Gli e-book di EdilTecnico.it

Mario Petrulli

PRIVACY 2018: GUIDA PER I PROFESSIONISTI

Il nuovo regolamento europeo

MAGGIOLI EDITORE

Mario Petrulli

PRIVACY 2018: GUIDA PER I PROFESSIONISTI

IL NUOVO REGOLAMENTO EUROPEO

MAGGIOLI EDITORE

Mario Petrulli

Avvocato (www.studiolegalepetrulli.it), esperto in edilizia, urbanistica, appalti e diritto degli enti locali, consulente e formatore, autore di pubblicazioni per Maggioli Editore.

Codice 978.88.916.2915.9

Maggioli Editore è un marchio di Maggioli S.p.A.
Azienda con sistema qualità certificato ISO 9001: 2008

47822 Santarcangelo di Romagna (RN) • Via del Carpino, 8
Tel. 0541/628111 • Fax 0541/622595

www.maggiolieditore.it
e-mail: clienti.editore@maggioli.it

1. Indice

Prefazione

Il Regolamento UE 2016/679, pubblicato sulla Gazzetta UE lo scorso 4 maggio 2016, rappresenta la conclusione di un lungo percorso normativo che mira ad improntare un adeguato sistema di misure a tutela dei dati personali, con conseguente individuazione di una serie di adempimenti connessi, uniforme per tutti i Paesi dell'Unione. Dalla sua entrata in vigore (il 24 maggio 2016, ossia venti giorni dopo la pubblicazione sulla Gazzetta UE), i Paesi membri hanno avuto due anni di tempo per allineare le normative interne al Regolamento, le cui disposizioni si applicano in tutto il territorio UE a partire dal 25 maggio 2018.

Il presente *e-book* ha lo scopo di fornire ai professionisti, obbligati anche loro al rispetto delle nuove disposizioni, uno strumento agile che consenta di avere una rapida visione delle novità e degli adempimenti a cui sono chiamati, sia allo scopo di applicare correttamente le disposizioni, sia per evitare le sanzioni.

Saranno brevemente analizzate le principali norme di interesse, gli adempimenti richiesti, le possibili sanzioni; l'ultimo capitolo offrirà uno schema per la valutazione dei rischi nel trattamento dei dati e le misure di sicurezza da adottare, mentre in appendice abbiamo ritenuto opportuno inserire alcuni documenti presenti sul sito del Garante della privacy sulla figura del responsabile della protezione dei dati.

In appendice troverete le "Linee guida sui responsabilidella protezione dati" e le nuove FAQ del Garante della Privacy.

1. Le definizioni

1.1. La nozione di dato personale

Nell'analisi del nuovo Regolamento non si può non partire dalla nozione di dato personale: secondo quanto espressamente previsto dall'art. 4, è tale 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.

È facile verificare che la norma si sofferma sul concetto di identificabilità ma non chiarisce quanto una persona fisica è identificata. Evidentemente, l'identificazione richiede elementi che descrivano una persona in modo tale da poterla distinguere da qualsiasi altro soggetto e riconoscere come individuo, come nel caso tipico del nome e cognome o in quello della carica ricoperta quando la stessa ha rilievo pubblico (ad esempio, il Presidente della Repubblica Italiana).

Sovente ai fini dell'identificazione di una persona possono accompagnarsi altri dati ed informazioni: si pensi, ad esempio, alla data e al luogo di nascita, ai dati biometrici (impronte digitali e scansioni dell'iride), alle tracce informatiche (indirizzi internet).

Ragionando *a contrario*, il Regolamento non trova applicazione nel caso di persona non identifica né identificabile, come accade nel caso di informazioni anonime, anche per finalità statistiche o di ricerca.

1.2. Il trattamento dei dati

Sempre l'art. 4 del Regolamento chiarisce cose deve intendersi per "*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.

Tre sono le modalità con cui il trattamento può avvenire: cartacea (o analogica), informatica (o digitale) e mista.

1.3. La limitazione di trattamento

È il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro. In altri termini, l'interessato può modificare o revocare il proprio consenso al trattamento nel tempo: ciò avviene attraverso l'inaccessibilità di dati, il loro trasferimento, la loro rimozione o la selezione degli stessi.

Quando il titolare proceda a limitare il trattamento, tali dati personali sono trattati solo per la conservazione, e ulteriori trattamenti saranno possibili soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.

1.4. La profilazione

È 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 (si pensi, ad esempio, alla profilazione per finalità di *marketing*).

A scopo protettivo, chiunque ha il diritto di non essere sottoposto a una misura che produca effetti giuridici o significativamente incida sulla sua persona, basata unicamente su un trattamento automatizzato destinato a valutare taluni aspetti della sua personalità o ad analizzarne o prevederne in particolare il rendimento professionale, la situazione economica, l'ubicazione, lo stato di salute, le preferenze personali, l'affidabilità o il comportamento.

Se i dati sono trattati in base a un contratto o con il consenso dell'interessato, o nel rispetto di una disposizione di legge, devono essere chiaramente previste e indicate le garanzie a tutela dei suoi legittimi interessi.

La profilazione, di norma, prevede due diverse attività:
- l'acquisizione di dati personali di una persona fisica da far confluire in un archivio;
- l'elaborazione dei dati raccolti (prima attività) al fine di inserire la singola persona fisica in un cluster comprendente soggetti che hanno determinate caratteristiche (ad esempio, stessa tendenza a consumare determinati beni o a richiedere determinati servizi).

1.5. La pseudonimizzazione

È il trattamento dei dati personali in modo tale che gli stessi 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.

Caratteristiche della pseudonimizzazione sono:
- la possibilità di risalire alla identità della persona fisica a cui i dati si riferiscono.
- la non identificabilità diretta del soggetto interessato;
- rappresentare una misura di sicurezza;

- potersi accompagnare ad altre misure di protezione dei dati (ad esempio, la crittografia);
- consentire al titolare che effettua il trattamento la possibilità di risalire alla persona interessata (cd informazioni aggiuntive) previa indicazione delle persone autorizzate all'interno della stessa organizzazione.

1.6. L'archivio

È 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.

