98

Riesame di altri atti legislativi dell'Unione in materia di protezione dei dati

Se del caso, la Commissione presenta proposte legislative di modifica di altri atti legislativi dell'Unione in materia di protezione dei dati personali, allo scopo di garantire una protezione uniforme e coerente delle persone fisiche con riguardo al trattamento. Ciò riguarda in particolare le norme relative alla protezione delle persone fisiche con riguardo

al trattamento da parte di istituzioni, organi, uffici e agenzie dell'Unione e le norme sulla libera circolazione di tali dati.

Articolo 99

Entrata in vigore e applicazione

1. Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

2. Esso si applica a decorrere da 25 maggio 2018.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 27 aprile 2016

Per il Parlamento europeo

Il presidente

M. SCHULZ

Per il Consiglio

Il presidente

J.A. HENNIS-PLASSCHAERT

([1]) GU C 229 del 31.7.2012, pag. 90.

([2]) GU C 391 del 18.12.2012, pag. 127.

([3]) Posizione del Parlamento europeo del 12 marzo 2014 (non ancora pubblicata nella Gazzetta ufficiale) e posizione del Consiglio in prima lettura dell'8 aprile 2016 (non ancora pubblicata nella Gazzetta ufficiale). Posizione del Parlamento europeo del 14 aprile 2016.

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

([5]) Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (C(2003) 1422) (GU L 124 del 20.5.2003, pag. 36).

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

([7]) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (Cfr. pagina 89 della presente Gazzetta ufficiale).

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

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

([10]) Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori (GU L 95 del 21.4.1993, pag. 29).

([11]) Regolamento (CE) n. 1338/2008 del Parlamento europeo e del Consiglio, del 16 dicembre 2008, relativo alle statistiche comunitarie in materia di sanità pubblica e di salute e sicurezza sul luogo di lavoro (GU L 354 del 31.12.2008, pag. 70).

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

([13]) Regolamento (UE) n. 1215/2012 del Parlamento europeo e del Consiglio, del 12 dicembre 2012, concernente la competenza giurisdizionale, il riconoscimento e l'esecuzione delle decisioni in materia civile e commerciale (GU L 351 del 20.12.2012, pag. 1).

([14]) Direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico (GU L 345 del 31.12.2003, pag. 90).

([15]) Regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano e che abroga la direttiva 2001/20/CE (GU L 158 del 27.5.2014, pag. 1).

([16]) Regolamento (CE) n. 223/2009 del Parlamento europeo e del Consiglio, dell'11 marzo 2009, relativo alle statistiche europee e che abroga il regolamento (CE, Euratom) n. 1101/2008 del Parlamento europeo e del Consiglio, relativo alla trasmissione all'Istituto statistico delle Comunità europee di dati statistici protetti dal segreto, il regolamento (CE) n. 322/97 del Consiglio, relativo alle statistiche comunitarie, e la decisione 89/382/CEE, Euratom del Consiglio, che istituisce un comitato del programma statistico delle Comunità europee (GU L 87 del 31.3.2009, pag. 164).

([17]) GU C 192 del 30.6.2012, pag. 7.

([18]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

([19]) Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche delle regole relative ai servizi della società dell'informazione (GU L 241 del 17.9.2015, pag. 1).

([20]) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

([21]) Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione (GU L 145 del 31.5.2001, pag. 43).

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 69677.1
e-mail: garante@gpdp.it
www.garanteprivacy.it

A cura del **Servizio relazioni esterne e media**

Stampa:
UGO QUINTILY S.p.A.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GUIDA ALL'APPLICAZIONE DEL

REGOLAMENTO EUROPEO

IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

EDIZIONE AGGIORNATA **FEBBRAIO 2018**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Indice

Introduzione

La Guida intende offrire un panorama delle principali problematiche che imprese e soggetti pubblici dovranno tenere presenti in vista della piena applicazione del regolamento, prevista il 25 maggio 2018.

Attraverso raccomandazioni specifiche vengono suggerite alcune azioni che possono essere intraprese sin d'ora perché fondate su disposizioni precise del regolamento che non lasciano spazi a interventi del legislatore nazionale (come invece avviene per altre norme del regolamento, in particolare quelle che disciplinano i trattamenti per finalità di interesse pubblico ovvero in ottemperanza a obblighi di legge).

Vengono, inoltre, segnalate alcune delle principali novità introdotte dal regolamento rispetto alle quali sono suggeriti possibili approcci.

La presente Guida è soggetta a integrazioni e modifiche alla luce dell'evoluzione della riflessione a livello nazionale ed europeo

Fondamenti di liceità del trattamento

Il regolamento conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; **i fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003** (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

In particolare:

Consenso

COSA CAMBIA

- Per i dati "sensibili" (si veda art. 9 regolamento) il consenso **deve** essere "esplicito"; lo stesso dicasi per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – art. 22). Si segnalano, al riguardo, le linee-guida in materia di profilazione e decisioni automatizzate del Gruppo "Articolo 29" (WP 251), qui disponibili: www.garanteprivacy.it/regolamentoue/profilazione.

- **Non** deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare l'inequivocabilità del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il titolare (art. 7.1) **deve** essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento.

- **Il consenso dei minori** è valido **a partire dai 16 anni** (il limite di età può essere abbassato fino a 13 anni dalla normativa nazionale); prima di tale età occorre raccogliere il consenso dei genitori o di chi ne fa le veci.

COSA NON CAMBIA

- **Deve** essere, in tutti i casi, libero, specifico, informato e inequivocabile e **non** è ammesso il consenso tacito o presunto (no a caselle pre-spuntate su un modulo).

- **Deve** essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Raccomandazioni

Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica.
In particolare, occorre verificare che la richiesta di consenso sia **chiaramente distinguibile** da altre richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di modulistica. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20).

Interesse vitale di un terzo

COSA CAMBIA

- Si può invocare tale base giuridica **solo** se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46).

Interesse legittimo prevalente di un titolare o di un terzo

COSA CAMBIA

- Il **bilanciamento** fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato **non spetta** all'Autorità ma **è compito dello stesso titolare**; si tratta di una delle principali espressioni del principio di "responsabilizzazione" introdotto dal nuovo pacchetto protezione dati.

COSA NON CAMBIA

- L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità.
- Il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

Raccomandazioni

Il regolamento offre alcuni criteri per il bilanciamento in questione (si veda considerando 47) e soprattutto appare utile fare riferimento al documento pubblicato dal Gruppo "Articolo 29" sul punto (WP217).

Si confermano, inoltre, nella sostanza, i requisiti indicati dall'Autorità nei propri provvedimenti in materia di bilanciamento di interessi (si veda, per esempio, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680 con riguardo all'utilizzo della video-sorveglianza; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6068256 in merito all'utilizzo di sistemi di rilevazione informatica anti-frode; ecc.) con particolare riferimento agli esiti delle verifiche preliminari condotte dall'Autorità, con eccezione ovviamente delle disposizioni che il regolamento ha espressamente abrogato (per esempio: obbligo di notifica dei trattamenti). I titolari dovrebbero condurre la propria valutazione alla luce di tutti questi principi.

Informativa

Contenuti dell'informativa

COSA CAMBIA

- I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento e in parte sono più ampi rispetto al Codice. In particolare, il titolare **deve sempre** specificare **i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer)**, ove esistente, la **base giuridica** del trattamento, **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento, nonché **se trasferisce i dati personali in Paesi terzi** e, in caso affermativo, **attraverso quali strumenti** (esempio: si tratta di un Paese terzo giudicato adeguato dalla Commissione europea; si utilizzano BCR di gruppo; sono state inserite specifiche clausole contrattuali modello, ecc.).
- Il regolamento prevede anche **ulteriori informazioni** in quanto "necessarie per garantire un trattamento corretto e trasparente": in particolare, il titolare deve specificare il **periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di **presentare un reclamo** all'autorità di controllo.
- Se il trattamento comporta processi decisionali automatizzati (anche la **profilazione**), l'informativa deve specificarlo e deve indicare anche la **logica** di tali processi decisionali e le conseguenze previste per l'interessato.

Tempi dell'informativa

COSA CAMBIA

- Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve essere fornita **entro un termine ragionevole che non può superare 1 mese** dalla raccolta, oppure **al momento della comunicazione** (**non** della registrazione) dei dati (a terzi o all'interessato) (diversamente da quanto prevede attualmente l'art. 13, comma 4, del Codice).

Modalità dell'informativa

COSA CAMBIA

- Il regolamento specifica molto più in dettaglio rispetto al Codice le caratteristiche dell'informativa, che deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice**, e per i minori occorre prevedere informative idonee (si veda anche considerando 58).
- L'informativa è data, **in linea di principio, per iscritto e preferibilmente in formato elettronico** (soprattutto nel contesto di servizi online: si vedano art. 12, paragrafo 1, e considerando 58), anche se sono ammessi "altri mezzi", quindi può essere fornita anche oralmente, ma nel rispetto delle caratteristiche di cui sopra (art. 12, paragrafo 1). Il regolamento ammette, soprattutto, l'utilizzo di **icone** per presentare i contenuti dell'informativa in forma sintetica, **ma solo "in combinazione" con l'informativa estesa** (art. 12, paragrafo 7); queste icone dovranno essere identiche in tutta l'Ue e saranno definite prossimamente dalla Commissione europea.
- Sono inoltre **parzialmente diversi i requisiti che il regolamento fissa per l'esonero dall'informativa** (si veda art. 13, paragrafo 4 e art. 14, paragrafo 5 del regolamento, oltre a quanto previsto dall'articolo 23, paragrafo 1, di quest'ultimo), anche se occorre sottolineare che **spetta al titolare**,

COSA NON CAMBIA

in caso di dati personali raccolti da fonti diverse dall'interessato, **valutare se la prestazione dell'informativa agli interessati comporti uno sforzo sproporzionato** (si veda art. 14, paragrafo 5, lettera b)) – a differenza di quanto prevede l'art. 13, comma 5, lettera c) del Codice.

- L'informativa (disciplinata nello specifico dagli artt. 13 e 14 del regolamento) deve essere fornita all'interessato **prima di effettuare la raccolta dei dati** (se raccolti direttamente presso l'interessato – art. 13 del regolamento). Se i dati non sono raccolti direttamente presso l'interessato (art. 14 del regolamento), l'informativa deve comprendere anche le **categorie** dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare **la propria identità e quella dell'eventuale rappresentante nel territorio italiano, le finalità del trattamento, i diritti degli interessati** (compreso il diritto alla portabilità dei dati), se esiste un **responsabile del trattamento e la sua identità, e quali sono i destinatari dei dati**.

NOTA: ogni volta che le finalità cambiano il regolamento impone di informarne l'interessato prima di procedere al trattamento ulteriore.

Raccomandazioni

È opportuno che i titolari di trattamento **verifichino la rispondenza delle informative** attualmente utilizzate a tutti i criteri sopra delineati, con particolare riguardo ai **contenuti obbligatori** e alle **modalità di redazione**, in modo da apportare le modifiche o le integrazioni eventualmente necessarie ai sensi del regolamento.

Il regolamento supporta chiaramente il concetto di **informativa "stratificata"**, più volte esplicitato dal Garante nei suoi provvedimenti (si veda http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1712680

relativo all'utilizzo di un'icona specifica per i sistemi di videosorveglianza con o senza operatore; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1246675 contenente prescrizioni analoghe rispetto all'utilizzo associato di sistemi biometrici e di videosorveglianza in istituti bancari), in particolare attraverso l'impiego di icone associate (in vario modo) a contenuti più estesi, che devono essere facilmente accessibili, e promuove **l'utilizzo di strumenti elettronici** per garantire la massima diffusione e semplificare la prestazione delle informative.

I titolari potranno, dunque, una volta adeguata l'informativa nei termini sopra indicati, **continuare o iniziare a utilizzare queste modalità** per la prestazione dell' informativa, comprese le icone che l'Autorità ha in questi anni suggerito nei suoi provvedimenti (videosorveglianza, banche, ecc.) – in attesa della definizione di icone standardizzate da parte della Commissione.
Dovranno essere adottate anche le **misure organizzative interne** idonee a garantire il rispetto della tempistica: il termine di 1 mese per l'informativa all'interessato è chiaramente un termine massimo, e occorre ricordare che l'art. 14, paragrafo 3, lettera a), del regolamento menziona in primo luogo che il **termine deve essere "ragionevole"**.

Poiché spetterà al titolare valutare lo **sforzo sproporzionato** richiesto dall'informare una pluralità di interessati, qualora i dati non siano stati raccolti presso questi ultimi, e salva l'esistenza di specifiche disposizioni normative nei termini di cui all'art. 23, paragrafo 1, del regolamento, sarà utile fare riferimento ai **criteri evidenziati nei provvedimenti** con cui il Garante ha riconosciuto negli anni l'esistenza di tale sproporzione (si veda, in particolare, il provvedimento del 26 novembre 1998 – http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39624; più di recente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3864423 in tema di esonero dagli obblighi di informativa).

Diritti degli interessati

Modalità per l'esercizio dei diritti

Le modalità per l'esercizio di tutti i diritti da parte degli interessati sono stabilite, in via generale, negli artt. 11 e 12 del regolamento.

COSA CAMBIA

- **Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso), 1 mese,** estendibile fino a 3 mesi in casi di particolare complessità; **il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego**.

- **Spetta al titolare** valutare la complessità del riscontro all'interessato e **stabilire l'ammontare dell'eventuale contributo** da chiedere all'interessato, ma soltanto se si tratta di richieste **manifestamente infondate o eccessive** (anche ripetitive) (art.12, paragrafo 5), a differenza di quanto prevedono gli art. 9, comma 5, e 10, commi 7 e 8, del Codice, ovvero se sono chieste **più "copie" dei dati personali** nel caso del diritto di accesso (art. 15, paragrafo 3); in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il **riscontro all'interessato** di regola deve avvenire in **forma scritta** anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato **oralmente solo se così richiede l'interessato** stesso (art. 12, paragrafo 1; si veda anche art. 15, paragrafo 3).

- La risposta fornita all'interessato non deve essere solo "intelligibile", ma anche **concisa**, **trasparente e facilmente accessibile**, oltre a utilizzare un **linguaggio semplice e chiaro**.

COSA NON CAMBIA

- **Il titolare del trattamento deve agevolare l'esercizio dei diritti** da parte dell'interessato, adottando ogni misura (tecnica e organizzativa) a ciò idonea. **Benché sia il solo titolare a dover dare riscontro** in caso di esercizio dei diritti (art. 15-22), il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)).

- **L'esercizio dei diritti è, in linea di principio, gratuito** per l'interessato, ma possono esservi eccezioni (si veda il paragrafo "Cosa cambia"). Il titolare ha il diritto di chiedere informazioni necessarie a identificare l'interessato, e quest'ultimo ha il dovere di fornirle, secondo modalità idonee (si vedano, in particolare, art. 11, paragrafo 2 e art. 12, paragrafo 6).

- Sono ammesse **deroghe ai diritti** riconosciuti dal regolamento, ma solo sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 nonché di altri articoli relativi ad ambiti specifici (si vedano, in particolare, art. 17, paragrafo 3, per quanto riguarda il diritto alla cancellazione/"oblio", art. 83 - trattamenti di natura giornalistica e art. 89 - trattamenti per finalità di ricerca scientifica o storica o di statistica).

Raccomandazioni

È opportuno che i titolari di trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza di quanto attualmente previsto – dovrà avere per impostazione predefinita forma scritta (anche elettronica). Potranno risultare utili le indicazioni fornite dal Garante nel corso degli anni con riguardo all'intelligibilità del riscontro fornito agli interessati e alla completezza del riscontro stesso (si vedano varie decisioni relative a ricorsi contenute nel Bollettino dell'Autorità pubblicato qui: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/766652, e più recentemente, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1449401 in materia di dati sanitari, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1290018 in materia di dati telematici).

Quanto alla definizione eventuale di un contributo spese da parte degli interessati, che il regolamento rimette al titolare del trattamento, l'Autorità intende valutare l'opportunità di definire linee-guida specifiche (anche sul fondamento delle determinazioni assunte sul punto nel corso degli anni: si veda in particolare la Deliberazione n. 14 del 23 dicembre 2004 - http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1104892), di concerto con le altre autorità Ue, alla luce di quanto prevede l'art. 70 del regolamento con riguardo ai compiti del Board.

Diritto di accesso (art. 15)

COSA CAMBIA

- Il diritto di accesso prevede **in ogni caso** il diritto di ricevere **una copia dei dati** personali oggetto di trattamento.

- Fra le informazioni che il titolare deve fornire **non rientrano le "modalità" del trattamento**, mentre **occorre indicare il periodo di conservazione** previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le **garanzie** applicate **in caso di trasferimento dei dati verso Paesi terzi**.

Raccomandazioni

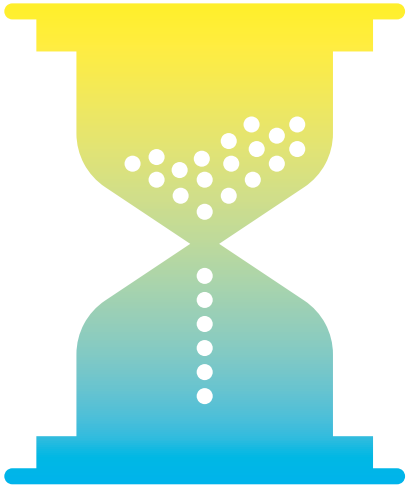
Oltre al rispetto delle prescrizioni relative alla modalità di esercizio di questo e degli altri diritti (si veda "Modalità per l'esercizio dei diritti"), i titolari possono **consentire agli interessati di consultare direttamente, da remoto** e in modo sicuro, i propri dati personali (si veda considerando 68).

Diritto di cancellazione (diritto all'oblio) (art.17)

COSA CAMBIA

- Il diritto cosiddetto "all'oblio" si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) **di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati**, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2).

- Ha **un campo di applicazione più esteso** di quello di cui all'art. 7, comma 3, lettera b), del Codice, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento (si veda art. 17, paragrafo 1).



Diritto di limitazione del trattamento (art. 18)

COSA CAMBIA

- Si tratta di un diritto **diverso e più esteso rispetto al "blocco" del trattamento** di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile **non solo in caso di violazione** dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche **se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica da parte del titolare) o si oppone al loro trattamento** ai sensi dell'art. 21 del regolamento (in attesa della valutazione da parte del titolare).

- Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Raccomandazioni

Il diritto alla limitazione prevede che **il dato personale sia "contrassegnato"** in attesa di determinazioni ulteriori; pertanto, è opportuno che i titolari prevedano nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

Diritto alla portabilità dei dati (art. 20)

COSA CAMBIA

- Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

- **Non si applica ai trattamenti non automatizzati** (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili **solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato** (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati **"forniti" dall'interessato** al titolare (si veda il considerando 68 per maggiori dettagli).