In sintesi, è una raccolta organizzata e sistematica di documenti di diversa natura (atti, scritture private e altri documenti originali) prodotti e/o acquisiti da un soggetto pubblico o privato (quindi, anche da un professionista), da enti, istituzioni, famiglie o persone, nel normale esercizio delle proprie funzioni, durante lo svolgimento della propria attività, custoditi in funzione del loro valore di attestazione e informazione. Esempi tipici di archivi nel caso dei professionisti sono l'elenco clienti, l'elenco fornitori, l'elenco dei dipendenti.

1.7. Il titolare del trattamento

È 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; sul titolare del trattamento incide il potere/dovere di stabilire oltre che le finalità ed i mezzi del trattamento dei dati personali, anche le misure di sicurezza da adottare, che varieranno, almeno in parte, a seconda della:

- tipologia di dati personali trattati (comuni, sensibili, giudiziari);
- modalità di trattamento (cartacea, informatica, mista);
- ambito di diffusione (interno alla UE oppure anche in Paesi esterni alla UE).

Eccezionalmente, laddove le finalità e i mezzi del trattamento sono stabiliti dal diritto dell'UE o degli Stati membri, anche il titolare del trattamento (o i criteri specifici applicabili alla sua designazione) può essere individuato dallo stesso diritto dell'Unione o degli Stati membri.

1.8. Il responsabile del trattamento

È la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, secondo le direttive fornite da quest'ultimo; di norma è un dipendente.

1.9. Il destinatario

È 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.

Le Autorità pubbliche che ricevono suddette comunicazioni nell'ambito di una indagine regolamentata dalla normativa comunitaria o di un Paese membro non si considerano destinatari, sebbene il trattamento – da parte loro – dei dati debba essere conforme ai principi esplicitati nel Regolamento.

1.10. Il terzo

È 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.

1.11. Il consenso dell'interessato

Si intende 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.

Il consenso di caratterizza per le seguenti peculiarità:
- va richiesto all'interessato, prima della raccolta dei dati, salvo particolari situazioni in cui il Legislatore ammette la possibilità di richiedere e rilasciare il consenso da parte di un soggetto diverso da quello cui si riferiscono le informazioni;
- deve essere informato e la informativa costituisce condizione di validità del consenso stesso;
- deve essere espresso e non può essere implicito;
- deve essere inequivocabile e specifico;
- può riguardare anche una o più parti delle operazioni di trattamento.

È lecito trattare i dati sensibili se "*il trattamento riguarda dati resi manifestamente pubblici dall'interessato*"; così come per il trattamento di dati di natura sanitaria, non servirà più il consenso dell'interessato, se trattati da personale sanitario tenuto al rispetto del segreto professionale.

1.12. Violazione dei dati personali

È 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. Il titolare del trattamento deve adottare determinati adempimenti in caso di violazione delle misure di sicurezza.

1.13. Dati genetici

Sono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite successivamente alla nascita 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.

1.14. Dati biometrici

Sono 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.

I dati biometrici sono, per loro natura, direttamente, univocamente e in modo tendenzialmente stabile nel tempo, collegati all'individuo e denotano la profonda relazione tra corpo, comportamento e identità della persona, richiedendo particolari cautele in caso di loro trattamento. L'adozione di sistemi biometrici, in ragione della tecnica prescelta, del contesto di utilizzazione, del numero e della tipologia di potenziali interessati, delle modalità e delle finalità del trattamento, può comportare quindi rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato.

1.15. Dati relativi alla salute

Sono 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. Si tratta di dati sensibili.

1.16. Stabilimento principale

Per quanto riguarda il titolare del trattamento con stabilimenti in più di uno Stato membro, è 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.

Con riferimento al responsabile del trattamento con stabilimenti in più di uno Stato membro, è 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 Regolamento.

1.17. Il rappresentante

È la persona fisica o giuridica stabilita nell'Unione che, designata per iscritto dal titolare del trattamento o dal responsabile del trattamento, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del Regolamento; la figura deve avere essere stabilita all'interno dell'Unione Europea. La nomina del rappresentante è obbligatoria quando il titolare o il responsabile risiedono al di fuori della UE.

1.18. Impresa

Si intende 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.

1.19. Il gruppo imprenditoriale

È un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

1.20. Norme vincolanti d'impresa

Sono 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.

1.21. Autorità di controllo

È l'Autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 5. Oltre a svolgere un compito di controllo, ha anche la funzione di monitorare l'applicazione del Regolamento ed agevolare la libera circolazione dei dati personali all'interno della UE.

1.22. Autorità di controllo interessata

È un'Autorità di controllo interessata dal trattamento di dati personali in quanto:
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;
c) un reclamo è stato proposto a tale Autorità di controllo.

Questa definizione ha, sostanzialmente, lo scopo di consentire di individuare l'Autorità competente partendo dal trattamento dei dati personali e tenendo conto dello "stabilimento", ove i dati vengono trattati.

1.23. Trattamento transfrontaliero

Consiste nel 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 nel 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.

1.24. Obiezione pertinente e motivata

È un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del Regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al 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.

Si tratta dell'espressione di un parere relativa alla fattispecie disciplinata attraverso l'art. 60 del Regolamento, il quale prevede che nell'attività di cooperazione tra l'Autorità di controllo capofila e le altre Autorità di controllo interessate, una di queste può sollevare un'obiezione pertinente e motivata al "progetto di decisione".

1.25. Servizio della società dell'informazione

È il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, secondo cui per «servizio» si intende qualsiasi servizio della società dell›informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende per:

- a distanza: un servizio fornito senza la presenza simultanea delle parti;
- per via elettronica: un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici o altri mezzi elettromagnetici;
- a richiesta individuale di un destinatario di servizi: un servizio fornito mediante trasmissione di dati su richiesta individuale.

1.26. Organizzazione internazionale

È 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.

2. I principi fondamentali del regolamento

2.1. Premessa

L'art. 5[1] del Regolamento individua i numerosi principi fondamentali in materia di *privacy*. Nel prosieguo della nostra breve trattazione andremo ad illustrarli singolarmente.

2.2. I principi di liceità, correttezza e trasparenza

Il trattamento deve essere, in primo luogo, lecito: lo è quando l'interessato ha espresso il suo consenso al trattamento o se esso è necessario per l'esecuzione di un contratto, l'adempimento di un obbligo legale, la salvaguardia di interessi vitali per una persona fisica, l'esecuzione da parte del titolare di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri o il perseguimento di un legittimo interesse ove non prevalgano i diritti e le libertà del soggetto interessato.