- Inoltre, il titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

Raccomandazioni

Il Gruppo "Articolo 29" ha pubblicato recentemente linee-guida specifiche dove sono illustrati e spiegati i requisiti e le caratteristiche del diritto alla portabilità con particolare riguardo ai diritti di terzi interessati i cui dati siano potenzialmente compresi fra quelli "relativi all'interessato" di cui quest'ultimo chiede la portabilità (versione italiana con le relative FAQ qui disponibile: www.garanteprivacy.it/regolamentoue/portabilita).

Al riguardo, si ricordano i numerosi **provvedimenti con cui l'Autorità ha indicato criteri per il bilanciamento** fra i diritti e le libertà fondamentali di terzi e quelli degli interessati esercitanti i diritti di cui all'art. 7 del Codice (si vedano, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3251012 e, con riguardo all'attività bancaria in generale, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1457247).
Poiché la trasmissione dei dati da un titolare all'altro prevede che si utilizzino formati interoperabili, i titolari che ricadono nel campo di applicazione di questo diritto dovrebbero adottare sin da ora le misure necessarie a produrre i dati richiesti in un **formato interoperabile** secondo le indicazioni fornite nel considerando 68 e nelle linee-guida del Gruppo "Articolo 29".

Titolare, responsabile, incaricato del trattamento

COSA CAMBIA

Il regolamento:

- disciplina la **contitolarità del trattamento** (art. 26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido ai sensi del diritto nazionale) il rispettivo ambito di responsabilità e i compiti **con particolare riguardo all'esercizio dei diritti degli interessati**, che hanno comunque la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

- fissa più dettagliatamente (rispetto al Codice) le **caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento** attribuendogli specifici compiti: deve trattarsi, infatti, di un **contratto** (o altro atto giuridico conforme al diritto nazionale) e deve **disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art. 28** al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento, le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento;

- consente la **nomina di sub-responsabili del trattamento** da parte di un responsabile (si veda art. 28, paragrafo 4), per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario; quest'ultimo **risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile**, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo

dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (si veda art. 82, paragrafo 1 e paragrafo 3);

- prevede **obblighi specifici in capo ai responsabili del trattamento**, in quanto distinti da quelli pertinenti ai rispettivi titolari. Ciò riguarda, in particolare, la tenuta del **registro dei trattamenti** svolti (ex art. 30, paragrafo 2); l'adozione di idonee **misure tecniche e organizzative per garantire la sicurezza** dei trattamenti (ex art. 32 regolamento); **la designazione di un RPD-DPO** (si segnalano, al riguardo, le linee-guida in materia di responsabili della protezione dei dati recentemente adottate dal Gruppo "Articolo 29", qui disponibili: www.garante-privacy.it/regolamentoue/rpd), nei casi previsti dal regolamento o dal diritto nazionale (si veda art. 37 del regolamento). Si ricorda, inoltre, che **anche il responsabile** non stabilito nell'Ue dovrà **designare un rappresentante in Italia** quando ricorrono le condizioni di cui all'art. 27, paragrafo 3, del regolamento – diversamente da quanto prevedeva l'art. 5, comma 2, del Codice.

COSA NON CAMBIA

- Il regolamento definisce **caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento** negli stessi termini di cui alla direttiva 95/46/CE e, quindi, al Codice italiano. Pur non prevedendo espressamente la **figura dell' "incaricato" del trattamento** (ex art. 30 Codice), il regolamento **non ne esclude** la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (si veda, in particolare, art. 4, n. 10, del regolamento).

Raccomandazioni

I titolari di trattamento dovrebbero valutare attentamente l'esistenza di eventuali situazioni di contitolarità (si vedano, in proposito, le indicazioni fornite dal Garante in vari provvedimenti, fra cui http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/39785), essendo obbligati in tal caso a stipulare l'accordo interno di cui parla l'art. 26, paragrafo 1, del regolamento. Sarà necessario, in particolare, individuare il "punto di contatto per gli interessati" previsto dal suddetto articolo ai fini dell'esercizio dei diritti previsti dal regolamento.

I titolari di trattamento dovrebbero verificare che i contratti o altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto, in particolare, dall'art. 28, paragrafo 3, del regolamento. Dovranno essere apportate le necessarie integrazioni o modifiche, in particolare qualora si intendano designare sub-responsabili nei termini sopra descritti. La Commissione e le autorità nazionali di controllo (fra cui il Garante) stanno valutando la definizione di clausole contrattuali modello da utilizzare a questo scopo.

Attraverso l'adesione a codici deontologici ovvero l'adesione a schemi di certificazione il responsabile può dimostrare le "garanzie sufficienti" di cui all'art. 28, paragrafi 1 e 4. Il Garante sta valutando i codici deontologici attualmente vigenti per alcune tipologie di trattamento nell'ottica dei requisiti fissati nel regolamento (art. 40), mentre per quanto concerne gli schemi di certificazione occorrerà attendere anche l'intervento del legislatore nazionale che dovrà stabilire alcune modalità di accreditamento dei soggetti certificatori (se diversi dal Garante: si veda art. 43).
In ogni caso, il Gruppo "Articolo 29" sta lavorando sui temi e sarà opportuno tenere conto degli sviluppi che interverranno in materia nei prossimi mesi.

Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene che titolari e responsabili del trattamento possano mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante (si veda art. 30 del Codice e, fra molti, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1507921, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1508059 per quanto riguarda la pubblica amministrazione, ovvero http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953 in materia di tracciamento delle attività bancarie) in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al regolamento (si veda art. 24, paragrafo 1, del regolamento).

Approccio basato sul rischio e misure di accountability di titolari e responsabili

COSA CAMBIA

- Il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull' **adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento** (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

- Il primo fra tali criteri è sintetizzato dall'espressione inglese **"data protection by default and by design"** (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che **devono sostanziarsi in una serie di attività specifiche e dimostrabili.**

- Fondamentali fra tali attività sono quelle connesse al secondo criterio individuato nel regolamento rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**. Quest'ultimo è da intendersi come rischio

di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi (si segnalano, al riguardo, le linee-guida in materia di valutazione di impatto sulla protezione dei dati del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/regolamentoue/DPIA). All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

- Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega **l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano**, come la **notifica preventiva dei trattamenti** all'autorità di controllo e il cosiddetto **prior checking** (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia con eventuale successiva consultazione dell'Autorità, tranne alcune specifiche situazioni di trattamento (vedi art. 36, paragrafo 5 del regolamento). Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamenta-

le al fine di garantire uniformità di approccio e fornire ausili interpretativi e analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

Nei paragrafi seguenti si richiamano **alcune delle principali novità** in termini di adempimenti da parte di titolari e responsabili del trattamento.

Registro dei trattamenti

COSA CAMBIA

- Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30. Si tratta di uno **strumento fondamentale** non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – **indispensabile per ogni valutazione e analisi del rischio**. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Raccomandazioni

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì **parte integrante di un sistema di corretta gestione dei dati personali**. Per tale motivo, si invitano tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata rico-

gnizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta. I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo si riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

Misure di sicurezza

COSA CAMBIA

- Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (art. 32, paragrafo 1); in questo senso, **la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva** ("tra le altre, se del caso"). Per lo stesso motivo, **non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza** (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento. Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate. Tuttavia, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Notifica delle violazioni di dati personali

COSA CAMBIA

- A partire dal 25 maggio 2018, **tutti i titolari** – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, **entro 72 ore** e comunque "senza ingiustificato ritardo", ma **soltanto se ritengono probabile che da tale violazione derivino rischi** per i diritti e le libertà degli interessati (si veda considerando 85). Pertanto, **la notifica all'Autorità** dell'avvenuta violazione **non è obbligatoria**, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'art. 34, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. **I contenuti della notifica** all'Autorità e della comunicazione agli interessati sono indicati, **in via non esclusiva, agli art. 33 e 34 del regolamento.** Si segnalano, al riguardo, le linee-guida in materia di notifica delle violazioni di dati personali del Gruppo "Articolo 29", qui disponibili: www.garanteprivacy.it/regolamentoue/databreach.

Raccomandazioni

Tutti i titolari di trattamento dovranno in ogni caso **documentare le violazioni** di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze e conseguenze e i provvedimenti adottati (si veda art. 33, paragrafo 5); tale obbligo non è diverso, nella sostanza, da quello attualmente previsto dall'art. 32-bis, comma 7, del Codice. Si raccomanda, pertanto, ai titolari di trattamento di adottare le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuti a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Responsabile della protezione dei dati

COSA CAMBIA

- Anche la designazione di un "responsabile della protezione dati" (RPD, ovvero DPO se si utilizza l'acronimo inglese: Data Protection Officer) riflette l'approccio responsabilizzante che è proprio del regolamento (si veda art. 39), essendo finalizzata a facilitare l'attuazione del regolamento da parte del titolare/responsabile. Non è un caso, infatti, che fra i compiti del RPD rientrino "la sensibilizzazione e la formazione del personale" e la sorveglianza sullo svolgimento della valutazione di impatto di cui all'art. 35. La sua designazione è obbligatoria in alcuni casi (si veda art. 37), e il regolamento tratteggia le caratteristiche soggettive e oggettive di questa figura (indipendenza, autorevolezza, competenze manageriali: si vedano art. 38 e 39) in termini che Gruppo "Articolo 29" ha ritenuto opportuno chiarire attraverso alcune linee-guida di recente pubblicazione, disponibili anche sul sito del Garante, e alle quali si rinvia per maggiori delucidazioni unitamente alle relative FAQ (si veda: www.garanteprivacy.it/regolamentoue/rpd).

Trasferimenti di dati verso Paesi terzi e organismi internazionali

COSA CAMBIA

- In primo luogo, **viene meno il requisito dell'autorizzazione nazionale** (si vedano art. 45, paragrafo 1, e art. 46, paragrafo 2). Ciò significa che il trasferimento verso un Paese terzo "adeguato" ai sensi della decisione assunta in futuro dalla Commissione, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del regolamento, potrà avere inizio senza attendere l'autorizzazione nazionale del Garante - a differenza di quanto attualmente previsto dall'art. 44 del Codice.
  Tuttavia, **l'autorizzazione del Garante sarà ancora necessaria** se un titolare desidera utilizzare **clausole contrattuali ad-hoc** (cioè non riconosciute come adeguate tramite decisione della Commissione europea) oppure **accordi amministrativi** stipulati tra autorità pubbliche – una delle novità introdotte dal regolamento.

- Il regolamento consente di ricorrere anche a **codici di condotta ovvero a schemi di certificazione** per dimostrare le "garanzie adeguate" previste dall'art. 46. Ciò significa che **i titolari o i responsabili del trattamento stabiliti in un Paese terzo potranno far valere gli impegni sottoscritti attraverso l'adesione al codice di condotta o allo schema di certificazione**, ove questi disciplinino anche o esclusivamente i trasferimenti di dati verso Paesi terzi, al fine di legittimare tali trasferimenti. **Tuttavia** (si vedano art. 40, paragrafo 3, e art. 42, paragrafo 2), tali titolari dovranno assumere, inoltre, **un impegno vincolante mediante uno specifico strumento contrattuale o un altro strumento** che sia giuridicamente vincolante e azionabile dagli interessati.

- Il regolamento vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di **decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo**, a meno dell'esistenza di accordi internazionali in particolare di mutua assistenza giudiziaria o analoghi accordi fra gli Stati (si veda art. 48). Si potranno utilizzare, tuttavia, gli altri presupposti e in particolare le deroghe previste per situazioni specifiche di cui all'art. 49. A tale riguardo, si deve ricordare che il regolamento chiarisce come sia lecito trasferire dati personali verso un Paese terzo non adeguato "per importanti motivi di interesse pubblico", in deroga al divieto generale, ma deve trattarsi di un **interesse pubblico riconosciuto dal diritto dello Stato membro** del titolare o dal diritto dell'Ue (si veda art. 49, paragrafo 4) – e dunque non può essere fatto valere l'interesse pubblico dello Stato terzo ricevente.

- Il regolamento **fissa i requisiti per l'approvazione delle norme vincolanti d'impresa e i contenuti obbligatori di tali norme**. L'elenco indicato al riguardo nel paragrafo 2 dell'art. 47 non è esaustivo e, pertanto, potranno essere previsti dalle autorità competenti, a seconda dei casi, requisiti ulteriori. Ad ogni modo, l'approvazione delle norme vincolanti d'impresa dovrà avvenire esclusivamente attraverso il meccanismo di coerenza di cui agli artt. 63-65 del regolamento – ossia, **è previsto in ogni caso l'intervento del Comitato europeo per la protezione dei dati** (si veda art. 64, paragrafo 1, lettera d)).

COSA NON CAMBIA

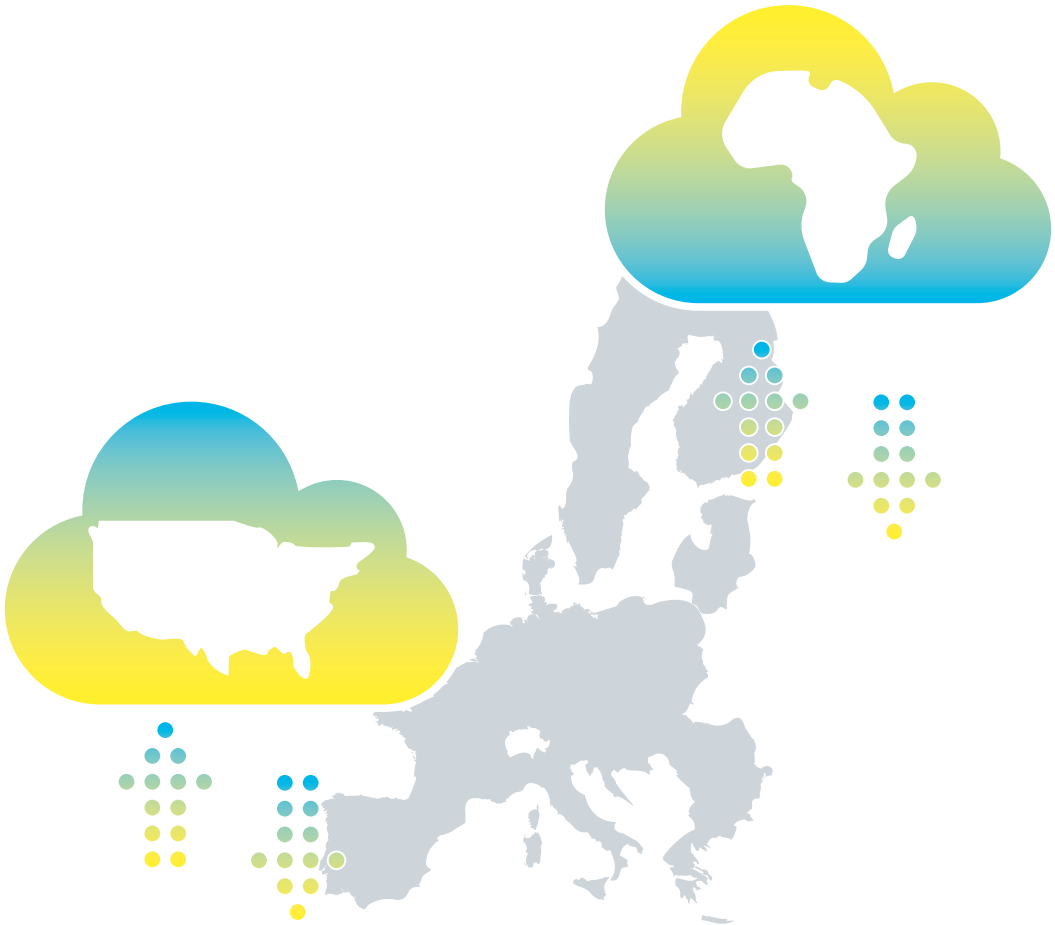
- **Il regolamento** (si veda Capo V) **ha confermato l'approccio attualmente vigente** per quanto riguarda i flussi di dati al di fuori dell'Unione europea e dello spazio economico europeo, prevedendo che tali flussi sono vietati, in linea di principio, a meno che intervengano specifiche garanzie che il regolamento elenca in ordine gerarchico:

  i. adeguatezza del Paese terzo riconosciuta tramite decisione della Commissione europea;

  ii. in assenza di decisioni di adeguatezza della Commissione, garanzie adeguate di natura contrattuale o pattizia che devono essere fornite dai titolari coinvolti (fra cui le norme vincolanti d'impresa - BCR, e clausole contrattuali modello);

  iii. in assenza di ogni altro presupposto, utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

- **Le decisioni di adeguatezza sinora adottate** dalla Commissione (livello di protezione dati in Paesi terzi, a partire dal Privacy Shield, e clausole contrattuali tipo per titolari e responsabili) e gli accordi internazionali in materia di trasferimento dati stipulati prima del 24 maggio 2016 dagli Stati membri restano in vigore fino a loro eventuale revisione o modifica (si vedano art. 45, paragrafo 9, e art. 96). Restano valide, conseguentemente, le autorizzazioni nazionali sinora emesse dal Garante successivamente a tali decisioni di adeguatezza della Commissione (si veda http://www.garanteprivacy.it/home/provvedimenti-normativa/normativa/normativa-comunitaria-e-intenazionale/trasferimento-dei-dati-verso-paesi-terzi#1). Restano valide, inoltre, le autorizzazioni nazionali che il Garante ha rilasciato in questi anni per specifici casi (si veda art. 46, paragrafo 5), sino a loro eventuale modifica.



Appendice

Linee guida sul regolamento gia' adottate dal gruppo di lavoro "Articolo 29" (WP29)

(Tutte le Linee guida sono disponibili sul sito internet del Garante www.garanteprivacy.it)

1. **Linee-guida sui responsabili della protezione dei dati (RPD) -** WP243
   Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016
   Comprende l'Allegato alle linee-guida sul RPD - Indicazioni essenziali

2. **Linee-guida sul diritto alla "portabilità dei dati"** - WP242
   Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016

3. **Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento** - WP244
   Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016

4. **Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679** - WP248
   Adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017

5. **Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative** - WP253
   Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017

6. **Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e profilazione** - WP251
   Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018

7. **Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification)** - WP250
   Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
Tel: +39-06-696771
Fax: +39-06-696773785
www.garanteprivacy.it

Per informazioni presso l'Autorità:
Ufficio per le relazioni con il pubblico
lunedì - venerdì ore 10.00 - 12.30
tel. 06 696772917
e-mail: urp@gpdp.it

Pubblicazione a cura
del Servizio relazioni esterne e media

Stampa: Ugo Quintily Spa - **Edizione aggiornata – febbraio 2018**

VERTIGO DESIGN

La privacy a scuola

DAI TABLET ALLA PAGELLA ELETTRONICA. LE REGOLE DA RICORDARE

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

La privacy a scuola

Garante per la protezione dei dati personali

Temi in classe

Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale.

Sta invece nella sensibilità dell'insegnante, nel momento in cui gli elaborati vengono letti in classe, trovare l'equilibrio tra esigenze didattiche e tutela della riservatezza, specialmente se si tratta di argomenti delicati.