Il trattamento, inoltre, deve essere corretto e trasparente: ciò significa che le informazioni che il titolare del trattamento deve fornire all'interessato con riferimento alle modalità di trattamento dei suoi dati, devono sempre essere rese in forma chiara, intelligibile, facilmente accessibile, con un linguaggio semplice e comprensibile.

1. **Art. 5 Principi applicabili al trattamento dei dati personali**
1. I dati personali sono: 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»).

2.3. Il principio di finalità

In ossequio a tale principio, l'informativa deve illustrare in maniera esauriente le finalità per le quali saranno trattati i dati personali; dette finalità devono essere:
- determinate, ossia ben definite;
- esplicite, ossia chiare nel loro contenuto preciso;
- legittime, ossia conformi alla legislazione in materia.

2.4. Il principio di minimizzazione dei dati

In ossequio a tale principio, i dati raccolti devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.

2.5. I principi dell'esattezza e dell'aggiornamento

I dati devono essere esatti, ossia coerenti con la realtà a cui si riferiscono e tempestivamente cancellati e/o rettificati. Inoltre, devono essere aggiornati nel tempo, laddove necessario.

2.6. Il principio della conservazione

I dati devono essere 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. È consentito un periodo di conservazione maggiore esclusivamente per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, sempre con adeguate misure tecniche ed organizzative.

2.7. I principi di sicurezza, integrità e riservatezza

Prima del trattamento, i dati devono trovare applicazione misure di sicurezza tecniche ed organizzative; tali misure devono consentire anche la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

2.8. La responsabilizzazione del titolare del trattamento

Il principio di *accountability* (responsabilità) in capo al titolare del trattamento obbligo quest'ultimo ad un approccio sostanziale e non meramente formalistico agli adempimenti richiesti. È suo preciso compito:
- individuare ed adottare politiche e scelte aziendali, misure tecniche ed organizzative idonee a rendete rendere effettiva la protezione dei dati personali;
- dimostrarne la reale applicazione.

I due strumenti operativi di cui il titolare ed il responsabile possono avvalersi sono:
- i codici di condotta, redatti dalle associazioni di categoria e presentati alle Autorità di controllo per l'approvazione, che potranno contenere ulteriori indicazioni rispetto a quelle già contenute nel Regolamento;

- la certificazione**,** ossia "*L'atto mediante il quale la terza parte indipendente dichiara che con ragionevole attendibilità un prodotto, processo o servizio è conforme ad una specifica norma o ad altro documento normativo*" (UNI CEI 70001). Attraverso tale strumento, rilasciato a seguito di verifica ispettiva, l'impresa dimostra la rispondenza delle procedure al paradigma previsto dal Regolamento. Ai fini di una corretta valutazione dei rischi, della mappatura dei dati e dei trattamenti sembra opportuno rifarsi agli standard ISO 27001[2].

Il principio di responsabilizzazione deve essere attuato anche nella scelta del responsabile del trattamento, per cui il titolare del trattamento deve dimostrare che questi siano dotati "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".

Ai fini della piena realizzazione del principio di *accountability*, inoltre, il titolare o il responsabile del trattamento devono "tenere un registro delle attività di trattamento", con obbligo di messa a disposizione dell'Autorità di controllo che ne faccia richiesta.

Il Regolamento prevede diverse ipotesi di responsabilità del titolare del trattamento:
- ex art. 5, lett. f), i dati personali devono essere trattati sotto la responsabilità del titolare del trattamento, che assicura e comprova, per ciascuna operazione, la conformità al Regolamento;
- ex art. 22, comma 1, il titolare del trattamento adotta politiche e attua misure adeguate per garantire di essere in grado di dimostrare che il trattamento dei dati personali è conforme al Regolamento;
- ex art. 22, comma 3, il titolare del trattamento mette in atto meccanismi per assicurare la verifica dell'efficacia delle misure di sicurezza di cui all'art. 30; qualora ciò sia proporzionato, la verifica è effettuata da revisori interni o esterni indipendenti.

Nessuna responsabilizzazione può essere efficace senza le sanzioni in caso di inosservanza: ed infatti, il Regolamento prevede che il titolare e il responsabile che violano le prescrizioni di cui all'art. 5 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. a)).

2.9. La liceità del trattamento

Secondo quanto previsto dall'art. 6[3] del Regolamento, il trattamento dei dati personali è considerarsi lecito se si verificava almeno una delle seguenti condizioni:

2. È una norma internazionale che definisce i requisiti per impostare e gestire un sistema di gestione della sicurezza delle informazioni (SGSI o ISMS, Information Security Management System).
3. **Art. 6 Liceità del trattamento**
1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; 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; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; 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; 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. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle Autorità pubbliche nell'esecuzione dei loro compiti.

a) espressione del consenso, esplicito e specifico; il titolare del trattamento di deve prevedere una dichiarazione di consenso predisposta in una forma comprensibile e facilmente accessibile, che usi un linguaggio semplice e chiaro e non contenga clausole abusive;
b) esecuzione di un contratto di cui l'interessato sia parte;
c) adempimento di un obbligo legale in capo al titolare;
d) salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
e) trattamento necessario per l'esecuzione di un compito di interesse pubblico (si pensi, ad esempio, alla salute pubblica, all'ordine pubblico, alle emergenze umanitarie, alle catastrofi, ecc.);
f) trattamento reso necessario dalla esigenza di tutelare un interesse legittimo del titolare o di un terzo, sempre che non sussista un interesse o un diritto prevalente dell'interessato: si pensi ad esempio, all'esistenza di un rapporto di dipendenza oppure di clientela.

Se il trattamento avviene per un fine diverso da quello per il quale si è acquisito il consenso occorre verificare:
a) l'esistenza di un eventuale nesso tra la finalità di trattamento per la quale si è acquisito il consenso e la nuova finalità;
b) la relazione esistente tra il titolare e l'interessato;
c) la natura dei dati personali trattati (se comuni o sensibili);
d) le conseguenze che potrebbero derivare, in capo all'interessato, dal nuovo trattamento;
e) la presenza di misure atte ad impedire la identificazione dell'interessato (cifratura o pseudonimizzazione).

Il Regolamento prevede che il titolare e il responsabile che violano le prescrizioni di cui all'art. 6 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. a)).