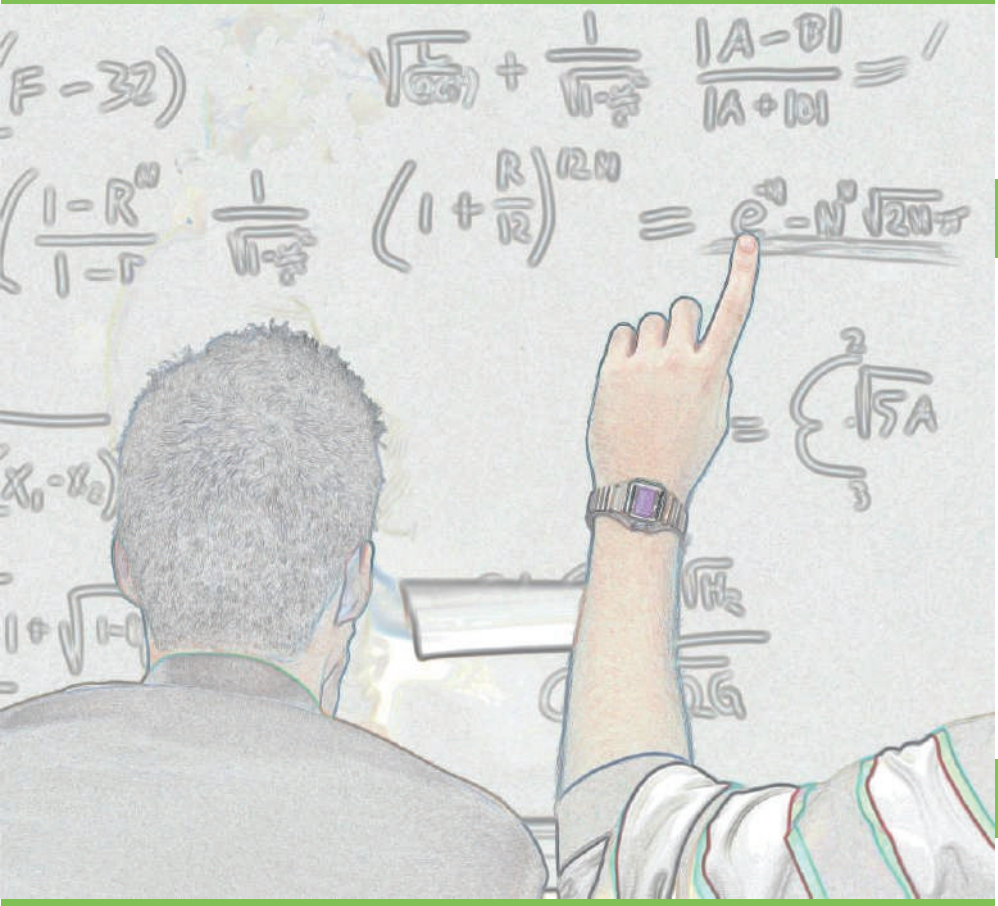
Cellulari e tablet

L'uso di cellulari e smartphone è in genere consentito per fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone.

Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. E' bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati.

Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line.

La privacy a scuola



Garante per la protezione dei dati personali

Recite e gite scolastiche

Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini in questi casi sono raccolte a fini personali e destinati ad un ambito familiare o amicale. Nel caso si intendesse pubblicarle e diffonderle in rete, anche sui social network, è necessario ottenere di regola il consenso delle persone presenti nei video o nelle foto.

Retta e servizio mensa

E' illecito pubblicare sul sito della scuola il nome e cognome degli studenti i cui genitori sono in ritardo nel pagamento della retta o del servizio mensa.
Lo stesso vale per gli studenti che usufruiscono gratuitamente del servizio mensa in quanto appartenenti a famiglie con reddito minimo o a fasce deboli. Gli avvisi messi on line devono avere carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale. A salvaguardia della trasparenza sulla gestione delle risorse scolastiche, restano ferme le regole sull'accesso ai documenti amministrativi da parte delle persone interessate.

Telecamere

Si possono in generale installare telecamere all'interno degli istituti scolastici, ma devono funzionare solo negli orari di chiusura degli istituti e la loro presenza deve essere segnalata con cartelli. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato. Le immagini registrare devono essere cancellate in generale dopo 24 ore.

La privacy a scuola

Garante per la protezione dei dati personali

Inserimento professionale

Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale le scuole, su richiesta degli studenti, possono comunicare e diffondere alle aziende private e alle pubbliche amministrazioni i dati personali dei ragazzi.

Questionari per attività di ricerca

L'attività di ricerca con la raccolta di informazioni personali tramite questionari da sottoporre agli studenti è consentita solo se ragazzi e genitori sono stati prima informati sugli scopi delle ricerca, le modalità del trattamento e le misure di sicurezza adottate.

Gli studenti e i genitori devono essere lasciati liberi di non aderire all'iniziativa.

Iscrizione e registri on line, pagella elettronica

In attesa di poter esprimere il previsto parere sui provvedimenti attuativi del Ministero dell'istruzione riguardo all'iscrizione on line degli studenti, all'adozione dei registri on line e alla consultazione della pagella via web, il Garante auspica l'adozione di adeguate misure di sicurezza a protezione dei dati.

La privacy a scuola

Garante per la protezione dei dati personali

Voti, scrutini, esami di Stato

I voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato sono pubblici.
Le informazioni sul rendimento scolastico sono soggette ad un regime di trasparenza e il regime della loro conoscibilità è stabilito dal Ministero dell'istruzione.

E' necessario però, nel pubblicare voti degli scrutini e degli esami nei tabelloni, che l'istituto eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti: il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap, ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.

Trattamento dei dati personali

Le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano.
Spesso le scuole utilizzano nella loro attività quotidiana dati delicati - come quelli riguardanti le origini etniche, le convinzioni religiose, lo stato di salute - anche per fornire semplici servizi, come ad esempio la mensa.

E' bene ricordare che nel trattare queste categorie di informazioni gli istituti scolastici devono porre estrema cautela, in conformità al regolamento sui dati sensibili adottato dal Ministero dell'istruzione.
Famiglie e studenti hanno diritto di conoscere quali informazioni sono trattate dall'istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

LA PRIVACY TRA I BANCHI DI SCUOLA

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

REGOLE GENERALI

VOTI ED ESAMI

INFORMAZIONI
SUGLI STUDENTI

FOTO, AUDIO E VIDEO

SICUREZZA E CONTROLLO

PAROLE CHIAVE

PER APPROFONDIRE

La privacy tra i banchi di scuola

La scuola è chiamata ogni giorno a costruire le condizioni per un futuro migliore delle nuove generazioni.
Non solo nello studio, ma anche nelle esperienze di vita che coinvolgono alunni, professori e personale scolastico si definisce il mondo dei valori che permette alla società di crescere nel rispetto reciproco.

Questa sfida positiva – nella scuola – riguarda anche il "corretto trattamento dei dati personali". Un'espressione che può sembrare asettica, ma che in realtà costituisce una condizione essenziale per il rispetto della dignità delle persone, della loro identità, del loro diritto alla riservatezza.

Nelle scuole, di ogni ordine e grado, vengono trattate giornalmente numerose informazioni sugli studenti e sulle loro famiglie, sui loro problemi sanitari o di disagio sociale, sulle abitudini alimentari. A volte può bastare una lettera contenente dati sensibili (quelli più delicati) su un minorenne, o un tabellone scolastico con riferimenti indiretti sulle condizioni di salute degli studenti, per violare anche involontariamente la riservatezza, la dignità di una persona. Al tempo stesso, "la privacy" è stata talvolta utilizzata in maniera impropria, per non rendere pubbliche determinate informazioni, come i risultati scolastici e quelli degli esami.

Il Garante ritiene utile sgombrare il campo da interpretazioni errate e fornire chiarimenti sulla corretta applicazione della normativa in materia di protezione dei dati personali. Anche allo scopo di sviluppare in ogni componente della comunità scolastica una sempre maggiore consapevolezza dei propri diritti e dei propri doveri.

Questa breve guida propone indicazioni generali tratte da provvedimenti, pareri e note del Garante in tema di privacy a scuola. Per facilitare un agile approfondimento dei vari temi, a conclusione del testo sono segnalati alcuni dei documenti che possono essere consultati sul sito Internet dell'Autorità.

Con il vademecum, il Garante intende offrire un contributo a favore di una comunità scolastica che possa promuovere il rispetto reciproco e tutelare il diritto degli studenti alla riservatezza.

REGOLE GENERALI

TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE PUBBLICHE

Le scuole hanno l'obbligo di far conoscere agli studenti e alle loro famiglie – se gli studenti sono minorenni – come usano i loro dati personali. Devono cioè rendere noto, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano. Le scuole pubbliche non sono tenute a chiedere il consenso per il trattamento dei dati personali degli studenti. Gli unici trattamenti permessi sono quelli necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore. Alcune categorie di dati personali degli studenti e delle famiglie – come quelli sensibili e giudiziari – devono essere trattate con estrema cautela, verificando prima non solo la pertinenza e completezza dei dati, ma anche la loro indispensabilità rispetto alle "rilevanti finalità pubbliche" che si intendono perseguire.

Ad esempio:

ORIGINI RAZZIALI ED ETNICHE

I dati sulle origini razziali ed etniche possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri.

CONVINZIONI RELIGIOSE

Gli istituti scolastici possono utilizzare i dati sulle convinzioni religiose al fine di garantire la libertà di credo – che potrebbe richiedere ad esempio misure particolari per la gestione della mensa scolastica – e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.

STATO DI SALUTE

I dati idonei a rivelare lo stato di salute possono essere trattati per l'assegnazione del sostegno agli alunni disabili; per la composizione delle classi; per la gestione delle assenze per malattia; per l'insegnamento domiciliare e ospedaliero nei confronti degli alunni affetti da gravi patologie; per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione.

CONVINZIONI POLITICHE

Le opinioni politiche possono essere trattate dalla scuola esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza: ad esempio, le consulte e le associazioni degli studenti e dei genitori.

DATI DI CARATTERE GIUDIZIARIO

I dati di carattere giudiziario possono essere trattati per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o di protezione. Il trattamento di dati sensibili e giudiziari è previsto anche per tutte le attività connesse ai contenziosi con gli alunni e con le famiglie (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.), e per tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche.

TRATTAMENTO DEI DATI NELLE ISTITUZIONI SCOLASTICHE PRIVATE

Per poter trattare i dati personali le scuole private sono obbligate non solo a presentare un'informativa completa, ma anche a ottenere il consenso puntuale e liberamente espresso dei soggetti interessati (studenti maggiorenni, famiglie...). Nel caso di trattamento di dati giudiziari e sensibili, gli istituti privati sono tenuti a rispettare anche le prescrizioni contenute nelle autorizzazioni generali del Garante, le quali esplicitano i trattamenti consentiti. È possibile, ad esempio, elaborare informazioni sulle convinzioni religiose degli studenti, al fine di permettere la scelta di avvalersi o meno dell'insegnamento della religione cattolica.

DIRITTO DI ACCESSO AI DATI PERSONALI

Anche in ambito scolastico, ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erronee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento" (la scuola) anche tramite suoi incaricati o responsabili. Se non si ottiene risposta, o se il riscontro non è sufficiente, è possibile rivolgersi alla magistratura ordinaria o al Garante.
A tale proposito, è opportuno precisare che l'accesso agli atti amministrativi non è regolato dal Codice della privacy, né vigilato dal Garante per la protezione dei dati personali. Come indicato nella legge n. 241 del 1990 (e successive modifiche) spetta alla singola amministrazione valutare se esistono i presupposti normativi che permettono di prendere visione e di estrarre copia di documenti amministrativi ai soggetti con un "interesse diretto, concreto e attuale" alla conoscibilità degli atti.

VOTI ED ESAMI

TEMI IN CLASSE

Non commette violazione della privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale o familiare.
Nel momento in cui gli elaborati vengono letti in classe - specialmente se sono presenti argomenti delicati - è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali.
Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d'ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

VOTI SCOLASTICI, SCRUTINI, TABELLONI, ESAMI DI STATO

Non esiste alcun provvedimento del Garante che imponga di tenere segreti i voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato, perché le informazioni sul rendimento scolastico sono soggette a un regime di trasparenza. Il regime attuale relativo alla conoscibilità dei risultati degli esami di maturità è stabilito dal Ministero dell'istruzione. Per il principio di trasparenza a garanzia di ciascuno, i voti degli scrutini e degli esami devono essere pubblicati nell'albo degli istituti. È necessario prestare attenzione, però, a non fornire – anche indirettamente – informazioni sulle condizioni di salute degli studenti, o altri dati personali non pertinenti. Ad esempio, il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap non va inserito nei tabelloni affissi all'albo dell'istituto, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.

INFORMAZIONI SUGLI STUDENTI

CIRCOLARI E COMUNICAZIONI SCOLASTICHE

Il diritto–dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere sempre bilanciato con l'esigenza di tutelare la personalità dei minori. È quindi necessario, ad esempio, evitare di inserire nelle comunicazioni scolastiche elementi che consentano di risalire, anche indirettamente, all'identità di minori coinvolti in vicende particolarmente delicate.

ORIENTAMENTO, FORMAZIONE E INSERIMENTO PROFESSIONALE

Su richiesta degli studenti interessati, le scuole possono comunicare, anche a privati e per via telematica, i dati relativi ai loro risultati scolastici per aiutarli nell'orientamento, la formazione e l'inserimento professionale anche all'estero.

MARKETING E PUBBLICITÀ

Non è possibile utilizzare i dati presenti nell'albo degli istituti scolastici per inviare materiale pubblicitario a casa degli studenti.
La conoscibilità a chiunque degli esiti scolastici (ad esempio attraverso il tabellone affisso nella scuola) risponde a essenziali esigenze di trasparenza.
Ciò non autorizza soggetti terzi a utilizzare i dati degli studenti per altre finalità come, ad esempio, il marketing e la promozione commerciale.

QUESTIONARI PER ATTIVITÀ DI RICERCA

Svolgere attività di ricerca con la raccolta di informazioni personali, spesso anche sensibili, tramite questionari da sottoporre agli alunni, è consentito soltanto se i ragazzi, o i genitori nel caso di minori, sono stati preventivamente informati sulle modalità di trattamento e conservazione dei dati raccolti e sulle misure di sicurezza adottate.
Gli intervistati, inoltre, devono sempre avere la facoltà di non aderire all'iniziativa.

FOTO, AUDIO E VIDEO

RECITE, GITE SCOLASTICHE E FOTO DI CLASSE

Non violano la privacy le riprese video e le fotografie raccolte dai genitori, durante le recite, le gite e i saggi scolastici. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione.
Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet, e sui social network in particolare.
In caso di comunicazione sistematica o diffusione diventa, infatti, necessario di regola ottenere il consenso delle persone presenti nelle fotografie e nei video.

REGISTRAZIONE DELLA LEZIONE

È possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti...), e ottenere il loro esplicito consenso.
Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire gli apparecchi in grado di registrare. (Vedi anche il paragrafo: "Videofonini, filmati, mms")

SICUREZZA E CONTROLLO

RILEVAMENTO DELLE PRESENZE CON DATI BIOMETRICI

L'utilizzo delle impronte digitali o di altri dati biometrici per rilevare la presenza di un gruppo di individui è giustificato soltanto dall'esistenza di reali esigenze di sicurezza, determinate da concrete e gravi situazioni di rischio. Il sistema di rilevamento delle impronte digitali, ad esempio, è stato giudicato sproporzionato rispetto all'obiettivo di consentire agli studenti l'accesso ai servizi di mensa universitaria.

VIDEOFONINI, FILMATI, MMS

L'utilizzo di videofonini, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per fini personali, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte, in particolare della loro immagine e dignità.
Le istituzioni scolastiche hanno, comunque, la possibilità di regolare o di inibire l'utilizzo di registratori audio-video, inclusi i telefoni cellulari abilitati, all'interno delle aule di lezione o nelle scuole stesse.
Non è possibile, in ogni caso, diffondere o comunicare sistematicamente i dati personali di altre persone (ad esempio immagini o registrazioni audio/video) senza aver prima informato adeguatamente le persone coinvolte e averne ottenuto l'esplicito consenso.

Gli studenti e gli altri membri della comunità scolastica devono quindi prestare particolare attenzione a non mettere on line immagini (ad esempio su blog, siti web, social network) o a diffonderle via mms. Succede spesso, tra l'altro, che una fotografia inviata a un amico/familiare, poi venga inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti.
Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, incorrendo in sanzioni disciplinari, pecuniarie ed eventuali reati.

VIDEOSORVEGLIANZA

L'installazione di sistemi di videosorveglianza nelle scuole deve garantire il diritto dello studente alla riservatezza. In caso di stretta necessità le telecamere sono ammesse, ma devono funzionare solo negli orari di chiusura degli istituti.
Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato.
Le immagini registrate possono essere conservate per brevi periodi.
Infine, i cartelli che segnalano il sistema di videosorveglianza devono essere visibili anche di notte.

PAROLE CHIAVE

CONSENSO
La libera manifestazione della volontà con la quale, previa idonea informativa, l'interessato accetta in modo esplicito – per iscritto, se vi sono dati sensibili – un determinato trattamento di dati personali che lo riguardano.

DATO PERSONALE
Qualunque informazione relativa a un individuo, a una persona giuridica, a un ente o associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

DATO SENSIBILE
Qualunque dato che può rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'appartenenza a partiti, sindacati o ad associazioni, lo stato di salute e la vita sessuale.

INFORMATIVA
Contiene le informazioni che il titolare del trattamento deve fornire all'interessato per chiarire, in particolare, se quest'ultimo è obbligato o meno a rilasciare i dati, quali sono gli scopi e le modalità del trattamento, l'ambito di circolazione dei dati e in che modo si possono esercitare i diritti riconosciuti dalla legge.

INTERESSATO
La persona cui si riferiscono i dati personali.

TRATTAMENTO
Qualunque operazione effettuata sui dati personali: ad esempio la raccolta, la registrazione, la conservazione, l'elaborazione, l'estrazione, la modifica, l'utilizzo, la diffusione, la cancellazione etc.