---

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

2.10. Condizioni per il consenso

Come indicato dall'art. 7[4], il titolare del trattamento deve essere sempre in grado di dimostrare che l'interessato ha prestato il consenso, inteso quale è una libera ed esplicita manifestazione di volontà dell'interessato in relazione all'utilizzo dei propri dati personali da parte di terzi che in qualità di titolari del trattamento dei dati ne decidono le finalità e modalità: l'esempio tipico è quello della firma su moduli o documenti redatti e sottoscritti appositamente.

Può capitare che il consenso sia prestato all'interno di dichiarazioni scritte riguardante anche altre questioni: in tal caso, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

Il consenso è revocabile in qualsiasi momento, con la medesima facilità con cui è stato concesso ed il diritto di revoca deve essere oggetto di precisa informativa a favore dell'interessato.

Come già ricordato nel precedente capitolo, il consenso:
- va richiesto all'interessato prima della raccolta dei dati, salvo particolari situazioni in cui il Legislatore ammette la possibilità di richiedere e rilasciare il consenso da parte di un soggetto diverso da quello cui si riferiscono le informazioni;
- deve essere informato e la informativa costituisce condizione di validità del consenso stesso;
- deve essere espresso e non implicito e può riguardare anche una o più parti delle operazioni di trattamento.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 7 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. (art. 83, par. 5, lett. a)).

2.11. Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione

L'art. 8[5] disciplina l'ipotesi in cui il minore ricorra ad uno dei servizi offerti dalla società dell'informazione (esempio tipico sono i *social network*), prevedendo che il minore possa prestare il

---

4. **Art. 7 Condizioni per il consenso**
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.
5. **Art. 8 Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione**
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.

consenso se ha compiuto 16 anni (salva la possibilità che ogni Paese disciplina legislativamente un'età inferiore, ma almeno pari a 13 anni); diversamente, il consenso può essere rilasciato da chi esercita la potestà sul minore.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 8 sono soggetti a sanzioni amministrative pecuniarie fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, lett. a)).

2.12. Il trattamento di categorie particolari di dati personali

L'art. 9[6] vieta il trattamento dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati

---

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.

6. **Art. 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.
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi: 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; 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; 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; 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

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, a meno che non vi sia una delle seguenti situazioni eccezionali:

a) presenza di un consenso esplicito da parte dell'interessato, salva diversa legislazione nazionale;
b) in materia di rapporti di lavoro, se vige una norma comunitaria o statale oppure un contratto collettivo che disciplina – nel rispetto delle garanzie per l'interessato – obblighi e diritti del titolare;
c) quando è in gioco la vita dell'interessato o di un terzo;
d) per i trattamenti posti in essere da associazioni, fondazioni, ecc. nei riguardi di associati o ex associati e sia svolto sempre per le finalità legate alla associazione/organismo e purché i dati personali non siano comunicati all'esterno senza il previo consenso dell'interessato;
e) l'interessato ha reso pubblici i propri dati, di cui si effettua il trattamento;
f) per fare valere un diritto in sede giudiziaria;
g) quando il trattamento è originato dalla necessità di tutelare un interesse pubblico, sancito dalla normativa comunitaria o statale e sempre nel rispetto dei diritti fondamentali dell'interessato;
h) il trattamento dei dati si svolge nell'esercizio di un'attività di medicina preventiva o del lavoro;
i) quando il trattamento è reso necessario dall'esigenza di tutelare un pubblico interesse che attiene alla salute pubblica;
j) quando il trattamento è reso necessario dall'esigenza di tutelare un pubblico interesse che attiene alla ricerca scientifica o storica, o a fini statistici.

Il trattamento di dati personali per finalità di medicina preventiva o del lavoro può essere svolto da un professionista, tenuto al segreto professionale.

Per quanto concerne i dati genetici, biometrici o relativi alla salute, i singoli Stati membri possono prevedere che il trattamento sia soggetto ad ulteriori condizioni.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 9 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. a)).

2.13. Trattamento dei dati personali relativi a condanne penali e reati

L'art. 10[7] del Regolamento dispone che il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'Autorità pubblica oppure 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.

---

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.
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.

7. **Art. 10 Trattamento dei dati personali relativi a condanne o 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.

Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'Autorità pubblica, in ragione della delicatezza dei dati.

2.14. Trattamento che non richiede l'identificazione

L'art. 11[8] precisa che il titolare del trattamento non è obbligato ad acquisire ulteriori informazioni per identificare l'interessato al solo fine di rispettare una disposizione del Regolamento.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 11 sono soggetti a sanzioni amministrative pecuniarie fino a 10 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, lett. a)).

8. **Art. 11 Trattamento che non richiede l'identificazione**
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.

3. I diritti dell'interessato

3.1. Trasparenza e modalità

L'art. 12[1] introduce l'obbligo in capo al titolare del trattamento di fornire all'interessato le informazioni 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, quali quelli elettronici. La forma orale è utilizzabile se richiesto dall'interessato, purché sia comprovata con altri mezzi l'identità dell'interessato.

1. **Art. 12 Trasparenza e modalità**
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.

Il titolare deve agevolare le richieste di accesso[2] provenienti dall'interessato: fondamentale, a tal fine, è la predisposizione di un regolamento interno all'ente o all'impresa o allo studio professionale che possa disciplinare la materia. Allo stesso modo, il titolare è obbligato ad eseguire la rettifica o la cancellazione dei dati, nonché garantire all'interessato l'esercizio del diritto di opposizione.

Le risposte alla richieste di accesso devono essere tempestive e, comunque, riscontrate entro 30 giorni; è possibile la proroga di due mesi tenuto conto della complessità e del numero delle richieste.

Se non ottempera alla richiesta dell'interessato, il titolare deve comunicarglielo entro 30 giorni, indicandogli anche le modalità per proporre, eventualmente, reclamo all'Autorità di controllo o ricorso giurisdizionale.

Le informazioni richieste vengono rilasciate gratuitamente a meno che nel caso di manifesta infondatezza delle stesse o loro ripetitività può essere addebitato all'interessato un rimborso delle spese sostenute: l'onere di dimostrare l'infondatezza della richiesta o la ripetitività o l'eccessività incombe sul titolare. Il rilascio delle informazioni può avvenire anche attraverso la predisposizione di icone, anche standardizzate, tali da rendere più facilmente visibili, intelligibili e leggibili le informazioni stesse.

In fase di identificazione del richiedente, il titolare, se persistono dubbi sulla sua identità, può richiedergli ulteriori informazioni in merito.

Per quanto attiene le sanzioni, il titolare ed il responsabile che violano le prescrizioni di cui all'articolo 12 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. (art. 83, par. 5, lett. a)).

3.2. Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato

L'art. 13[3] indica le informazioni che il titolare del trattamento deve fornire all'interessato in caso di raccolta dei dati presso quest'ultimo:

2. Trattasi, evidentemente, di diritto di accesso diverso da quello previsto dalla Legge n. 241/90 e dalle due forme di accesso civico previste dal Decreto Legislativo n. 97/2016.

3. **Art. 13 Informazione da fornire qualora i dati personali siano raccolti presso l'interessato**
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

a) identità e dati di contatto del titolare;
b) dati di contatti del responsabile;
c) identità e dati di contatto del rappresentante del titolare, se individuato;
d) le finalità del trattamento, con relativo riferimento normativo;
e) se il trattamento è svolto per l'esercizio di un legittimo interesse del titolare o di un terzo, l'individuazione di tale legittimo interesse;
f) gli eventuali destinatari dei dati personali;
g) l'eventuale intenzione di trasferire i dati trattati in un Paese terzo e la presenza o l'assenza di una decisione di adeguatezza della Commissione;
h) il periodo di conservazione;
i) i diritti in capo all'interessato, compresi quello di revoca del consenso e di reclamo ad una Autorità di controllo;
j) se la comunicazione dei dati è legata ad un obbligo di natura contrattuale o legale;
k) se al trattamento è connesso un processo decisionale automatizzato.

Nel caso in cui il titolare intenda continuare il trattamento dei dati per una finalità diversa da quella per la quale ha acquisito il consenso, deve fornire idonea informativa all'interessato.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 13 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

3.3. Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

L'art. 14[4] disciplina l'ipotesi in cui il trattamento di dati personali effettuato senza che gli stessi siano stati ottenuti presso l'interessato; in tal caso il titolare deve fornire le seguenti informazioni entro un termine ragionevole, comunque non superiore ai 30 giorni:

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.

4. **Art. 14 Informazioni da fornire qualora i dati personali non siano stati forniti presso l'interessato**
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

a) identità e dati di contatto del titolare e del responsabile (ed eventualmente del rappresentante, qualora nominato);
b) le finalità del trattamento unitamente al riferimento normativo che lo rende lecito; le categorie di dati personali che si trattano (comuni, sensibili, giudiziari);
c) se è prevista la comunicazione degli stessi, vanno indicati i destinatari o le categorie dei destinatari;
d) se è previsto il trasferimento al di fuori della UE e se c'è o meno una decisione di adeguatezza della Commissione;
e) il tempo di conservazione;
f) se il trattamento è necessario per tutelare un legittimo interesse del titolare o di terzi, quale è il legittimo interesse che si persegue;
g) le modalità di esercizio del diritto di accesso, rettifica e cancellazione dei dati;
h) la possibilità, in capo all'interessato, del diritto di revoca del consenso;
i) il diritto dell'interessato a proporre reclamo ad una Autorità di controllo;
j) la fonte di acquisizione dei dati;
k) se il titolare ha posto in essere un processo automatizzato e se questo comporta anche la profilazione.

Se i dati personali sono oggetto di comunicazione con l'interessato, tali informazioni gli devono essere fornite entro la prima comunicazione; se, invece, è prevista la comunicazione ad una terza persona, allora l'informativa all'interessato gli deve essere resa "*non oltre la prima comunicazione dei dati personali*".

Suddette informazioni all'interessato devono essergli reiterate qualora il titolare intenda procedere ad un trattamento degli stessi dati ma per una finalità diversa dalla prima.

---

dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; 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; il diritto di proporre reclamo a un'Autorità di controllo; la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; 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 la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; 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: 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; 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 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: l'interessato dispone già delle informazioni; 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; 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 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.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 14 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

3.4. Diritto di accesso dell'interessato

L'art. 15[5] disciplina il diritto di accesso dell'interessato ai propri dati.

Egli 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 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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 relative al trasferimento.

---

5. **Art. 15 Diritto di accesso dell'interessato**
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.

Il titolare del trattamento fornisce gratuitamente una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare 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.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Ovviamente il titolare deve verificare l'identità dell'interessato che richiede l'accesso, onde evitare che terzi possano avere informazioni per le quali non hanno titolo; le istanze di accesso, come anticipato, vanno evase senza ingiustificato ritardo e, comunque, entro un mese, prorogabile a due se sussistono oggettive difficoltà.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 15 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro e se è una impresa fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

3.5. Diritto di rettifica

L'art. 16[6] dispone che l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo (si pensi, ad esempio, a dati anagrafici errati).

Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Il titolare e il responsabile che violano le prescrizioni di cui all'articolo 16 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

3.6. Diritto alla cancellazione

L'art. 17[7] disciplina il diritto alla cancellazione, ossia il diritto all'oblio, inteso come diritto ad essere dimenticato, esercitabile quando si verificano le seguenti condizioni:

---

6. **Art. 16 Diritto di rettifica**
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.

7. **Art. 17 Diritto alla cancellazione**
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.

a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'interessato ritira il consenso su cui si basa il trattamento e non sussiste altro motivo legittimo per trattare i dati;
c) l'interessato si oppone al trattamento dei dati personali e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
d) i dati sono stati trattati illecitamente;
e) i dati devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento;
f) i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

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

La richiesta di cancellazione non sarà accolta in presenza di una delle seguenti circostanze:
a) la conservazione dei dati sia necessaria per esercitare il diritto alla libertà di espressione e di informazione,
b) per adempiere un obbligo legale (ad esempio, le cartelle cliniche devono essere conservate illimitatamente);
c) per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
d) per motivi di interesse pubblico nel settore della sanità pubblica;
e) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
f) per accertare, esercitare o difendere un diritto in sede giudiziaria.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 18 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

---

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'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento; c)per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e)per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

3.7. Diritto di limitazione di trattamento

L'art. 18[8] riconosce all'interessato il diritto di chiedere al titolare la limitazione dei suoi dati personali nelle seguenti ipotesi:

a) quando viene contestata l'esattezza dei dati, nelle more dell'accertamento, da parte del titolare, della valutazione circa l'esattezza;
b) per illiceità del trattamento, allorché l'interessato chieda la limitazione del loto utilizzo;
c) quando l'interessato ha necessità, per fare valere un diritto in sede giudiziaria, dei dati e il titolare non ne abbia più bisogno in quanto le finalità sottese al trattamento sono state raggiunte;
d) quando i dati sono trattati per l'esecuzione di un compito di interesse pubblico, di cui sia investito il titolare, o quando è necessario per fare valere un legittimo interesse del titolare, l'interessato che si oppone al trattamento.