PER APPROFONDIRE

Chi volesse approfondire i temi segnalati può consultare i seguenti documenti pubblicati sul sito Internet dell'Autorità: www.garanteprivacy.it

Codice in materia di protezione dei dati personali
- Decreto legislativo n. 196 del 30 giugno 2003 (doc. web. n.1311248)
- Relazione annuale 2008 (doc. web. n.1632972) e precedenti

Circolari scolastiche
- Comunicato stampa - 21 marzo 2000 (doc. web. n.46989)

Questionari per attività di ricerca
- Newsletter - 11-24 aprile 2005 (doc. web. n.1120077)
- Provvedimento – 23 dicembre 2004 (doc. web. n.1121429)

Recite, gite scolastiche e foto di classe
- Comunicato stampa - 6 giugno 2007 (doc. web. n.1410643)
- Newsletter – 8-21 dicembre 2003 (doc. web. n. 476650)

Registrazione della lezione
- Vedi sezione "Videofonini, filmati, mms"

Rilevamento delle presenze con dati biometrici
- Newsletter - 12-18 gennaio 2004 (doc. web. n. 567037)

Temi in classe
- Comunicato stampa - 10 marzo 1999 (doc. web. n.48456)

Trattamento dei dati nelle istituzioni scolastiche pubbliche e private
- Autorizzazione n. 2/2009 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale - 16 dicembre 2009 (doc. web. n.1682956)
- Autorizzazione n. 3/2009 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni - 16 dicembre 2009 (doc. web. n.1682967)
- Newsletter - 12 maggio 2006 (doc. web. n.1278310)
- Parere del 16 marzo 2006 sullo schema di regolamento presentato dal Ministero dell'istruzione, dell'università e della ricerca (Decreto ministeriale del 7 dicembre 2006, n. 305) (doc. web. n.1259641)
- Newsletter – 15-21 aprile 2002 (doc. web. n.43899)
- Provvedimento – 10 aprile 2002 (doc. web. n.1065249)

Videofonini, filmati, mms
- Parere del 29 novembre 2007 sulla direttiva del Ministero della pubblica istruzione n. 104 del 30 novembre 2007 (doc. web. n.1466996)
- Provvedimento a carattere generale - 20 gennaio 2005 - (doc. web. n.1089812)
- Provvedimento - 12 marzo 2003 - (doc. web. n.29816)

Videosorveglianza
- Provvedimento generale – 8 aprile 2010 (doc. web. n.1712680)
- Newsletter - 22 settembre 2009 (doc. web n.1651564)
- Verifica preliminare - 4 settembre 2009 (doc. web. n.1651744)

Voti scolastici, scrutini, tabelloni, esami di stato
- Comunicato stampa - 28 agosto 2008 (doc. web. n.1543188)
- Provvedimento - 17 luglio 2008 (doc. web. n.1541699)
- Newsletter - 14 giugno 2005 (doc. web. n.1136703)
- Comunicato stampa - 3 dicembre 2004 (doc. web. n.1069385)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 696771 - fax 06 69677785
www.garanteprivacy.it

giugno 2010

Per informazioni presso l'Autorità:
Ufficio per le relazioni con il pubblico
Lunedì - Venerdì ore 10.00 - 13.00
e-mail: urp@garanteprivacy.it

**A cura del Servizio relazioni
con i mezzi di informazione**

www.garanteprivacy.it

Vertigo Design

CAMERA DEI DEPUTATI

N.22

ATTO DEL GOVERNO SOTTOPOSTO A PARERE PARLAMENTARE

Schema di decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (22)

(articolo 13 della legge 25 ottobre 2017, n. 163)

Trasmesso alla Presidenza il 10 maggio 2018

SCHEMA DI DECRETO LEGISLATIVO RECANTE DISPOSIZIONI PER L'ADEGUAMENTO DELLA NORMATIVA NAZIONALE ALLE 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 E CHE ABROGA LA DIRETTIVA 95/46/CE (REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI)

IL PRESIDENTE DELLA REPUBBLICA

Visti gli articoli 76 e 87 della Costituzione;

Vista la legge 25 ottobre 2017, n. 163, recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017" e, in particolare, l'articolo 13, che delega il Governo all'emanazione di uno o più decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

Vista la legge 24 dicembre 2012, n. 234, recante "Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea";

Visto il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

Visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Vista la direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;

Vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

Vista la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, come modificata dalla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006;

Vista la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 21 marzo 2018;

Acquisito il parere del Garante per la protezione dei dati personali, adottato nell'adunanza del ...;

Acquisiti i pareri delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

Vista la deliberazione del Consiglio dei ministri, adottata nella riunione del...;

Sulla proposta del Presidente del Consiglio dei ministri e del Ministro della giustizia, di concerto con i Ministri per la semplificazione e la pubblica amministrazione, degli affari esteri e della cooperazione internazionale, dell'economia e delle finanze e dello sviluppo economico;

EMANA

il seguente decreto legislativo:

CAPO I
Modifiche al titolo e alle premesse del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196

ART. 1
(Modifiche al titolo e alle premesse del decreto legislativo 30 giugno 2003, n. 196)

1. Al titolo del decreto legislativo 30 giugno 2003, n. 196, dopo le parole "dati personali" sono aggiunte le seguenti: ", recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE".
2. Alle premesse del decreto legislativo 30 giugno 2003, n. 196, dopo il terzo Visto sono inseriti i seguenti:

"Vista la legge 25 ottobre 2017, n. 163, recante "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2016-2017" e, in particolare, l'articolo 13, che delega il Governo all'emanazione di uno o più decreti legislativi di adeguamento del quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016;

Vista la legge 24 dicembre 2012, n. 234, recante "Norme generali sulla partecipazione dell'Italia alla formazione e all'attuazione della normativa e delle politiche dell'Unione europea;

Visto il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);".

CAPO II
Modifiche alla Parte I del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196

ART. 2
(Modifiche alla Parte I, Titolo I, del decreto legislativo 30 giugno 2003, n. 196)

1. Alla Parte I, Titolo I, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica del Titolo I è sostituita dalla seguente: "Disposizioni generali";

b) l'articolo 1 è sostituito dal seguente:

"Art. 1
(*Oggetto*)

1. Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, di seguito "Regolamento", e del presente codice, nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.";

c) l'articolo 2 è sostituito dal seguente:

"Art. 2
(*Finalità*)

1. Il presente codice reca disposizioni per l'adeguamento dell'ordinamento nazionale alle disposizioni del Regolamento.";

d) dopo l'articolo 2 è inserito il seguente:

"Art. 2-*bis*
(*Autorità di controllo*)

1. L'Autorità di controllo di cui all'articolo 51 del Regolamento è individuata nel Garante per la protezione dei dati personali, di seguito "Garante", di cui all'articolo 153.";

e) dopo il Titolo I, sono inseriti i seguenti:

"TITOLO I-*bis*
Principi

Art. 2-*ter*
(*Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*)

1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del Regolamento è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.
2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.
3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1.
4. Si intende per:
a) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile, dalle persone autorizzate, ai sensi dell'articolo 2-*terdecies*, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Art. 2-*quater*
(*Regole deontologiche*)

1. Il Garante promuove, nell'osservanza del principio di rappresentatività e tenendo conto delle raccomandazioni del Consiglio d'Europa sul trattamento dei dati personali, l'adozione di regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, e al Capo IX del Regolamento e ne verifica la conformità alle disposizioni vigenti, anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.
2. Lo schema di regole deontologiche è sottoposto a consultazione pubblica per almeno sessanta giorni.
3. Concluse la fase delle consultazioni, le regole deontologiche sono approvate dal Garante ai sensi dell'articolo 154-bis, comma 1, lettera b), pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono riportate nell'allegato A del presente codice.
4. Il rispetto delle disposizioni contenute nelle regole deontologiche di cui al comma 1 costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali.

Art. 2-*quinquies*
(*Consenso del minore in relazione ai servizi della società dell'informazione*)

1. Al consenso del minore al trattamento dei propri dati personali, in relazione ai servizi della società dell'informazione, si applicano le condizioni di cui all'articolo 8, paragrafo 1, del Regolamento. In relazione a tali servizi, il trattamento dei dati personali del minore di età inferiore a sedici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale.
2. In relazione all'offerta diretta ai minori dei servizi di cui al comma 1, il titolare del trattamento redige con linguaggio particolarmente chiaro e semplice, facilmente accessibile e comprensibile dal minore, le informazioni e le comunicazioni relative al trattamento che lo riguardi.

Art. 2-*sexies*
(*Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante*)

1. I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi della lettera g), paragrafo 2, del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante.
2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a:
a) accesso a documenti amministrativi e accesso civico;
b) tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché rilascio di documenti di riconoscimento o di viaggio o cambiamento delle generalità;
c) tenuta dell'anagrafe nazionale degli abilitati alla guida e dell'archivio nazionale dei veicoli;
d) cittadinanza, immigrazione, asilo, condizione dello straniero e del profugo, stato di rifugiato;
e) elettorato attivo e passivo ed esercizio di altri diritti politici, protezione diplomatica e consolare;
f) attività dei soggetti pubblici dirette all'applicazione, anche tramite i loro concessionari, delle disposizioni in materia tributaria e doganale;

g) attività di controllo e ispettive;

h) concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni;

i) conferimento di onorificenze e ricompense, riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché rilascio e revoca di autorizzazioni o abilitazioni, concessione di patrocini, patronati e premi di rappresentanza, adesione a comitati d'onore e ammissione a cerimonie ed incontri istituzionali;

l) rapporti tra i soggetti pubblici e gli enti del terzo settore;

m) obiezione di coscienza;

n) attività sanzionatorie e di tutela in sede amministrativa o giudiziaria;

o) rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose;

p) attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci;

q) attività amministrative correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale;

r) compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica;

s) tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili;

t) istruzione e formazione in ambito scolastico, professionale, superiore o universitario;

u) trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di rilevante interesse storico, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan);

v) instaurazione, gestione ed estinzione, da parte di soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

3. Per i dati genetici, biometrici e relativi alla salute il trattamento avviene comunque nel rispetto di quanto previsto dall'articolo 2-*septies*.

Art. 2-*septies*.

(*Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute*)

1. In attuazione di quanto previsto dall'articolo 9, paragrafo 4, del Regolamento, i dati genetici, biometrici e relativi alla salute, possono essere oggetto di trattamento in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante, nel rispetto di quanto previsto dal presente articolo.

2. Il provvedimento che stabilisce le misure di garanzia di cui al comma 1 è adottato con cadenza almeno biennale e tenendo conto:

a) delle linee guida, delle raccomandazioni e delle migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e delle migliori prassi in materia di trattamento dei dati personali;

b) dell'evoluzione scientifica e tecnologica nel settore oggetto delle misure;

c) dell'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea.

3. Lo schema di provvedimento è sottoposto a consultazione pubblica per un periodo non inferiore a sessanta giorni.

4. Le misure di garanzia sono adottate nel rispetto di quanto previsto dall'articolo 9, paragrafo 2, del Regolamento e riguardano anche le cautele da adottare relativamente a:

a) contrassegni sui veicoli e accessi a zone a traffico limitato;

b) profili organizzativi e gestionali in ambito sanitario;

c) modalità per la comunicazione diretta all'interessato delle diagnosi e dei dati relativi alla propria salute;

d) prescrizioni di medicinali.

5. Le misure di garanzia sono adottate in relazione a ciascuna categoria dei dati personali di cui al comma 1, avendo riguardo alle specifiche finalità del trattamento e possono individuare, in conformità a quanto previsto al comma 2, ulteriori condizioni sulla base delle quali il trattamento di tali dati è consentito.

6. Le misure di garanzia relative ai dati genetici e quelle di cui al comma 4, lettere b), c) e d), sono adottate sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio superiore di sanità. Per i dati genetici, le misure di garanzia possono individuare, in caso di particolare ed elevato livello di rischio, il consenso come ulteriore misura di protezione dei diritti dell'interessato, a norma dell'articolo 9, paragrafo 4, del Regolamento, o altre cautele specifiche.

7. I dati personali di cui al comma 1 non possono essere diffusi.

Art. 2-*octies*

(*Principi relativi al trattamento di dati relativi a condanne penali e reati*)

1. Fatto salvo quanto previsto dal decreto legislativo adottato in attuazione dell'articolo 11 della legge 25 ottobre 2017, n. 163, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento, che non avviene sotto il controllo dell'autorità pubblica, è consentito, ai sensi dell'articolo 10 del medesimo Regolamento, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

2. In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonché le garanzie di cui al medesimo comma sono individuate con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante.

3. Fermo quanto previsto dai commi 1 e 2, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, riguardanti, in particolare:

a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi, secondo quanto previsto dagli articoli 9, paragrafo 2, lettera b), e 88 del Regolamento;

b) l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;

c) la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;

d) l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

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

f) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;

g) l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del Testo unico delle leggi di pubblica sicurezza;

h) l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o *in materia di prevenzione* della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;

i) l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;

l) l'attuazione della disciplina in materia di attribuzione del *rating* di legalità delle imprese ai sensi dell'articolo 5-*ter* del decreto-legge 24 gennaio 2012, n.1, convertito, con modificazioni, dalla legge 24 marzo 2012, n. 27;

m) l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

4. Nei casi in cui le disposizioni di cui al comma 3 non individuano le garanzie appropriate per i diritti e le libertà degli interessati, tali garanzie sono previste con il decreto di cui al comma 2.

5. Quando il trattamento dei dati di cui al presente articolo avviene sotto il controllo dell'autorità pubblica si applicano le disposizioni previste dall'articolo 2-*sexies*.

6. Con il decreto di cui al comma 2 è autorizzato il trattamento dei dati di cui all'articolo 10 del Regolamento, effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata, stipulati con il Ministero dell'interno o con le Prefetture-UTG. In relazione a tali protocolli, il decreto di cui al comma 2 individua, le tipologie dei dati trattati, gli interessati, le operazioni di trattamento eseguibili, anche in relazione all'aggiornamento e alla conservazione e prevede le garanzie appropriate per i diritti e le libertà degli interessati. Il decreto è adottato, limitatamente agli ambiti di cui al presente comma, di concerto con il Ministro dell'interno.

Art. 2-*novies*
(*Inutilizzabilità dei dati*)

1. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

TITOLO I-*ter*
Disposizioni in materia di diritti dell'interessato

Art. 2-*decies*
(*Limitazioni ai diritti dell'interessato*)

1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare o al responsabile del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;

b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;

c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;

d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria.

2. Nei casi di cui al comma 1, lettera c), si applica quanto previsto dai regolamenti parlamentari ovvero dalla legge o dalle norme istitutive della Commissione d'inchiesta.

3. Nei casi di cui al comma 1, lettere a), b), d) ed e), i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere a), b), d) ed e). In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facoltà di cui al presente comma.

Art. 2-*undecies*
(*Limitazioni per ragioni di giustizia*)

1. In applicazione dell'articolo 23, paragrafo 1, lettera f), del Regolamento, in relazione ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, i diritti e gli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento sono disciplinati nei limiti e con le modalità previste dalle disposizioni di legge o di regolamento che regolano tali procedimenti, nel rispetto di quanto previsto dal paragrafo 2 dell'articolo 23 del Regolamento.

2. Fermo quanto previsto dal comma 1, l'esercizio dei diritti e l'adempimento degli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento possono essere ritardati, limitati o esclusi, con comunicazione motivata e resa senza ritardo all'interessato, nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari.

3. Si applica l'articolo 2-*decies*, comma 3, terzo, quarto e quinto periodo.

4. Ai fini del presente articolo si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari. Le ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.

Art. 2-*duodecies*
(*Diritti riguardanti le persone decedute*)

1. I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

2. L'esercizio dei diritti di cui al comma 1 non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'interessato lo ha espressamente vietato con dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata.
3. La volontà dell'interessato di vietare l'esercizio dei diritti di cui al comma 1 deve risultare in modo non equivoco e deve essere specifica, libera e informata; il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui al predetto comma.
4. L'interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui ai commi 2 e 3.
5. In ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

TITOLO I-*quater*
Disposizioni relative al titolare del trattamento e responsabile del trattamento

Art. 2-*terdecies*
(*Attribuzione di funzioni e compiti a soggetti designati*)

1. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.
2. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Art. 2-*quaterdecies*
(*Trattamento che presenta rischi specifici per l'esecuzione di un compito di interesse pubblico*)

1. Con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che può presentare rischi particolarmente elevati ai sensi dell'articolo 35 del Regolamento, il Garante può, sulla base di quanto disposto dall'articolo 36, paragrafo 5, del medesimo Regolamento e con provvedimenti di carattere generale adottati d'ufficio, prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

Art. 2-*quinquiesdecies*
(*Organismo nazionale di accreditamento*)

1. L'organismo nazionale di accreditamento di cui all'articolo 43, paragrafo 1, lettera b), del Regolamento è l'Ente unico nazionale di accreditamento, istituito ai sensi del regolamento (CE) n. 765/2008, del Parlamento europeo e del Consiglio, del 9 luglio 2008, fatto salvo il potere del Garante di assumere direttamente l'esercizio di tali funzioni con riferimento a una o più categorie di trattamenti.".

CAPO III
Modifiche alla Parte II del codice in materia di protezione dei dati personali di cui decreto legislativo 30 giugno 2003, n. 196

ART. 3
(*Modifiche alla rubrica e al Titolo I della Parte II, del decreto legislativo 30 giugno 2003, n. 196*)

1. La rubrica della Parte II del decreto legislativo 30 giugno 2003, n. 196, è sostituita dalla seguente: "Disposizioni specifiche per i trattamenti necessari per adempiere ad un obbligo legale o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri nonché disposizioni per i trattamenti di cui al capo IX del Regolamento".

2. Al Titolo I della Parte II, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) prima del Titolo I, è inserito il seguente:

"TITOLO 0.I
Disposizioni sulla base giuridica

Art. 2-*sexiesdecies*
(*Base giuridica*)

1. Le disposizioni contenute nella presente parte sono stabilite in attuazione dell'articolo 6, paragrafo 2, nonché dell'articolo 23, paragrafo 1, del Regolamento.";

b) all'articolo 50, è aggiunto, in fine, il seguente periodo: "La violazione del divieto di cui al presente articolo è punita ai sensi dell'articolo 684 del codice penale.";

c) all'articolo 52:
1) al comma 1, le parole: "per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica," sono soppresse;
2) al comma 6, le parole "dell'articolo 32 della legge 11 febbraio 1994, n. 109," sono sostituite dalle seguenti: "dell'articolo 209 del Codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50,".