In tali ipotesi, i dati personali sono trattati – salvo che per la conservazione – solo con il consenso dell'interessato o per consentire al titolare l'esercizio o la difesa di un interesse in sede giudiziaria o per tutelare gli interessi di un'altra persona fisica o giuridica o per motivi di interesse pubblico, ritenuti rilevanti dalla normativa comunitaria.

Il titolare comunica all'interessato la revoca della limitazione, prima che la revoca abbia efficacia.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 18 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

3.8. Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento

L'art. 19[9] obbliga il titolare a comunicare ai destinatari cui sono stati trasmessi i dati personali eventuali rettifiche o cancellazioni o limitazioni al trattamento che hanno riguardato gli stessi dati, salve le ipotesi in cui tale attività risulti impossibile o particolarmente gravoso. Ovviamente detti destinatari devono essere stati già censiti da parte del titolare.

---

8. **Art. 18 Diritto di limitazione al trattamento**
1. L'interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi: a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al Titolare del trattamento per verificare l'esattezza di tali dati personali; b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; c) benché il Titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del Titolare del trattamento rispetto a quelli dell'interessato.
2. Se il trattamento è limitato a norma del paragrafo 1, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
3. L'interessato che ha ottenuto la limitazione del trattamento a norma del paragrafo 1 è informato dal Titolare del trattamento prima che detta limitazione sia revocata.

9. **Art. 19 Obbligo di notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento**
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.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 19 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

3.9. Diritto alla portabilità dei dati

L'art. 20[10] sancisce il diritto alla portabilità dei dati personali in capo all'interessato, attraverso la possibilità di ottenere dal titolare e riutilizzare i dati forniti e la possibilità di trasmettere detti dati da un sistema di trattamento elettronico ad un altro e, quindi, ad un diverso titolare, senza che il primo possa opporsi. I proprio dati devono essere ricevuti dall'interessato in un formato strutturato, di uso comune e leggibile da un dispositivo automatico.

Il diritto alla portabilità dei dati può essere esercitato qualora il trattamento sia effettuato con mezzi automatizzati e si basi sul consenso prestato esplicitamente dall'interessato per una o più finalità specifiche, ovvero se il trattamento è necessario all'esecuzione di un contratto.

I dati forniti non sono solo quelli comunicati in modo consapevole (ad esempio, il nome o i recapiti postali e telefonici), ma anche quelli derivanti dall'osservazione delle attività svolte dal soggetto (ad esempio, la cronologia delle ricerche su internet effettuate dall'interessato e i dati relativi al traffico sul web).

L'interessato può chiedere la trasmissione diretta dei dati ad un altro titolare, se tecnicamente possibile.

Il diritto alla portabilità non opera qualora il trattamento sia 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. La portabilità, inoltre, non può condurre alla violazione della tutela dei diritti o delle libertà altrui.

La portabilità non comporta la cancellazione automatica dei dati trasferiti da parte dell'originario titolare.

La richiesta di portabilità deve essere adempiuta senza ingiustificato ritardo e, comunque, entro 30 giorni, salva l'ipotesi di particolare complessità, nella quale si può arrivare ad un massimo di 3 mesi, previa informazione all'interessato della motivazione di tale proroga, da comunicare nei 30 giorni.

10. **Art. 20 Diritto alla portabilità dei dati**
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.

Per quanto riguarda le modalità di trasmissione, sicuramente sono utilizzabili la trasmissione via Internet e l'utilizzo di supporti fisici.

L'eventuale opposizione del titolare alla richiesta di portabilità deve essere comunicata all'interessato, con l'indicazione dei motivi e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale, al massimo entro 30 giorni dal ricevimento della richiesta.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 20 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

3.10. Diritto di opposizione

L'art. 21[11] prevede che l'interessato, in qualsiasi momento, possa opporsi al trattamento dei dati personali che lo riguardano, compresa la profilazione. In tal caso, 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.

Tale diritto di opposizione è utilizzabile anche per il trattamento dei dati personali per finalità di marketing diretto, ossia la comunicazione diretta di natura commerciale/pubblicitaria da parte di un'azienda nei confronti di clienti specifici, senza avvalersi di intermediari.

Il diritto deve essere 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.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 21 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

11. **Art. 21 Diritto di opposizione**
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.

3.11. Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

L'art. 22[12] riconosce all'interessato il diritto a non essere valutato esclusivamente attraverso il ricorso ad un trattamento automatizzato (compresa la profilazione), allorquando tale valutazione produrrà effetti giuridici rilevanti nei suoi confronti. Ricordiamo che, come indicato nell'art. 4, comma 1, n. 4 del Regolamento, per profilazione si intende "*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*".

Il diritto non opera nei casi in cui:
a) la decisione si renda necessaria per la stipula o l'esecuzione di un contratto tra l'interessato ed il titolare;
b) la legislazione comunitaria o di uno Stato membra lo preveda, pur nel rispetto – in capo al titolare – di adottare le misure adeguate a garantire la tutela dei diritti, delle libertà e degli interessi legittimi dell'interessato;
c) l'interessato abbia fornito il consenso ad un trattamento dei propri dati personali con tali finalità.

Nei casi di cui alle lettere a) e c), il titolare del trattamento deve attuare 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.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 22 sono soggetti a sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 5, lett. b)).

3.12. Limitazioni

L'art. 23[13] consente al diritto dell'Unione o dello Stato membro di limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui:

---

12. **Art. 22 Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione**
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.

13. **Art. 23 Limitazioni**
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

- all'art. 5, lettere da a) a e),
- agli articoli da 11 a 20,
- all'art. 32,

qualora tale limitazione costituisca una misura necessaria e proporzionata in una società democratica per salvaguardare:

a) la pubblica sicurezza;
b) le attività volte a prevenire, indagare, accertare e perseguire reati;
c) altri interessi pubblici 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, e la stabilità e l'integrità del mercato;
d) le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
e) una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi di cui alle lettere a), b), c), e d);
f) la tutela dell'interessato o dei diritti e delle libertà altrui.

Gli interventi legislativi di cui si prospetta la realizzazione devono riguardare almeno uno dei punti elencati alle lettere da a) a h) del comma 2 dell'art. 23, ossia:

a) finalità e categorie del trattamento;
b) categorie di dati personali;
c) portata delle limitazioni introdotte;
d) garanzie contro gli abusi o l'accesso o il trasferimento illeciti;
e) indicazione precisa del titolare del trattamento o delle categorie di titolari;
f) 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) rischi per i diritti e le libertà degli interessati;
h) diritto degli interessati di essere informati della limitazione, a meno che ciò possa compromettere la finalità della stessa.

---

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.

4. L’organizzazione prevista dal regolamento

4.1. Responsabilità del titolare del trattamento

L’art. 24[1] del Regolamento disciplina la responsabilità del titolare del trattamento (per rimanere nel nostro ambito, la responsabilità del professionista rispetto ai dati dei proprio clienti).

In primis, il titolare deve utilizzare misure tecniche e organizzative adeguate a garantire il rispetto di quanto previsto dal Regolamento; è, altresì, tenuto a riesaminare ed aggiornare, se necessario, tali misure e, aspetto non secondario, deve essere in grado di dimostrare che le misure suddette sono adeguate.

In secundis, le misure devono essere modulate per tenere 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.

In sintesi, perciò, il titolare (*rectius*, il professionista) dovrà, anche tenendo conto della competenze specifiche presenti nello studio:

- organizzare il proprio studio, da un punto di vista strumentale e di risorse umane, allo scopo di garantire la gestione dei dati nel rispetto di quanto previsto dal Regolamento;
- prevedere una formazione continua per se stesso e per i collaboratori;
- individuare ed applicare codici di condotta ed ottenere le certificazioni (utili anche ai fini della dimostrazione di essersi adeguatamente attivato);
- verificare periodicamente l’adeguatezza delle misure e, se opportuno, intervenire per migliorarle;
- adottare protocolli organizzativi per la gestione delle richieste in merito al trattamento dei dati, ivi compresi eventuali reclami presentati dai soggetti interessati;
- adottare protocolli organizzativi per la gestione degli episodi in cui si verifichino violazioni di dati.

1. **Art. 24 Responsabilità del Titolare del trattamento**
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.

4.2. Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

L'art. 25[2] obbliga il titolare a predisporre l'opportuna tutela dei dati sin dalla progettazione dello strumento (c.d. *privacy by design*), allo scopo di individuare rischi e misure di tutela, con una protezione del dato quale impostazione predefinita della propria organizzazione aziendale (c.d. *privacy by default*).

In particolare, è previsto il corretto utilizzo delle tecniche di pseudonimizzazione e di minimizzazione; inoltre, il titolare deve utilizzare 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.

Anche in questo caso, un meccanismo di certificazione può essere utile, anche fini della dimostrazione di aver adempiuto ai propri obblighi.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 25 sono soggetti a sanzioni amministrative pecuniarie fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, lett. a)).

4.3. Contitolari del trattamento

Secondo quanto disposto dall'art. 26[3], si ha l'ipotesi del contitolare del trattamento quando due o più titolari condividono e decidono insieme le finalità ed i mezzi del trattamento; in tal caso, deve

---

2. **Art. 25 Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita**
1.Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e tutelare i diritti degli interessati.
2. Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.
3. Un meccanismo di certificazione approvato ai sensi dell'articolo 42 può essere utilizzato come elemento per dimostrare la conformità ai requisiti di cui ai paragrafi 1 e 2 del presente articolo.

3. **Art. 26 Contitolari del trattamento**
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.

essere sottoscritto un accordo interno per regolare la ruoli e responsabilità di ciascuno. Tale accordo deve essere reso noto all'interessato.

In ogni caso, quest'ultimo può inviare una istanza di accesso indistintamente ad uno dei due contitolari, a prescindere da quanto regolato attraverso l'accordo; inoltre, indipendentemente dalle suddivisioni di responsabilità determinate con l'accordo, l'interessato può esercitare i propri diritti nei confronti e contro ciascun titolare del trattamento.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 26 sono soggetti a sanzioni amministrative pecuniarie fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, lett. a)).

4.4. Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione

L'art. 27[4] dispone che, qualora il trattamento venga svolto da un titolare o da un responsabile che non siano stabiliti all'interno della UE, è fatto obbligo al titolare di procedere alla designazione, per iscritto, di un rappresentante con sede nella UE, a meno che:

a) il trattamento sia occasionale e non riguardante dati sensibili o dati relativi a condanne penali e, comunque, a seguito di una valutazione condotta dal titolare deve risultare improbabile il rischio di lesione dei diritti e delle libertà delle persone fisiche;
b) se il trattamento sia effettuato da Autorità pubbliche o organismi pubblici.

Trattandosi di un'ipotesi probabilmente meno frequente per i professionisti, si rinvia all'articolo citato in nota.

4. **Art. 27 Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione**
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.

4.5. Responsabile del trattamento

L'art. 28[5] dispone che il responsabile del trattamento è il soggetto che effettua il trattamento per

5. **Art. 28 Responsabile del trattamento**
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.

conto del titolare; il responsabile, ovviamente, deve possedere adeguate capacità tecniche ed organizzative, in ossequio a quanto previsto dal Regolamento, per la tutela dell'interessato.

Con apposito contratto, dovrà essere disciplinata la materia, la durata, le finalità del trattamento, il tipo di dati personali, la categoria dei soggetti interessati, gli obblighi ed i diritti delle parti.

Nel caso di più responsabili (ognuno dei quali deve avere idonea capacità tecnica-organizzativa), il titolare deve darne preventiva autorizzazione scritta, specifica e generale: immaginiamo, ad esempio, il professionista che commissiona una campagna di marketing ad un responsabile e l'analisi dei dati raccolti ad altro responsabile. Ovviamente, anche i rapporti fra i vari responsabili saranno oggetto di apposito contratto e rimane ferma la responsabilità del primo responsabile anche per l'operato degli altri.