ART. 4
(*Modifiche alla Parte II, Titolo III, del decreto legislativo 30 giugno 2003, n. 196*)

1. Alla Parte II, Titolo III, del decreto legislativo 30 giugno 2003, n. 196, l'articolo 58 è sostituito dal seguente:

"Art. 58
(*Trattamenti di dati personali per fini di sicurezza nazionale o difesa*)

1. Ai trattamenti di dati personali effettuati dagli organismi di cui agli articoli 4, 6 e 7 della legge 3 agosto 2007, n. 124, sulla base dell'articolo 26 della predetta legge o di altre disposizioni di legge o regolamento, ovvero relativi a dati coperti da segreto di Stato ai sensi degli articoli 39 e seguenti della medesima legge, si applicano le disposizioni di cui all'articolo 160, comma 4, nonché, in quanto compatibili, le disposizioni di cui agli articoli 2, 3, 8, 15, 16, 18, 25, 37, 41, 42 e 43 del decreto legislativo adottato in attuazione dell'articolo 11 della legge 25 ottobre 2017, n. 163.
2. Fermo restando quanto previsto dal comma 1, ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, si applicano le disposizioni di cui al comma 1 del presente articolo, nonché quelle di cui agli articoli 23 e 24 del decreto legislativo adottato in attuazione dell'articolo 11 della legge 25 ottobre 2017, n. 163.
3. Con uno o più regolamenti sono individuate le modalità di applicazione delle disposizioni di cui ai commi 1 e 2, in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del

titolare o del responsabile ai sensi dell'articolo 2-*terdecies*, anche in relazione all'aggiornamento e alla conservazione. I regolamenti, negli ambiti di cui al comma 1, sono adottati ai sensi dell'articolo 43 della legge 3 agosto 2007, n. 124, e, negli ambiti di cui al comma 2, sono adottati con decreto del Presidente del Consiglio dei ministri, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, su proposta dei Ministri competenti.
4. Con uno o più regolamenti adottati con decreto del Presidente della Repubblica su proposta del Ministro della difesa, sono disciplinate le misure attuative del presente decreto in materia di esercizio delle funzioni di difesa e sicurezza nazionale da parte delle Forze armate.".

ART. 5

(Modifiche alla Parte II, Titolo IV, del decreto legislativo 30 giugno 2003, n. 196)

1. Alla Parte II, Titolo IV, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) all'articolo 59:
1) alla rubrica sono aggiunte, in fine, le seguenti parole: "e accesso civico";
2) al comma 1, le parole "sensibili e giudiziari" sono sostituite dalle seguenti: "di cui agli articoli 9 e 10 del Regolamento" e le parole "Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico." sono soppresse;
3) dopo il comma 1 è aggiunto il seguente: "1-*bis*. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal decreto legislativo 14 marzo 2013, n. 33.";

b) l'articolo 60 è sostituito dal seguente:

"Art. 60

(Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale)

1. Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.";

c) all'articolo 61:
1) alla rubrica sono aggiunte, in fine, le seguenti parole: "e regole deontologiche";
2) i commi 1 e 2 sono sostituiti dai seguenti:
"1. Il Garante promuove, ai sensi dell'articolo 2-*quater*, l'adozione di regole deontologiche per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui deve essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da più archivi, tenendo presenti le pertinenti Raccomandazioni del Consiglio d'Europa.
2. Agli effetti dell'applicazione del presente codice i dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, che devono essere inseriti in un albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 2-*ter* del presente codice, anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che a qualsiasi titolo incidono sull'esercizio della professione.".

ART. 6

(*Modifiche alla Parte II, Titolo V, del decreto legislativo 30 giugno 2003, n. 196*)

1. Alla Parte II, Titolo V, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) l'articolo 75 è sostituito dal seguente:

"Art. 75
(*Specifiche condizioni in ambito sanitario*)

1. Il trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività deve essere effettuato ai sensi dell'articolo 9, paragrafi 2, lettere h) ed i), e 3 del Regolamento, dell'articolo 2-*septies* del presente codice, nonché nel rispetto delle specifiche disposizioni di settore.
2. In applicazione dell'articolo 23, comma 1, lettera e) del Regolamento, al trattamento dei dati personali effettuato per finalità di tutela della salute e incolumità fisica dell'interessato o di terzi o della collettività non si applica il diritto di cui agli articoli 17 e 20 del medesimo Regolamento.".

b) la rubrica del Capo II è sostituita dalla seguente: "Modalità particolari per informare l'interessato e per il trattamento dei dati personali";

c) l'articolo 77 è sostituito dal seguente:

"Art. 77
(*Modalità particolari*)

1. Le disposizioni del presente titolo individuano modalità particolari utilizzabili dai soggetti di cui al comma 2:
a) per informare l'interessato ai sensi degli articoli 13 e 14 del Regolamento;
b) per il trattamento dei dati personali.
2. Le modalità di cui al comma 1 sono applicabili:
a) dalle strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie e dagli esercenti le professioni sanitarie;
b) dai soggetti pubblici indicati all'articolo 80.";

d) all'articolo 78:
1) alla rubrica la parola "Informativa" è sostituita dalla seguente: "Informazioni";
2) al comma 1, le parole "nell'articolo 13, comma 1" sono sostituite dalle seguenti: "negli articoli 13 e 14 del Regolamento";
3) al comma 2, le parole "L'informativa può essere fornita" sono sostituite dalle seguenti: "Le informazioni possono essere fornite" e le parole "prevenzione, diagnosi, cura e riabilitazione" sono sostituite dalle seguenti: "diagnosi, assistenza e terapia sanitaria";
4) il comma 3, è sostituito dal seguente: "3. Le informazioni possono riguardare, altresì, dati personali eventualmente raccolti presso terzi e sono fornite preferibilmente per iscritto.";
5) al comma 4, le parole "L'informativa" sono sostituite dalle seguenti: "Le informazioni" e la parola "riguarda" è sostituita dalla seguente "riguardano";
6) al comma 5:
6.1. le parole "L'informativa resa" sono sostituite dalle seguenti: "Le informazioni rese";
6.2. la parola "evidenzia" è sostituita dalla seguente: "evidenziano";
6.3. la lettera a) è sostituita dalla seguente: "a) per fini di ricerca scientifica anche nell'ambito di sperimentazioni cliniche, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;";

6.4. sono aggiunte, in fine, le seguenti lettere: "*c-bis*) ai fini dell'implementazione del fascicolo sanitario elettronico di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221; *c-ter*) ai fini dei sistemi di sorveglianza e dei registri di cui all'articolo 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221.";

e) all'articolo 79:

1) la rubrica è sostituita dalla seguente: "(*Informazioni da parte di strutture pubbliche e private che erogano prestazioni sanitarie e socio-sanitarie*)";

2) il comma 1 è sostituito dal seguente: "1. Le strutture pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie possono avvalersi delle modalità particolari di cui all'articolo 78 in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità della stessa struttura o di sue articolazioni ospedaliere o territoriali specificamente identificate.";

3) al comma 2, le parole "l'organismo e le strutture" sono sostituite dalle seguenti: "la struttura o le sue articolazioni" e le parole "informativa e il consenso" sono sostituite dalla seguente: "informazione";

4) al comma 3, le parole "semplificate di cui agli articoli 78 e 81" sono sostituite dalle seguenti: "particolari di cui all'articolo 78";

5) al comma 4, la parola "semplificate" è sostituita dalla seguente "particolari";

f) l'articolo 80 è sostituito dal seguente:

"ART. 80

(*Informazioni da parte di altri soggetti*)

"1. Nel fornire le informazioni di cui agli articoli 13 e 14 del Regolamento, oltre a quanto previsto dall'articolo 79, possono avvalersi della facoltà di fornire un'unica informativa per una pluralità di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti servizi o strutture di altri soggetti pubblici, diversi da quelli di cui al predetto articolo 79, operanti in ambito sanitario o della protezione e sicurezza sociale.

2. Le informazioni di cui al comma 1 sono integrate con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attività amministrative effettuate per motivi di interesse pubblico rilevante che non richiedono il consenso degli interessati.";

g) all'articolo 82:

1) al comma 1, le parole da "L'informativa" fino a "intervenire" sono sostituite dalle seguenti: "Le informazioni di cui agli articoli 13 e 14 del Regolamento possono essere rese";

2) al comma 2: le parole da "L'informativa" fino a "intervenire" sono sostituite dalle seguenti: "Tali informazioni possono altresì essere rese", e la lettera a) è sostituita dalla seguente: "a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile rendere le informazioni, nei casi previsti, a chi esercita legalmente la rappresentanza, ovvero a un prossimo congiunto, a un familiare, a un convivente o unito civilmente ovvero a un fiduciario ai sensi dell'articolo 4 della legge 22 dicembre 2017, n. 219 o, in loro assenza, al responsabile della struttura presso cui dimora l'interessato;";

3) al comma 3, le parole da "L'informativa" fino a "intervenire" sono sostituite dalle seguenti: "Le informazioni di cui al comma 1 possono essere rese" e le parole "dall'acquisizione preventiva del consenso" sono sostituite dalle seguenti: "dal loro preventivo rilascio";

4) al comma 4, le parole "l'informativa è fornita" sono sostituite dalle seguenti: "le informazioni sono fornite" e le parole da "anche" fino a "necessario" sono sostituite dalle seguenti: "nel caso in cui non siano state fornite in precedenza";

h) dopo l'articolo 89 è aggiunto il seguente:

"Art. 89-*bis*
(*Prescrizioni di medicinali*)

1. Per le prescrizioni di medicinali, laddove non è necessario inserire il nominativo dell'interessato, si adottano cautele particolari in relazione a quanto disposto dal Garante nelle misure di garanzia di cui all'articolo 2-*septies*, anche ai fini del controllo della correttezza della prescrizione ovvero per finalità amministrative o per fini di ricerca scientifica nel settore della sanità pubblica.";

i) all'articolo 92:

1) al comma 1, le parole "organismi sanitari pubblici e privati" sono sostituite dalle seguenti: "strutture, pubbliche e private, che erogano prestazioni sanitarie e socio-sanitarie";

2) al comma 2, lettera a), le parole "di far valere" sono sostituite dalle seguenti: "di esercitare", le parole "ai sensi dell'articolo 26, comma 4, lettera c)," sono sostituite dalle seguenti: ", ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento," e le parole "e inviolabile" sono soppresse;

3) alla lettera b), le parole "e inviolabile" sono soppresse.

ART. 7
(*Modifiche alla Parte II, Titolo VI, del decreto legislativo 30 giugno 2003, n. 196*)

1. Alla Parte II, Titolo VI, del decreto legislativo 30 giugno 2003, n. 196, l'articolo 96 è sostituito dal seguente:

"Art. 96
(*Trattamento di dati relativi a studenti*)

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.".

ART. 8
(*Modifiche alla Parte II, Titolo VII, del decreto legislativo 30 giugno 2003, n. 196*)

1. Alla Parte II, Titolo VII, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica è sostituita dalla seguente: "(*Trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*)";

b) l'articolo 97 è sostituito dal seguente:

"Art. 97
(*Ambito applicativo*)

1. Il presente titolo disciplina il trattamento dei dati personali effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ai sensi dell'articolo 89 del Regolamento.";

c) l'articolo 99 è sostituito dal seguente:

"Art. 99
(*Durata del trattamento*)

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.
2. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento nel rispetto di quanto previsto dall'articolo 89, paragrafo 1, del Regolamento.";

d) all'articolo 100:
1) al comma 1, le parole "sensibili o giudiziari" sono sostituite dalle seguenti: "di cui agli articoli 9 e 10 del Regolamento";
2) al comma 2, le parole da "opporsi" fino alla fine del comma, sono sostituite dalle seguenti: "rettifica, cancellazione, limitazione e opposizione ai sensi degli articoli 16, 17, 18 e 21 del Regolamento";
3) dopo il comma 4, è aggiunto il seguente: "4-*bis*. I diritti di cui al comma 2 si esercitano con le modalità previste dalle regole deontologiche.";

e) la rubrica del Capo II è sostituita dalla seguente: "Trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica";

f) all'articolo 101:
1) al comma 1, le parole "per scopi storici" sono sostituite dalle seguenti: "a fini di archiviazione nel pubblico interesse o di ricerca storica" e le parole "dell'articolo 11" sono sostituite dalle seguenti: "dell'articolo 5 del Regolamento";
2) al comma 2, le parole "per scopi storici" sono sostituite dalle seguenti: "a fini di archiviazione nel pubblico interesse o di ricerca storica";

g) all'articolo 102:
1) la rubrica è sostituita dalla seguente: "(*Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica*)";
2) il comma 1 è sostituito dal seguente: "1. Il Garante promuove, ai sensi dell'articolo 2-*quater*, la sottoscrizione di regole deontologiche per i soggetti pubblici e privati, ivi comprese

le società scientifiche e le associazioni professionali, interessati al trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica.";

3) al comma 2 sono apportate le seguenti modificazioni:

3.1 l'alinea è sostituito dal seguente: "2. Le regole deontologiche di cui al comma 1 individuano garanzie adeguate per i diritti e le libertà dell'interessato in particolare:";

3.2 alla lettera a), dopo la parola "codice" sono inserite le seguenti: "e del Regolamento";

3.3 alla lettera c) le parole "a scopi storici" sono sostituite dalle seguenti: "a fini di archiviazione nel pubblico interesse o di ricerca storica";

h) l'articolo 103 è sostituito dal seguente:

"Art. 103

(Consultazione di documenti conservati in archivi)

1. La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati dichiarati di notevole interesse storico è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42 e dalle relative regole deontologiche.";

i) la rubrica del Capo III è sostituita dalla seguente: "Trattamento a fini statistici o di ricerca scientifica";

l) all'articolo 104:

1) alla rubrica, le parole "per scopi statistici o scientifici" sono sostituite dalle seguenti: "a fini statistici o di ricerca scientifica";

2) al comma 1, le parole "scopi statistici" sono sostituite dalle seguenti: "fini statistici" e le parole "scopi scientifici" sono sostituite dalle seguenti: "per fini di ricerca scientifica";

m) all'articolo 105:

1) al comma 1, le parole "per scopi statistici o scientifici" sono sostituite dalle seguenti: "a fini statistici o di ricerca scientifica";

2) al comma 2, le parole "Gli scopi statistici o scientifici" sono sostituite dalle seguenti: "I fini statistici e di ricerca scientifica", le parole "all'articolo 13" sono sostituite dalle seguenti: "agli articoli 13 e 14 del Regolamento" e le parole ", e successive modificazioni" sono soppresse;

3) al comma 3, le parole "dai codici" sono sostituite dalle seguenti: "dalle regole deontologiche" e le parole "l'informativa all'interessato può essere data" sono sostituite dalle seguenti: "le informazioni all'interessato possono essere date";

4) al comma 4, le parole "per scopi statistici o scientifici" sono sostituite dalle seguenti: "a fini statistici o di ricerca scientifica", le parole "l'informativa all'interessato non è dovuta" sono sostituite dalle seguenti: "le informazioni all'interessato non sono dovute" e le parole "dai codici" sono sostituite dalle seguenti: "dalle regole deontologiche";

n) l'articolo 106 è sostituito dal seguente:

"Art. 106

(Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica)

1. Il Garante promuove, ai sensi dell'articolo 2-*quater*, regole deontologiche per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per fini statistici o di ricerca scientifica, volte a individuare garanzie adeguate per i diritti e le libertà dell'interessato in conformità all'articolo 89 del Regolamento.

2. Con le regole deontologiche di cui al comma 1, tenendo conto, per i soggetti già compresi nell'ambito del Sistema statistico nazionale, di quanto già previsto dal decreto legislativo 6

settembre 1989, n. 322, e, per altri soggetti, sulla base di analoghe garanzie, sono individuati in particolare:

a) i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal medesimo decreto legislativo n. 322 del 1989, siano effettuati per idonei ed effettivi fini statistici o di ricerca scientifica;

b) per quanto non previsto dal presente codice, gli ulteriori presupposti del trattamento e le connesse garanzie, anche in riferimento alla durata della conservazione dei dati, alle informazioni da rendere agli interessati relativamente ai dati raccolti anche presso terzi, alla comunicazione e diffusione, ai criteri selettivi da osservare per il trattamento di dati identificativi, alle specifiche misure di sicurezza e alle modalità per la modifica dei dati a seguito dell'esercizio dei diritti dell'interessato, tenendo conto dei principi contenuti nelle pertinenti raccomandazioni del Consiglio d'Europa;

c) l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare direttamente o indirettamente l'interessato, anche in relazione alle conoscenze acquisite in base al progresso tecnico;

d) le garanzie da osservare nei casi in cui si può prescindere dal consenso dell'interessato, tenendo conto dei principi contenuti nelle raccomandazioni di cui alla lettera b);

e) modalità semplificate per la prestazione del consenso degli interessati relativamente al trattamento dei dati di cui all'articolo 9 del Regolamento;

f) i casi nei quali i diritti di cui agli articoli 15, 16, 18 e 21 del Regolamento possono essere limitati ai sensi dell'articolo 89, paragrafo 2, del medesimo Regolamento;

g) le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire alle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-*terdecies*;

h) le misure da adottare per favorire il rispetto del principio di minimizzazione e delle misure tecniche e organizzative di cui all'articolo 32 del Regolamento, anche in riferimento alle cautele volte ad impedire l'accesso da parte di persone fisiche che non sono autorizzate o designate e l'identificazione non autorizzata degli interessati, all'interconnessione dei sistemi informativi anche nell'ambito del Sistema statistico nazionale e all'interscambio di dati per fini statistici o di ricerca scientifica da effettuarsi con enti ed uffici situati all'estero;

i) l'impegno al rispetto di regole deontologiche da parte delle persone che, ai sensi dell'articolo 2-*terdecies*, risultano autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento, che non sono tenute in base alla legge al segreto d'ufficio o professionale, tali da assicurare analoghi livelli di sicurezza e di riservatezza.";

o) l'articolo 107 è sostituito dal seguente:

"Art. 107

(*Trattamento di categorie particolari di dati personali*)

1. Fermo restando quanto previsto dall'articolo 2-*sexies* e fuori dei casi di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di dati di cui all'articolo 9 del Regolamento, quando è richiesto, può essere prestato con modalità semplificate, individuate dalle regole deontologiche di cui all'articolo 106 o dalle misure di cui all'articolo 2-*septies*.";

p) l'articolo 108 è sostituito dal seguente:

"Art. 108

(*Sistema statistico nazionale*)

1. Il trattamento di dati personali da parte di soggetti che fanno parte del Sistema statistico nazionale, oltre a quanto previsto dalle regole deontologiche di cui all'articolo 106, comma 2, resta inoltre disciplinato dal decreto legislativo 6 settembre 1989, n. 322, in particolare per quanto

riguarda il trattamento dei dati di cui all'articolo 9 del Regolamento indicati nel programma statistico nazionale, le informative all'interessato, l'esercizio dei relativi diritti e i dati non tutelati dal segreto statistico ai sensi dell'articolo 9, comma 4, del medesimo decreto legislativo n. 322 del 1989.";

q) all'articolo 109, comma 1, le parole "della statistica, sentito il Ministro" sono sostituite dalle seguenti: "di statistica, sentiti i Ministri";

r) l'articolo 110 è sostituito dal seguente:

"Art. 110
(*Ricerca medica, biomedica ed epidemiologica*)

1. Il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-*bis* del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento.
2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 16 del Regolamento nei riguardi dei trattamenti di cui al comma 1, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.";

s) l'articolo 110-*bis* è sostituito dal seguente:

"Art. 110-*bis*
(*Riutilizzo dei dati a fini di ricerca scientifica o a fini statistici*)

1. Il Garante può autorizzare il riutilizzo dei dati, compresi quelli dei trattamenti speciali di cui all'articolo 9 del Regolamento, ad esclusione di quelli genetici, a fini di ricerca scientifica o a fini statistici da parte di soggetti che svolgano principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione che siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati.
2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione o anche successivamente, sulla base di eventuali verifiche, il Garante stabilisce le condizioni e le misure necessarie ad assicurare adeguate garanzie a tutela degli interessati nell'ambito del riutilizzo dei dati, anche sotto il profilo della loro sicurezza.
3. Non costituisce riutilizzo il trattamento dei dati raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del

carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca.".

ART. 9

(Modifiche alla Parte II, Titolo VIII, del decreto legislativo 30 giugno 2003, n. 196)

1. Alla Parte II, Titolo VIII, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica è sostituita dalla seguente: "Trattamenti nell'ambito del rapporto di lavoro";
b) l'articolo 111 è sostituito dal seguente:

"Art. 111

(Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro)

1. Il Garante promuove, ai sensi dell'articolo 2-*quater*, l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.";

c) dopo l'articolo 111 è aggiunto il seguente:

"Art. 111-*bis*

(Informazioni in caso di ricezione di curriculum)

1. Le informazioni di cui all'articolo 13 del Regolamento e il consenso al trattamento non sono dovuti in caso di ricezione di *curriculum* spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Le informazioni vengono comunque fornite al momento del primo contatto successivo all'invio del *curriculum*.";

d) la rubrica del Capo III è sostituita dalla seguente: "Trattamento di dati riguardanti i prestatori di lavoro";

e) all'articolo 114:
1) la rubrica è sostituita dalla seguente: "*(Raccolta di dati, pertinenza e garanzie in materia di controllo a distanza)*";
2) sono aggiunte, in fine, le seguenti parole: ", nonché dall'articolo 10 del decreto legislativo 10 settembre 2003, n. 276.";

f) all'articolo 115:
1) la rubrica è sostituita dalla seguente: "*(Telelavoro, lavoro agile e lavoro domestico)*";
2) al comma 1, le parole "e del telelavoro" sono sostituite dalle seguenti: "del telelavoro e del lavoro agile";

g) all'articolo 116, comma 1, le parole "ai sensi dell'articolo 23" sono sostituite dalle seguenti: "dall'interessato medesimo".

ART. 10

(Modifiche alla Parte II, Titolo IX, del decreto legislativo 30 giugno 2003, n. 196)

1. Alla Parte II, Titolo IX, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica è sostituita dalla seguente: "Altri trattamenti in ambito pubblico o di interesse pubblico";

b) la rubrica del Capo I è sostituita dalla seguente: "Assicurazioni";

c) all'articolo 120:

1) al comma 1, le parole "private e di interesse collettivo (ISVAP)" sono soppresse;

2) al comma 3, sono aggiunte, in fine, le seguenti parole: "di cui al decreto legislativo 7 settembre 2005, n. 209".

ART. 11

(Modifiche alla Parte II, Titolo X, del decreto legislativo 30 giugno 2003, n. 196)

1. Alla Parte II, Titolo X, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) all'articolo 121:

1) la rubrica è sostituita dalla seguente: "*(Servizi interessati e definizioni)*";

2) dopo il comma 1, è aggiunto il seguente:

"1-*bis*. Ai fini dell'applicazione delle disposizioni del presente titolo si intende per:

a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;

b) "chiamata", la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;

c) "reti di comunicazione elettronica", i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) "rete pubblica di comunicazioni", una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;

e) "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) "contraente", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) "dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) "servizio a valore aggiunto", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.";

b) all'articolo 122, comma 1, le parole "con le modalità semplificate di cui all'articolo 13, comma 3" e il terzo periodo, sono soppressi;

c) all'articolo 123:

1) al comma 4, le parole "l'informativa di cui all'articolo 13" sono sostituite dalle seguenti: "le informazioni di cui agli articoli 13 e 14 del Regolamento";

2) al comma 5, le parole "ad incaricati del trattamento che operano ai sensi dell'articolo 30" sono sostituite dalle seguenti: "a persone che, ai sensi dell'articolo 2-*terdecies*, risultano autorizzate al trattamento e che operano" e le parole "dell'incaricato" sono sostituite dalle seguenti: "della persona autorizzata";

d) all'articolo 125, comma 1, è aggiunto, in fine, il seguente periodo: "Rimane in ogni caso fermo quanto previsto dall'articolo 2, comma 1, della legge 11 gennaio 2018, n. 5.";

e) all'articolo 126, comma 4, le parole "ad incaricati del trattamento che operano ai sensi dell'articolo 30," sono sostituite dalle seguenti: "a persone autorizzate al trattamento, ai sensi dell'articolo 2-*terdecies*, che operano" e le parole "dell'incaricato" sono sostituite dalle seguenti: "della persona autorizzata";

f) l'articolo 129 è sostituito dal seguente:

"Art. 129
(*Elenchi dei contraenti*)

1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 4, e in conformità alla normativa dell'Unione europea, le modalità di inserimento e di successivo utilizzo dei dati personali relativi ai contraenti negli elenchi cartacei o elettronici a disposizione del pubblico.

2. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per finalità di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale nonché per le finalità di cui all'articolo 21, paragrafo 2, del Regolamento, in base al principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca del contraente per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri.";

g) all'articolo 130:

1) al comma 1, è aggiunto, in fine, il seguente periodo: "Resta in ogni caso fermo quanto previsto dall'articolo 2, comma 14, della legge 11 gennaio 2018, n. 5.";

2) al comma 3, le parole "23 e 24" sono sostituite dalle seguenti: "6 e 7 del Regolamento" e le parole "del presente articolo" sono soppresse;

3) al comma 3-*bis*, le parole "all'articolo 129, comma 1," sono sostituite dalle seguenti: "al comma 1 del predetto articolo," e le parole "di cui all'articolo 7, comma 4, lettera b)" sono sostituite dalle seguenti: "di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale";

4) al comma 3-*ter*, lettera b), le parole "codice dei contratti pubblici relativi a lavori, servizi e forniture, di cui al decreto legislativo 12 aprile 2006, n. 163" sono sostituite dalle seguenti "codice dei contratti pubblici di cui al decreto legislativo 18 aprile 2016, n. 50";

5) al comma 3-*ter*, lettera f), le parole "di cui all'articolo 7, comma 4, lettera b)" sono sostituite dalle seguenti: "di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale";

6) al comma 3-*ter*, lettera g), le parole "degli articoli 23 e 24" sono sostituite dalle seguenti "degli articoli 6 e 7 del Regolamento";

7) al comma 5, le parole "all'articolo 7" sono sostituite dalle seguenti: "agli articoli da 15 a 22 del Regolamento";

8) al comma 6, le parole "dell'articolo 143, comma 1, lettera b)" sono sostituite dalle seguenti: "dell'articolo 58 del Regolamento";

h) all'articolo 131, la rubrica è sostituita dalla seguente: "(*Informazioni a contraenti e utenti*)";

i) all'articolo 132:

1) al comma 3, secondo periodo, le parole ", ferme restando le condizioni di cui all'articolo 8, comma 2, *lettera f)*, per il traffico entrante" sono soppresse ed è aggiunto, in fine, il seguente periodo: "La richiesta di accesso diretto alle comunicazioni telefoniche in entrata può essere effettuata solo quando possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397; diversamente, i diritti di cui agli articoli da 12 a 22 del Regolamento possono essere esercitati con le modalità di cui all'articolo 2-*decies*, comma 3, terzo, quarto e quinto periodo.";

2) al comma 5, le parole "ai sensi dell'articolo 17" sono sostituite dalle seguenti: "dal Garante secondo le modalità di cui all'articolo 2-*quaterdecies*" e le parole da "nonché a:" a "d)" sono sostituite dalle seguenti: ""nonché ad";

3) dopo il comma 5, è aggiunto il seguente: "5-*bis*. E' fatta salva la disciplina di cui all'articolo 24 della legge 20 novembre 2017, n. 167.";

l) dopo l'articolo 132-*bis* sono inseriti i seguenti:

"Art. 132-*ter*

(*Sicurezza del trattamento*)

1. Nel rispetto di quanto disposto dall'articolo 32 del Regolamento, ai fornitori di servizi di comunicazione elettronica accessibili al pubblico si applicano le disposizioni del presente articolo.
2. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta, ai sensi dell'articolo 32 del Regolamento, anche attraverso altri soggetti a cui sia affidata l'erogazione del servizio, misure tecniche e organizzative adeguate al rischio esistente.
3. I soggetti che operano sulle reti di comunicazione elettronica garantiscono che i dati personali siano accessibili soltanto al personale autorizzato per fini legalmente autorizzati.
4. Le misure di cui ai commi 2 e 3 garantiscono la protezione dei dati relativi al traffico ed all'ubicazione e degli altri dati personali archiviati o trasmessi dalla distruzione anche accidentale, da perdita o alterazione anche accidentale e da archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti, nonché garantiscono l'attuazione di una politica di sicurezza.
5. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di

mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

Art. 132-*quater*
(*Informazioni sui rischi*)

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare a norma dell'articolo 132-*ter*, commi 2, 3 e 5, tutti i possibili rimedi e i relativi costi presumibili. Analoghe informazioni sono rese al Garante e all'Autorità per le garanzie nelle comunicazioni.".

ART. 12
(*Modifiche alla Parte II, Titolo XII, del decreto legislativo 30 giugno 2003, n. 196*)

1. Alla Parte II, Titolo XII, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica è sostituita dalla seguente: "Giornalismo, libertà di informazione e di espressione";

b) all'articolo 136, comma 1:
1) all'alinea, dopo le parole "si applicano" inserire le seguenti: ", ai sensi dell'articolo 85 del Regolamento,";
2) alla lettera c), la parola "temporaneo" è soppressa e le parole "nell'espressione artistica" sono sostituite dalle seguenti: "nell'espressione accademica, artistica e letteraria";

c) l'articolo 137 è sostituito dal seguente:

"Art. 137
(*Disposizioni applicabili*)

1. Con riferimento a quanto previsto dall'articolo 136, possono essere trattati i dati di cui agli articoli 9 e 10 del Regolamento anche senza il consenso dell'interessato, purché nel rispetto delle regole deontologiche di cui all'articolo 139.
2. Ai trattamenti indicati nell'articolo 136 non si applicano le disposizioni relative:
a) alle misure di garanzia di cui all'articolo 2-*septies* e ai provvedimenti generali di cui all'articolo 2-*quaterdecies*;
b) al trasferimento dei dati all'estero, contenute nel Capo V del Regolamento.
3. In caso di diffusione o di comunicazione dei dati per le finalità di cui all'articolo 136 restano fermi i limiti del diritto di cronaca a tutela dei diritti di cui all'articolo 1, paragrafo 2, del Regolamento e all'articolo 1 del presente codice e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico. Possono essere trattati i dati personali relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico.";

d) all'articolo 138, comma 1, le parole "dell'articolo 7, comma 2, lettera a)" sono sostituite dalle seguenti: "dell'articolo 15, paragrafo 1, lettera g), del Regolamento";

e) la rubrica del Capo II è sostituita dalla seguente: "Regole deontologiche relative ad attività giornalistiche e ad altre manifestazioni del pensiero";

f) l'articolo 139 è sostituito dal seguente:

"Art. 139

(*Regole deontologiche relative ad attività giornalistiche*)

1. Il Garante promuove, ai sensi dell'articolo 2-*quater*, l'adozione da parte del Consiglio nazionale dell'ordine dei giornalisti di regole deontologiche relative al trattamento dei dati di cui all'articolo 136, che prevedono misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quanto riguarda quelli relativi alla salute e alla vita o all'orientamento sessuale. Le regole possono anche prevedere forme particolari per le informazioni di cui agli articoli 13 e 14 del Regolamento.
2. Nel periodo compreso tra la data di entrata in vigore del presente articolo e l'adozione delle regole deontologiche, ovvero successivamente, il Garante, in cooperazione con il Consiglio nazionale dell'ordine dei giornalisti, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto a recepire.
3. Le regole deontologiche o le modificazioni od integrazioni alle stesse che non sono adottate dal Consiglio entro sei mesi dalla proposta del Garante sono adottate in via sostitutiva dal Garante e sono efficaci sino a quando diviene efficace una diversa disciplina secondo la procedura di cooperazione.
4. Le regole deontologiche e le disposizioni di modificazione ed integrazione divengono efficaci quindici giorni dopo la loro pubblicazione nella Gazzetta Ufficiale ai sensi dell'articolo 2-*quater*.
5. In caso di violazione delle prescrizioni contenute nelle regole deontologiche, il Garante può vietare il trattamento ai sensi dell'articolo 58 del Regolamento.".

CAPO IV

Modifiche alla Parte III e agli allegati del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196

ART. 13

(*Modifiche alla Parte III, Titolo I, del decreto legislativo 30 giugno 2003, n. 196*)

1. Alla Parte III, Titolo I, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) prima del Capo I è inserito il seguente:

"CAPO 0.I

Alternatività delle forme di tutela

140-*bis*

(*Forme alternative di tutela*)

1. Qualora ritenga che i diritti di cui gode sulla base della normativa in materia di protezione dei dati personali siano stati violati, l'interessato può proporre reclamo al Garante o ricorso dinanzi all'autorità giudiziaria.
2. Il reclamo al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.
3. La presentazione del reclamo al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto, salvo quanto previsto dall'articolo 10, comma 4, del decreto legislativo 1 settembre 2011, n. 150.";

b) al capo I, le parole "Sezione I – Principi generali" sono soppresse;

c) l'articolo 141 è sostituito dal seguente:

"Art. 141
(*Reclamo al Garante*)

1. L'interessato può rivolgersi al Garante mediante reclamo ai sensi dell'articolo 77 del Regolamento.";

d) dopo l'articolo 141, le parole "Sezione II – Tutela amministrativa" sono soppresse;

e) l'articolo 142 è sostituito dal seguente:

"Art. 142
(*Proposizione del reclamo*)

1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare o del responsabile del trattamento, ove conosciuto.
2. Il reclamo è sottoscritto dall'interessato o, su mandato di questo, da un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati, con riguardo alla protezione dei dati personali.
3. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale mandato, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.
4. Il Garante predispone un modello per il reclamo, da pubblicare nel proprio sito istituzionale, di cui favorisce la disponibilità con strumenti elettronici.
5. Il Garante disciplina con proprio regolamento il procedimento relativo all'esame dei reclami, nonché modalità semplificate e termini abbreviati per la trattazione di reclami che abbiano ad oggetto la violazione degli articoli da 15 a 22 del Regolamento.";

f) l'articolo 143 è sostituito dal seguente:

"Art. 143
(*Decisione del reclamo*)

1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento può adottare i provvedimenti di cui all'articolo 58 del Regolamento nel rispetto delle disposizioni di cui all'articolo 56 dello stesso.
2. I provvedimenti di cui al comma 1 sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.
3. Il Garante decide il reclamo entro nove mesi dalla data di presentazione e, in ogni caso, entro tre mesi dalla predetta data informa l'interessato sullo stato del procedimento. In presenza di motivate esigenze istruttorie, che il Garante comunica all'interessato, il reclamo è deciso entro dodici mesi. In caso di attivazione del procedimento di cooperazione di cui all'articolo 60 del Regolamento, il termine rimane sospeso per la durata del predetto procedimento.
4. Avverso la decisione è ammesso ricorso giurisdizionale ai sensi dell'articolo 152.";

g) l'articolo 144 è sostituito dal seguente:

"Art. 144

(Segnalazioni)

1. Chiunque può rivolgere una segnalazione che il Garante può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento.
2. I provvedimenti del Garante di cui all'articolo 58 del Regolamento possono essere adottati anche d'ufficio.";

b) all'articolo 152, il comma 1 è sostituito dal seguente: "1. Tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelli comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché il diritto al risarcimento del danno ai sensi dell'articolo 82 del medesimo Regolamento, sono attribuite all'autorità giudiziaria ordinaria.".

ART. 14

(Modifiche alla Parte III, Titolo II, del decreto legislativo 30 giugno 2003, n. 196)

1. Alla Parte III, Titolo II, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) la rubrica è sostituita dalla seguente: "Autorità di controllo indipendente";

b) l'articolo 153 è sostituito dal seguente:

"Art. 153

(Garante per la protezione dei dati personali)

1. Il Garante è composto dal Collegio, che ne costituisce il vertice, e dall'Ufficio. Il Collegio è costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che risultano di comprovata esperienza nel settore della protezione dei dati personali, con particolare riferimento alle discipline giuridiche o dell'informatica.
2. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vice presidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.
3. L'incarico di presidente e quello di componente hanno durata settennale e non sono rinnovabili. Per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, anche non remunerata, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.
4. I membri del Collegio devono mantenere il segreto, sia durante sia successivamente alla cessazione dell'incarico, in merito alle informazioni riservate cui hanno avuto accesso nell'esecuzione dei propri compiti o nell'esercizio dei propri poteri.
5. All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.
6. Al presidente compete una indennità di funzione pari alla retribuzione in godimento al primo Presidente della Corte di cassazione, nei limiti previsti dalla legge per il trattamento economico annuo omnicomprensivo di chiunque riceva a carico delle finanze pubbliche emolumenti o retribuzioni nell'ambito di rapporti di lavoro dipendente o autonomo con pubbliche amministrazioni statali. Ai componenti compete una indennità pari ai due terzi di quella spettante al Presidente.

7. Alle dipendenze del Garante è posto l'Ufficio di cui all'articolo 155.
8. Il presidente, i componenti, il segretario generale e i dipendenti si astengono dal trattare, per i due anni successivi alla cessazione dell'incarico ovvero del servizio presso il Garante, procedimenti dinanzi al Garante, ivi compresa la presentazione per conto di terzi di reclami, richieste di parere o interpelli.";

c) l'articolo 154 è sostituito dal seguente:

"Art. 154
(*Compiti*)

1. Oltre a quanto previsto da specifiche disposizioni e dalla Sezione II del Capo VI del Regolamento, il Garante, ai sensi dell'articolo 57, paragrafo 1, lettera v), del Regolamento medesimo, anche di propria iniziativa e avvalendosi dell'Ufficio, in conformità alla disciplina vigente e nei confronti di uno o più titolari del trattamento, ha il compito di:

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico;

b) trattare i reclami presentati ai sensi del Regolamento, e delle disposizioni del presente codice, anche individuando con proprio regolamento modalità specifiche per la trattazione, nonché fissando annualmente le priorità delle questioni emergenti dai reclami che potranno essere istruite nel corso dell'anno di riferimento;

c) promuovere l'adozione di regole deontologiche, nei casi di cui all'articolo 2-*quater*;

d) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;

e) trasmettere la relazione, predisposta annualmente ai sensi dell'articolo 59 del Regolamento, al Parlamento e al Governo entro il 31 maggio dell'anno successivo a quello cui si riferisce;

f) assicurare la tutela dei diritti e delle libertà fondamentali degli individui dando idonea attuazione al Regolamento e al presente codice;

g) provvedere altresì all'espletamento dei compiti ad esso attribuiti dal diritto dell'Unione europea o dello Stato e svolgere le ulteriori funzioni previste dall'ordinamento.

2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da atti comunitari o dell'Unione europea e, in particolare:

a) dal regolamento (CE) n. 1987/2006 del Parlamento europeo e del Consiglio, del 20 dicembre 2006, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II) e Decisione 2007/533/GAI del Consiglio, del 12 giugno 2007, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen di seconda generazione (SIS II);

b) dal regolamento (UE) 2016/794 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI, 2009/936/GAI e 2009/968/GAI;

c) dal regolamento (UE) 2015/1525 del Parlamento Europeo e del Consiglio, del 9 settembre 2015, che modifica il regolamento (CE) n. 515/97 del Consiglio relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola e decisione 2009/917/GAI del Consiglio, del 30 novembre 2009, sull'uso dell'informatica nel settore doganale;

d) dal regolamento (CE) n. 603/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, che istituisce l'Eurodac per il confronto delle impronte digitali per l'efficace applicazione del regolamento (UE) n. 604/2013 che stabilisce i criteri e i meccanismi di determinazione dello Stato membro competente per l'esame di una domanda di protezione internazionale presentata in uno degli Stati membri da un cittadino di un paese terzo o da un apolide e per le richieste di

confronto con i dati Eurodac presentate dalle autorità di contrasto degli Stati membri e da Europol a fini di contrasto, e che modifica il regolamento (UE) n. 1077/2011 che istituisce un'agenzia europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia;

e) dal regolamento (CE) n. 767/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, concernente il sistema di informazione visti (VIS) e lo scambio di dati tra Stati membri sui visti per soggiorni di breve durata (regolamento VIS) e decisione n. 2008/633/GAI del Consiglio, del 23 giugno 2008, relativa all'accesso per la consultazione al sistema di informazione visti (VIS) da parte delle autorità designate degli Stati membri e di Europol ai fini della prevenzione, dell'individuazione e dell'investigazione di reati di terrorismo e altri reati gravi;

f) dal regolamento (CE) n. 1024/2012 del Parlamento europeo e del Consiglio, del 25 ottobre 2012, relativo alla cooperazione amministrativa attraverso il sistema di informazione del mercato interno e che abroga la decisione 2008/49/CE della Commissione (regolamento IMI) Testo rilevante ai fini del SEE;

g) dalle disposizioni di cui al capitolo IV della Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.

3. Per quanto non previsto dal Regolamento e dal presente codice, il Garante disciplina con proprio regolamento, ai sensi dell'articolo 156, comma 3, le modalità specifiche dei procedimenti relativi all'esercizio dei compiti e dei poteri ad esso attribuiti dal Regolamento e dal presente codice.

4. Il Garante collabora con altre autorità amministrative indipendenti nazionali nello svolgimento dei rispettivi compiti.

5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante, anche nei casi di cui agli articoli 36, paragrafo 4, del Regolamento, è reso nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.

6. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalità informatica è trasmessa, a cura della cancelleria, al Garante.

7. Il Garante non è competente per il controllo dei trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni.";

d) dopo l'articolo 154 sono aggiunti i seguenti:

"Art. 154-*bis*
(*Poteri*)

1. Oltre a quanto previsto da specifiche disposizioni, dalla Sezione II del Capo VI del Regolamento e dal presente codice, ai sensi dell'articolo 58, paragrafo 6, del Regolamento medesimo, il Garante ha il potere di:

a) adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento;

b) approvare le regole deontologiche di cui all'articolo 2-*quater*.

2. Il Garante può invitare rappresentanti di un'altra autorità amministrativa indipendente nazionale a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità amministrativa indipendente nazionale, prendendo parte alla discussione di argomenti di comune

interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità amministrativa indipendente nazionale.
3. Il Garante pubblica i propri provvedimenti sulla base di quanto previsto con atto di natura generale che disciplina anche la durata di tale pubblicazione, la pubblicità in *Gazzetta Ufficiale* e sul proprio sito internet istituzionale nonché i casi di oscuramento delle generalità degli interessati.

Articolo 154-*ter*
(*Potere di agire e rappresentanza in giudizio*)

1. Il Garante è legittimato ad agire in giudizio nei confronti del titolare o del responsabile del trattamento in caso di violazione delle disposizioni in materia di protezione dei dati personali.
2. Il Garante è rappresentato in giudizio dall'Avvocatura dello Stato, ai sensi dell'articolo 1 del regio decreto 30 ottobre 1933, n. 1611.
3. Nei casi di conflitto di interesse, il Garante, sentito l'Avvocato generale dello Stato, può stare in giudizio tramite propri funzionari iscritti nell'elenco speciale degli avvocati dipendenti di enti pubblici ovvero avvocati del libero foro.";

e) all'articolo 155, la rubrica è sostituita dalla seguente: "(*Ufficio del Garante*)";

f) l'articolo 156 è sostituito dal seguente:

"Art. 156
(*Ruolo organico e personale*)

1. All'Ufficio del Garante è preposto un segretario generale, nominato tra persone di elevata e comprovata qualificazione professionale rispetto al ruolo e agli obiettivi da conseguire, scelto anche tra i magistrati ordinari, amministrativi e contabili, gli avvocati dello Stato, i professori universitari di ruolo in materie giuridiche ed economiche, nonché i dirigenti di prima fascia dello Stato.
2. Il ruolo organico del personale dipendente è stabilito nel limite di centosessantadue unità. Al ruolo organico del Garante si accede esclusivamente mediante concorso pubblico. Nei casi in cui sia ritenuto utile al fine di garantire l'economicità e l'efficienza dell'azione amministrativa, nonché di favorire il reclutamento di personale con maggiore esperienza nell'ambito delle procedure concorsuali di cui al secondo periodo, il Garante può riservare una quota non superiore al cinquanta per cento dei posti banditi al personale di ruolo delle amministrazioni pubbliche che sia stato assunto per concorso pubblico e abbia maturato un'esperienza almeno triennale nel rispettivo ruolo organico. La disposizione di cui all'articolo 30 del decreto legislativo 30 marzo 2001, n. 165, si applica esclusivamente nell'ambito del personale di ruolo delle autorità amministrative indipendenti di cui all'articolo 22, comma 1, del decreto-legge 24 giugno 2014, n. 90, convertito, con modificazioni, dalla legge 11 agosto 2014, n.114.
3. Con propri regolamenti pubblicati nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce:
a) l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti e dei poteri di cui agli articoli 154, 154-bis, 160, nonché all'articolo 57, paragrafo 1, del Regolamento;
b) l'ordinamento delle carriere e le modalità di reclutamento del personale secondo i principi e le procedure di cui agli articoli 1, 35 e 36 del decreto legislativo n. 165 del 2001;
c) la ripartizione dell'organico tra le diverse aree e qualifiche;
d) il trattamento giuridico ed economico del personale, secondo i criteri previsti dalla legge 31 luglio 1997, n. 249, e, per gli incarichi dirigenziali, dagli articoli 19, comma 6, e 23-*bis* del decreto legislativo 30 marzo 2001, n. 165, tenuto conto delle specifiche esigenze funzionali e organizzative; al fine di adempiere ai nuovi e più onerosi compiti da svolgere anche in ambito

internazionale previsti dal Regolamento, al personale è attribuito il trattamento economico del personale dell'Autorità per le garanzie nelle comunicazioni;

e) la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato.

4. L'Ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, in numero non superiore, complessivamente, a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo.

5. In aggiunta al personale di ruolo, l'Ufficio può assumere dipendenti con contratto a tempo determinato o avvalersi di consulenti incaricati ai sensi dell'articolo 7, comma 6, del decreto legislativo n. 165 del 2001, in misura comunque non superiore a venti unità complessive. Resta in ogni caso fermo, per i contratti a tempo determinato, il rispetto dell'articolo 36 del decreto legislativo n. 165 del 2001.

6. Il personale addetto all'Ufficio del Garante ed i consulenti sono tenuti, sia durante che dopo il mandato, al segreto su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

7. Il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'articolo 158 e agli articoli 57, paragrafo 1, lettera h), 58, paragrafo 1, lettera b), e 62, del Regolamento riveste, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.

8. Le spese di funzionamento del Garante, in adempimento all'articolo 52, paragrafo 4, del Regolamento, ivi comprese quelle necessarie ad assicurare la sua partecipazione alle procedure di cooperazione e al meccanismo di coerenza introdotti dal Regolamento, nonché quelle connesse alle risorse umane, tecniche e finanziarie, ai locali e alle infrastrutture necessarie per l'effettivo adempimento dei suoi compiti e l'esercizio dei propri poteri, sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposita missione e programma di spesa del Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti. Il Garante può esigere dal titolare del trattamento il versamento di diritti di segreteria in relazione a particolari procedimenti.";

g) l'articolo 157 è sostituito dal seguente:

"Art. 157

(*Richiesta di informazioni e di esibizione di documenti*)

1. Nell'ambito dei poteri di cui all'articolo 58 del Regolamento, e per l'espletamento dei propri compiti, il Garante può richiedere al titolare, al responsabile, al rappresentante del titolare o del responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti anche con riferimento al contenuto di banche di dati.";

h) l'articolo 158 è sostituito dal seguente:

"Art. 158

(*Accertamenti*)

1. Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1, nonché quelli effettuati ai sensi dell'articolo 62 del Regolamento, sono eseguiti da personale dell'Ufficio, con la partecipazione, se del caso, di componenti o personale di autorità di controllo di altri Stati membri dell'Unione europea.

3. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali.
4. Gli accertamenti di cui ai commi 1 e 2, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.
5. Con le garanzie di cui al comma 4, gli accertamenti svolti nei luoghi di cui al medesimo comma possono altresì riguardare reti di comunicazione accessibili al pubblico, potendosi procedere all'acquisizione di dati e informazioni *on line*. A tal fine, viene redatto apposito verbale in contraddittorio con le parti ove l'accertamento venga effettuato presso il titolare del trattamento.";

i) all'articolo 159:

1) al comma 1, le parole "ai sensi dell'articolo 156, comma 8" sono sostituite dalle seguenti: "su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete";

2) al comma 3, dopo le parole "o il responsabile" sono inserite le seguenti: "o il rappresentante del titolare o del responsabile" e le parole "agli incaricati" sono sostituite dalle seguenti: "alle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile ai sensi dell'articolo 2-*terdecies*";

3) al comma 5, le parole "e telefax" sono soppresse;

l) l'articolo 160 è sostituito dal seguente:

"Art. 160
(*Particolari accertamenti*)

1. Per i trattamenti di dati personali di cui all'articolo 58, gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.
2. Se il trattamento non risulta conforme alle norme del Regolamento ovvero alle disposizioni di legge o di regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, se ciò non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato.
3. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere da personale specializzato tenuto al segreto su ciò di cui sono venuti a conoscenza in ordine a notizie che devono rimanere segrete. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal regolamento di cui all'articolo 156, comma 3, lettera a).
4. Per gli accertamenti di cui al comma 3 relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.
5. La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale.".

ART. 15

(Modifiche alla Parte III, Titolo III, del decreto legislativo 30 giugno 2003, n. 196)

1. Alla Parte III, Titolo III, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) l'articolo 166 è sostituito dal seguente:

"Art. 166

(Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori)

1. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 4, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-*quinquies*, comma 2, 2-*quaterdecies*, 92, comma 1, 93, comma 1, 123, comma 4, 124, 128, 129, comma 2, e 132-*ter*.
2. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-*ter*, 2-*quinquies*, comma 1, 2-*sexies*, 2-*septies*, comma 7, 2-*octies*, 2-*duodecies*, commi 1, 2, 3 e 4, 52, commi 1, 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110, comma 2, 111, 111-*bis*, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 4, 7 e 9, 131, 132, 132-*bis*, comma 2, 132-*quater*, 152, nonché delle misure di garanzia, delle regole deontologiche e delle modalità tecniche di cui rispettivamente agli articoli 2-*septies* e 2-*quater*.
3. Sono altresì soggette alla sanzione amministrativa di cui al comma 2 le violazioni di cui all'articolo 1, commi 9 e 10, della legge 11 gennaio 2018, n. 5.
4. Il Garante è l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58, paragrafo 2, del Regolamento, nonché ad irrogare le sanzioni di cui all'articolo 83 del medesimo Regolamento e di cui ai commi 1, 2 e 3.
5. Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 4 può essere avviato, nei confronti sia di soggetti privati, sia di autorità pubbliche ed organismi pubblici, a seguito di reclamo ai sensi dell'articolo 77 del Regolamento o di attività istruttoria d'iniziativa del Garante, nell'ambito dell'esercizio dei poteri d'indagine di cui all'articolo 58, paragrafo 1, del Regolamento, nonché in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante.
6. L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attività di cui al comma 5 configurino una o più violazioni indicate nel presente titolo e nell'articolo 83, paragrafi 4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 4, comunicando al titolare o al responsabile del trattamento le presunte violazioni.
7. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 6, il contravventore può inviare al Garante scritti difensivi o documenti e può chiedere di essere sentito dalla medesima autorità.
8. Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 4 si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689; nei medesimi casi può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante. I proventi delle sanzioni, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 8.
9. Entro il termine previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante e mediante il pagamento di un importo pari alla metà della sanzione irrogata.

10. Nel rispetto dell'articolo 58, paragrafo 4, del Regolamento, con proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica Italiana, il Garante definisce le modalità del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 4 ed i relativi termini.";

b) l'articolo 167 è sostituito dal seguente:

"Art. 167

(*Trattamento illecito di dati*)

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, è punito con la reclusione da sei mesi a un anno e sei mesi.
2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarre per sé o per altri profitto, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-*sexies* e 2-*octies*, o delle misure di garanzia ad esso relative ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-*quaterdecies* arreca nocumento all'interessato, è punito con la reclusione da uno a tre anni.
3. Salvo che il fatto costituisca più grave reato, la pena di cui al comma 2 si applica altresì a chiunque, al fine di trarre per sé o per altri profitto, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
4. Il Pubblico Ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attività di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al più tardi al termine dell'attività di accertamento delle violazioni delle disposizioni di cui al presente decreto.
6. Quando per lo stesso fatto è stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa è stata riscossa, la pena è diminuita.";

c) dopo l'articolo 167, sono inseriti i seguenti:

"Art. 167-*bis*

(*Comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone*)

1. Salvo che il fatto costituisca più grave reato, il titolare o il responsabile del trattamento o la persona designata a norma dell'articolo 2-*terdecies* che comunica o diffonde, al fine di trarre profitto per sé o altri, dati personali riferibili ad un rilevante numero di persone, in violazione degli articoli 2-*ter*, 2-*sexies* e 2-*octies*, è punito con la reclusione da uno a sei anni.
2. Salvo che il fatto costituisca più grave reato, il titolare o il responsabile del trattamento o la persona designata a norma dell'articolo 2-*terdecies* che, al fine trarne profitto per sé o altri, comunica o diffonde senza consenso dati personali riferibili a un rilevante numero di persone, è punito con la reclusione da uno a sei anni, quando il consenso dell'interessato è richiesto per le operazioni di comunicazione e di diffusione.
3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.

Art. 167-*ter*

(*Acquisizione fraudolenta di dati personali*)

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine trarne profitto per sé o altri, acquisisce con mezzi fraudolenti dati personali riferibili a un numero rilevante di persone è punito con la reclusione da uno a quattro anni.
2. Per il reato di cui al comma 1 si applicano i commi 4, 5 e 6 dell'articolo 167.";

d) l'articolo 168 è sostituito dal seguente:

"Art. 168

(*Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante*)

1. Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.
2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti.";

e) l'articolo 171 è sostituito dal seguente:

"Art. 171

(*Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori*)

1. La violazione delle disposizioni di cui agli articoli 4, commi 1 e 2, e 8 della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della medesima legge.";

f) all'articolo 172, comma 1, dopo le parole "pubblicazione della sentenza" sono aggiunte le seguenti: ", ai sensi dell'articolo 36, secondo e terzo comma, del codice penale".

ART. 16

(*Modifiche all'allegato A del decreto legislativo 30 giugno 2003, n. 196*)

1. L'allegato A è ridenominato: "Regole deontologiche".

CAPO V

Disposizioni processuali

ART. 17

(*Modifiche al decreto legislativo 1 settembre 2011, n. 150*)

1. L'articolo 10 del decreto legislativo 1 settembre 2011, n. 150, è sostituito dal seguente:

"ART. 10

(*Delle controversie in materia di applicazione delle disposizioni in materia di protezione dei dati personali*)

1. Le controversie previste dall'articolo 152 del decreto legislativo 30 giugno 2003, n. 196, sono regolate dal rito del lavoro, ove non diversamente disposto dal presente articolo.
2. Sono competenti, in via alternativa, il tribunale del luogo in cui il titolare del trattamento risiede o ha sede ovvero il tribunale del luogo di residenza dell'interessato.
3. Il ricorso avverso i provvedimenti del Garante per la protezione dei dati personali, ivi compresi quelli emessi a seguito di un reclamo dell'interessato, è proposto, a pena di inammissibilità, entro

trenta giorni dalla data di comunicazione del provvedimento ovvero entro sessanta giorni se il ricorrente risiede all'estero.
4. Decorso il termine previsto per la decisione del reclamo dall'articolo 143, comma 3, del decreto legislativo n. 196 del 2003, chi vi ha interesse può, entro trenta giorni dalla scadenza del predetto termine, ricorrere al Tribunale competente ai sensi del presente articolo. La disposizione di cui al primo periodo si applica anche qualora sia scaduto il termine trimestrale di cui all'articolo 143, comma 3, del decreto legislativo n. 196 del 2003 senza che l'interessato sia stato informato dello stato del procedimento.
5. L'interessato può dare mandato a un ente del terzo settore soggetto alla disciplina del decreto legislativo 3 luglio 2017, n. 117, che sia attivo nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di esercitare per suo conto l'azione, ferme le disposizioni in materia di patrocinio previste dal codice di procedura civile.
6. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.
7. L'efficacia esecutiva del provvedimento impugnato può essere sospesa secondo quanto previsto dall'articolo 5.
8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.
9. Nei casi in cui non sia parte in giudizio, il Garante può presentare osservazioni, da rendere per iscritto o in udienza, sulla controversia in corso con riferimento ai profili relativi alla protezione dei dati personali.
10. La sentenza che definisce il giudizio non è appellabile e può prescrivere le misure necessarie anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile dei dati, nonché il risarcimento del danno.".

Capo VI
Disposizioni transitorie, finali e finanziarie

ART. 18
(*Definizione agevolata delle violazioni in materia di protezione dei dati personali*)

1. In deroga all'articolo 16 della legge 24 novembre 1981, n. 689, per i procedimenti sanzionatori riguardanti le violazioni di cui agli articoli 161, 162, 162-bis, 162-ter, 163, 164, 164-bis, comma 2, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, e le violazioni delle misure di cui all'articolo 33 e 162, comma 2-bis, del medesimo codice, che, alla data del 21 marzo 2018, risultino non ancora definiti con l'adozione dell'ordinanza-ingiunzione, è ammesso il pagamento in misura ridotta di un somma pari a due quinti del minimo edittale. Fatti salvi i restanti atti del procedimento eventualmente già adottati, il pagamento potrà essere effettuato entro novanta giorni dalla data di entrata in vigore del presente decreto.
2. Decorsi i termini previsti dal comma 1, l'atto con il quale sono stati notificati gli estremi della violazione o l'atto di contestazione immediata di cui all'articolo 14 della legge 24 novembre 1981, n. 689, assumono il valore dell'ordinanza-ingiunzione di cui all'articolo 18 della predetta legge, senza obbligo di ulteriore notificazione, sempre che il contravventore non produca memorie difensive ai sensi del comma 4.
3. Nei casi di cui al comma 2, il contravventore è tenuto a corrispondere gli importi indicati negli atti di cui al primo periodo del predetto comma entro sessanta giorni dalla scadenza del termine previsto dal comma 1.

4. Entro il termine di cui al comma 3, il contravventore che non abbia provveduto al pagamento può produrre nuove memorie difensive. Il Garante per la protezione dei dati personali, esaminate tali memorie, dispone l'archiviazione degli atti comunicandola all'organo che ha redatto il rapporto o, in alternativa, adotta specifica ordinanza-ingiunzione con la quale determina la somma dovuta per la violazione e ne ingiunge il pagamento, insieme con le spese, all'autore della violazione ed alle persone che vi sono obbligate solidalmente.
5. L'entrata in vigore del presente decreto determina l'interruzione del termine di prescrizione del diritto a riscuotere le somme dovute a norma del presente articolo, di cui all'articolo 28 della legge 24 novembre 1981, n. 689.

ART. 19
(Trattazione di affari pregressi)

1. Entro il termine di sessanta giorni dalla data di pubblicazione nella Gazzetta Ufficiale dell'avviso di cui al comma 3, i soggetti che dichiarano il loro attuale interesse possono presentare al Garante per la protezione dei dati personali motivata richiesta di trattazione dei reclami, delle segnalazioni e delle richieste di verifica preliminare pervenuti entro la predetta data.
2. La richiesta di cui al comma 1 non riguarda i reclami e le segnalazioni di cui si è già esaurito l'esame o di cui il Garante per la protezione dei dati personali ha già esaminato nel corso del 2018 un motivato sollecito o una richiesta di trattazione, o per i quali il Garante medesimo è a conoscenza, anche a seguito di propria denuncia, che sui fatti oggetto di istanza è in corso un procedimento penale.
3. Entro quindici giorni dalla data di entrata in vigore del presente decreto il Garante per la protezione dei dati personali provvede a dare notizia di quanto previsto dai commi 1 e 2 mediante avviso pubblicato nel proprio sito istituzionale e trasmesso, altresì, all'Ufficio pubblicazioni leggi e decreti del Ministero della giustizia per la sua pubblicazione sulla Gazzetta Ufficiale della Repubblica italiana.
4. In caso di mancata presentazione di una richiesta di trattazione ai sensi del comma 1, e salvo quanto previsto dal comma 2, i relativi procedimenti di cui al comma 1 sono improcedibili.
5. I ricorsi pervenuti al Garante per la protezione dei dati personali e non definiti, neppure nelle forme del rigetto tacito, alla data di entrata in vigore del regolamento (UE) 2016/679 sono trattati come reclami ai sensi dell'articolo 77 del medesimo regolamento.

ART. 20
(Codici di deontologia e di buona condotta vigenti alla data di entrata in vigore del presente decreto)

1. Le disposizioni del codice di deontologia e di buona condotta di cui agli allegati A.5 e A.7 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, continuano a produrre effetti, sino alla definizione della procedura di approvazione cui alla lettera b), a condizione che si verifichino congiuntamente le seguenti condizioni:
a) entro sei mesi dalla data di entrata in vigore del presente decreto le associazioni e gli altri organismi rappresentanti le categorie interessate sottopongano all'approvazione del Garante per la protezione dei dati personali, a norma dell'articolo 40 del regolamento (UE) 2016/679, i codici di condotta elaborati a norma del paragrafo 2 del predetto articolo;
b) la procedura di approvazione si concluda entro sei mesi dalla sottoposizione del codice di condotta all'esame del Garante per la protezione dei dati personali.
2. Il mancato rispetto di uno dei termini di cui al comma 1, lettere a) e b) comporta la cessazione di efficacia delle disposizioni del codice di deontologia di cui al primo periodo a decorrere dalla scadenza del termine violato.

3. Le disposizioni contenute nei codici riportati negli allegati A.1, A.2, A.3, A.4 e A.6 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, continuano a produrre effetti fino alla pubblicazione delle disposizioni ai sensi del comma 4.
4. Entro novanta giorni dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali verifica la conformità al regolamento (UE) 2016/679 delle disposizioni di cui al comma 3. Le disposizioni ritenute compatibili, ridenominate regole deontologiche, sono pubblicate nella Gazzetta Ufficiale della Repubblica italiana e, con decreto del Ministro della giustizia, sono successivamente riportate nell'allegato A del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003.
5. Il Garante per la protezione dei dati personali promuove la revisione delle disposizioni dei codici di cui al comma 3 con le modalità di cui all'articolo 2-*quater* del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003.

ART. 21
(*Autorizzazioni generali del Garante per la protezione dei dati personali*)

1. Il Garante per la protezione dei dati personali, con provvedimento di carattere generale da adottarsi entro novanta giorni dalla data di entrata in vigore del presente decreto, individua le prescrizioni contenute nelle autorizzazioni generali già adottate, relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 4, nonché al capo IX del regolamento (UE) 2016/679, che risultano compatibili con le disposizioni del medesimo regolamento e del presente decreto e, ove occorra, provvede al loro aggiornamento. Il provvedimento di cui al presente comma è adottato all'esito di procedimento di consultazione pubblica.
2. Le autorizzazioni generali sottoposte a verifica a norma del comma 1 che siano state ritenute incompatibili con le disposizioni del regolamento (UE) 2016/679 richiamate al medesimo comma, ovvero in relazione alle quali non sia stato adottato il provvedimento di cui allo stesso comma, cessano di produrre effetti il novantesimo giorno successivo alla data di entrata in vigore del presente decreto.
3. Le autorizzazioni generali del Garante per la protezione dei dati personali adottate prima della data di entrata in vigore del presente decreto e relative a situazioni di trattamento diverse da quelle indicate al comma 1 cessano di produrre effetti alla predetta data.
4. Sino all'adozione delle regole deontologiche e delle misure di garanzia di cui agli articoli 2-*quater* e 2-*septies* del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, producono effetti, in quanto compatibili e per la corrispondente categoria di trattamenti, le autorizzazioni generali di cui al comma 1.
5. Le violazioni delle prescrizioni contenute nelle autorizzazioni generali di cui al presente articolo sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del regolamento (UE) 2016/679.

ART. 22
(*Altre disposizioni transitorie e finali*)

1. Il presente decreto e le disposizioni dell'ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra Stati membri ai sensi dell'articolo 1, paragrafo 3, del regolamento (UE) 2016/679.
2. A decorrere dal 25 maggio 2018 le espressioni "dati sensibili" e "dati giudiziari" utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite,

rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo regolamento.

3. Sino all'adozione dei corrispondenti provvedimenti generali di cui all'articolo 2-*quaterdecies* del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003 , i trattamenti di cui al medesimo articolo, già in corso alla data di entrata in vigore del presente decreto, possono proseguire qualora avvengano in base a espresse disposizioni di legge o regolamento o atti amministrativi generali, ovvero nel caso in cui siano stati sottoposti a verifica preliminare o autorizzazione del Garante per la protezione dei dati personali, che abbiano individuato misure e accorgimenti adeguati a garanzia dell'interessato.

4. A decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto.

5. A decorrere dal 25 maggio 2018, le disposizioni di cui ai commi 1022 e 1023 dell'articolo 1 della legge 27 dicembre 2017, n. 205 si applicano esclusivamente ai trattamenti di dati relativi al minore raccolti *on line*, nei limiti e con le modalità di cui all'articolo 36 del regolamento (UE) 2016/679.

6. Dalla data di entrata in vigore del presente decreto, i rinvii alle disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, abrogate dal presente decreto, contenuti in norme di legge e di regolamento, si intendono riferiti alle corrispondenti disposizioni del regolamento (UE) 2016/679 e a quelle introdotte o modificate dal presente decreto, in quanto compatibili.

7. All'articolo 1, comma 233, della legge 27 dicembre 2017, n. 205, dopo le parole "le modalità di restituzione" sono inserite le seguenti: "in forma aggregata".

8. Il registro dei trattamenti di cui all'articolo 37, comma 4, del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, cessa di essere alimentato a far data dal 25 maggio 2018. Da tale data e fino al 31 dicembre 2019, il registro resta accessibile a chiunque secondo le modalità stabilite nel suddetto articolo 37, comma 4, del decreto legislativo n. 196 del 2003.

9. Le disposizioni di legge o di regolamento che individuano il tipo di dati trattabili e le operazioni eseguibili al fine di autorizzare i trattamenti delle pubbliche amministrazioni per motivi di interesse pubblico rilevante trovano applicazione anche per i soggetti privati che trattano i dati per i medesimi motivi.

10. In considerazione delle esigenze di semplificazione delle micro, piccole e medie imprese, come definite dalla raccomandazione 2003/361/CE, il Garante per la protezione dei dati personali, nel rispetto delle disposizioni del regolamento (UE) 2016/679 e del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003 promuove, nelle linee guida adottate a norma dell'articolo 154-*bis* del medesimo codice, modalità semplificate di adempimento degli obblighi del titolare del trattamento.

11. La disposizione di cui all'articolo 160, comma 4, del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, limitatamente alla parte in cui ha riguardo ai dati coperti da segreto di Stato, si applica fino alla data di entrata in vigore della disciplina relativa alle modalità di opposizione al Garante per la protezione dei dati personali del segreto di Stato.

12. Le disposizioni del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, relative al trattamento di dati genetici, biometrici o relativi alla salute continuano a trovare applicazione, in quanto compatibili con il regolamento (UE) 2016/679, sino all'adozione delle corrispondenti misure di garanzia di cui all'articolo 2-*septies* del citato codice, introdotto dall'articolo 2, comma 1, lettera e) del presente decreto.

13. Sino alla data di entrata in vigore del decreto del Ministro della giustizia di cui all'articolo 2-octies, commi 2 e 6, del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, da adottarsi entro diciotto mesi dalla data di entrata in vigore del

presente decreto, il trattamento dei dati di cui all'articolo 10 del regolamento (UE) 2016/679 è consentito quando è effettuato in attuazione di protocolli di intesa per la prevenzione e il contrasto dei fenomeni di criminalità organizzata stipulati con il Ministero dell'interno o con le Prefetture - UTG, previo parere del Garante per la protezione dei dati personali, che specificano la tipologia dei dati trattati e delle operazioni eseguibili.

ART. 23
(*Disposizioni di coordinamento*)

1. A decorrere dalla data di entrata in vigore del presente decreto:

a) all'articolo 37, comma 2, alinea, del decreto legislativo adottato in attuazione dell'articolo 11 della legge 25 ottobre 2017, n. 163, il riferimento all'articolo 154 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, si intende effettuato agli articoli 154 e 154-*bis* del medesimo codice;

b) all'articolo 39, comma 1, del decreto legislativo adottato in attuazione dell'articolo 11 della legge 25 ottobre 2017, n. 163, il riferimento agli articoli 142 e 143 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003 si intende effettuato agli articoli 141, 142 e 143 del medesimo codice;

c) all'articolo 42 del decreto legislativo adottato in attuazione dell'articolo 11 della legge 25 ottobre 2017, n. 163, il riferimento all'articolo 165 del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, si intende effettuato all'articolo 166, comma 8, del medesimo codice;

d) all'articolo 45 del decreto legislativo adottato in attuazione dell'articolo 11 della legge 25 ottobre 2017, n. 163, il riferimento all'articolo 143, comma 1, lettera c), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, si intende effettuato all'articolo 58, paragrafo 2, lettera f), del regolamento (UE) 2016/679.

ART. 24
(*Applicabilità delle sanzioni amministrative alle violazioni anteriormente commesse*)

1. Le disposizioni del presente decreto che, mediante abrogazione, sostituiscono sanzioni penali con le sanzioni amministrative previste dal regolamento (UE) 2016/679 si applicano anche alle violazioni commesse anteriormente alla data di entrata in vigore del decreto stesso, sempre che il procedimento penale non sia stato definito con sentenza o con decreto divenuti irrevocabili.

2. Se i procedimenti penali per i reati depenalizzati dal presente decreto sono stati definiti, prima della sua entrata in vigore, con sentenza di condanna o decreto irrevocabili, il giudice dell'esecuzione revoca la sentenza o il decreto, dichiarando che il fatto non è previsto dalla legge come reato e adotta i provvedimenti conseguenti. Il giudice dell'esecuzione provvede con l'osservanza delle disposizioni dell'articolo 667, comma 4, del codice di procedura penale.

3. Ai fatti commessi prima della data di entrata in vigore del presente decreto non può essere applicata una sanzione amministrativa pecuniaria per un importo superiore al massimo della pena originariamente prevista o inflitta per il reato, tenuto conto del criterio di ragguaglio di cui all'articolo 135 del codice penale. A tali fatti non si applicano le sanzioni amministrative accessorie introdotte dal presente decreto, salvo che le stesse sostituiscano corrispondenti pene accessorie.

ART. 25

(Trasmissione degli atti all'autorità amministrativa)

1. Nei casi previsti dall'articolo 24, comma 1, l'autorità giudiziaria, entro novanta giorni dalla data di entrata in vigore del presente decreto, dispone la trasmissione all'autorità amministrativa competente degli atti dei procedimenti penali relativi ai reati trasformati in illeciti amministrativi, salvo che il reato risulti prescritto o estinto per altra causa alla medesima data.
2. Se l'azione penale non è stata ancora esercitata, la trasmissione degli atti è disposta direttamente dal pubblico ministero che, in caso di procedimento già iscritto, annota la trasmissione nel registro delle notizie di reato. Se il reato risulta estinto per qualsiasi causa, il pubblico ministero richiede l'archiviazione a norma del codice di procedura penale; la richiesta ed il decreto del giudice che la accoglie possono avere ad oggetto anche elenchi cumulativi di procedimenti.
3. Se l'azione penale è stata esercitata, il giudice pronuncia, ai sensi dell'articolo 129 del codice di procedura penale, sentenza inappellabile perché il fatto non è previsto dalla legge come reato, disponendo la trasmissione degli atti a norma del comma 1. Quando è stata pronunciata sentenza di condanna, il giudice dell'impugnazione, nel dichiarare che il fatto non è previsto dalla legge come reato, decide sull'impugnazione ai soli effetti delle disposizioni e dei capi della sentenza che concernono gli interessi civili.
4. L'autorità amministrativa notifica gli estremi della violazione agli interessati residenti nel territorio della Repubblica entro il termine di novanta giorni e a quelli residenti all'estero entro il termine di trecentosettanta giorni dalla ricezione degli atti.
5. Entro sessanta giorni dalla notificazione degli estremi della violazione l'interessato è ammesso al pagamento in misura ridotta, pari alla metà della sanzione, oltre alle spese del procedimento. Si applicano, in quanto compatibili, le disposizioni di cui all'articolo 16 della legge 24 novembre 1981, n. 689.
6. Il pagamento determina l'estinzione del procedimento.

ART. 26

(Disposizioni finanziarie)

1.Agli oneri derivanti dall' articolo 14, comma 1, lettera f), capoverso "Art. 156 Ruolo organico e personale", comma 3, lettera d) e dell'articolo 18, pari a euro 1.853.397 per il 2018, a euro 3.777.251 per il 2019, a euro 3.840.796 per il 2020, a euro 3.905.612 per il 2021, a euro 3.371.724 per il 2022, a euro 3.439.159 per il 2023, a euro 3.507.942 per il 2024, a euro 3.578.101 per il 2025, a euro 3.649.663 per il 2026, a euro 3.722.656 per il 2027 e a euro 3.797.109 annui a decorrere dal 2028, si provvede:
a) quanto a euro 1.853.397 per l'anno 2018 e ad euro 600.000 per ciascuno degli anni dal 2019 al 2021, mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 1025, della legge 27 dicembre 2017, n. 205;
b) quanto a euro 3.177.251 per il 2019, a euro 3.240.796 per il 2020, a euro 3.305.612 per il 2021, a euro 3.371.724 per il 2022, a euro 3.439.159 per il 2023, a euro 3.507.942 per il 2024, a euro 3.578.101 per il 2025, a euro 3.649.663 per il 2026, a euro 3.722.656 per il 2027 e a euro 3.797.109 annui a decorrere dal 2028, mediante corrispondente riduzione dell'autorizzazione di spesa di cui all'articolo 1, comma 1162, della legge 27 dicembre 2017, n. 205.
2.Dall'attuazione del presente decreto, ad esclusione dell'articolo 14, comma 1, lettera f), capoverso "Art. 156 Ruolo organico e personale", comma 3, lettera d) e dell'articolo 18, non devono derivare nuovi o maggiori oneri a carico della finanza pubblica. Le amministrazioni interessate provvedono agli adempimenti previsti con le risorse umane, strumentali e finanziarie disponibili a legislazione vigente.
3.Il Ministro dell'economia e delle finanze è autorizzato ad apportare le occorrenti variazioni di bilancio.

ART. 27
(*Abrogazioni*)

1. Sono abrogati i Titoli, Capi, Sezioni, articoli e allegati del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, di seguito elencati:

a) alla Parte I:
1) gli articoli 3, 4, 5 e 6;
2) il Titolo II, il Titolo III, il Titolo IV, il Titolo V, il Titolo VI e il Titolo VII;

b) alla Parte II:
1) il Capo I del Titolo I;
2) l'articolo 51;
3) i Capi III, IV e V del Titolo IV;
4) gli articoli 76, 81, 83 e 84;
5) il Capo III del Titolo V;
6) gli articoli 87, 88 e 89;
7) il Capo V del Titolo V;
8) gli articoli 91, 94, 95, 98, 112,117, 118 e 119;
9) i Capi II e III del Titolo X, il Titolo XI e il Titolo XIII;

c) alla Parte III:
1) la Sezione III del Capo I del Titolo I;
2) gli articoli 161, 162, 162-*bis*, 162-*ter*, 163, 164, 164-*bis*, 165, 169 e 170;
3) gli articoli 173, 174, 175, commi 1 e 2, 176, 177, 178 e 179;
4) il Capo II del Titolo IV;
5) gli articoli 184 e 185;

d) gli allegati B e C.

ART. 28
(*Entrata in vigore*)

1. Le disposizioni del presente decreto entrano in vigore il 25 maggio 2018.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. E' fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.