Più precisamente, il contratto deve avere il seguente contenuto minimo:
a) i dati personali da trattare, solo su istruzione documentata del titolare,
b) l'obbligo di riservatezza delle persone autorizzate al trattamento;
c) le misure di sicurezza adottate;
d) le garanzie circa l'applicazione di misure tecniche ed organizzative, il cui ricorso presuppone espressa autorizzazione del titolare;
e) modalità di esecuzione delle istruzioni del titolare per quanto attiene l'applicazione delle misure di sicurezza;
f) procedure per la cancellazione, su richiesta del titolare, i dati personali;
g) messa a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi.

Il contratto che disciplina i trattamenti in capo al responsabile e il ricorso, da parte del responsabile, ad un altro responsabile per l'esecuzione di specifiche attività di trattamento, richiede la forma scritta, compreso il formato digitale.

Qualora il responsabile determini le finalità ed i mezzi del trattamento, si considera egli stesso titolare.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 28 sono soggetti a sanzioni amministrative pecuniarie fino a 10 milioni di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, lett. a)).

4.6. Trattamento sotto l'Autorità del titolare del trattamento o del responsabile del trattamento

L'art. 29[6] dispone che il trattamento dei dati personali da parte del responsabile o di altro soggetto a questi sottoposto non può avvenire in assenza di istruzioni da parte del titolare, salva la possibilità che la legislazione UE e quella dei singoli Stati dispongano diversamente.

Il titolare e il responsabile che violano le prescrizioni di cui all'art. 29 sono soggetti a sanzioni amministrative pecuniarie fino a 10 milioni di euro e, se è una impresa, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, lett. a)).

6. **Art. 29 Trattamento sotto l'Autorità del titolare del trattamento o del responsabile del trattamento**
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.

5. Gli adempimenti richiesti

5.1. Premessa

Veniamo, a questo punto, alla parte essenziale per i professionisti: l'individuazione degli adempimenti richiesti dal Regolamento.

5.2. Il registro delle attività di trattamento

Il primo adempimento, previsto dall'art. 30[1] del Regolamento, è il registro delle attività di trattamento per il titolare e per il responsabile del trattamento. Per quanto attiene al contenuto, il registro deve contenere almeno le seguenti informazioni:
a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del

1. **Art. 30 Registri delle attività di trattamento**
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.

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;
e) ove applicabile, i trasferimenti di dati personali verso paesi terzi e la loro identificazione; in taluni casi deve essere allegata la documentazione delle garanzie adeguate;
f) i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) una descrizione generale delle misure di sicurezza tecniche e organizzative.

Anche il responsabile dovrà avere un analogo registro dei trattamenti relativi a quelli che sono oggetto della sua nomina, precisamente:
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'art. 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Ovviamente, i registri saranno tenuti in forma scritta, anche in formato elettronico; su richiesta dell'Autorità di controllo, il titolare ed il responsabile sono tenuti ad esibirli.

Nel caso di titolari con meno di 250 dipendenti i registri sono obbligatori solo se il trattamento comprende dati sensibili o se è presente un rischio per i diritti e le libertà dell'interessato o se il trattamento non sia occasionale.

È evidente che il professionista, per poter adempiere correttamente, deve porre in essere una serie di attività propedeutiche:
a) mappatura dei processi di trattamento;
b) individuazione delle principali aree di rischio e relative contromisure di sicurezza, sia in termini generali sia avendo riguardo al singolo trattamento;
c) definizione di ruoli di ciascuno dei dipendenti e collaboratori di studio ai fini del rispetto delle norme in materia di privacy;
d) aggiornamento del regolamento esistente, in modo da integrarlo con le nuove norme previste dal Regolamento.

Premessa l'opportunità (se non la necessità) di dotarsi di una apposito software gestionale anche ai fini del periodico aggiornamento, si può utilizzare uno schema con una spazio per i dati del titolare e più colonne, nella quali inserire diverse diciture:
a) tipologia di trattamento: ad esempio, elenco clienti, elenco fornitori, fogli di presenza dei dipendenti/collaboratori;
b) area dello studio interessata: ad esempio, la segreteria per la presenza dei dipendenti/collaboratori; l'area amministrativa per l'elenco dei clienti e dei fornitori;
c) finalità: ad esempio, gestione degli incassi e dei pagamenti;
d) tipologia di dati personali (dati sensibili, dati comuni, dati giudiziari, ecc.);
e) tipologia di interessati: ad esempio, clienti, fornitori, dipendenti, collaboratori;

f) informativa;
g) consenso necessario o meno;
h) modalità della conservazione;
i) misure di sicurezza tecniche e organizzative;
j) contitolare del trattamento (se previsto);
k) rappresentante del titolare (se previsto);
l) responsabile del trattamento (con la indicazione dell'indirizzo, del numero di telefono, dell'indirizzo e.mail, dell'indirizzo PEC, ecc.);
m) destinatari (i soggetti ai quali i dati saranno trasmessi);
n) Paese terzo o organizzazione internazionale (se previsto);
o) termini per la cancellazione;
p) valutazione di impatto sulla protezione dei dati (se previsto);
q) ulteriori voci ritenute opportune.

Ricordiamo, infine, che il titolare e il responsabile che violano l'obbligo di istituzione, di tenuta e di aggiornamento del Registro *privacy* sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4, lettera a)).

5.3. La cooperazione con l'Autorità di controllo

L'art. 31 del Regolamento obbliga il titolare del trattamento, il responsabile del trattamento e, ove applicabile, il loro rappresentante a cooperare, su richiesta, con l'Autorità di controllo nell'esecuzione dei suoi compiti. Ciò significa che tali soggetti dovranno fornire dati, informazioni, documenti ed agevolare le attività di indagine e controllo dell'Autorità.

Il titolare e il responsabile che violano l'obbligo di cooperazione con l'Autorità di controllo sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, comma 4, lettera a)).

5.4. Garantire la sicurezza del trattamento

L'art. 32[2] prevede uno dei principali adempimenti in capo al titolare e al responsabile del trattamento: la applicazione di adeguate misure di sicurezza del trattamento, individuate a seguito

2. **Art. 32 Sicurezza del trattamento**
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.

di opportuna analisi dei rischi che consenta di calibrare le misure. Dette misure devono consentire:

a) la pseudonimizzazione e la cifratura dei dati personali, ove ritenuto opportuno/necessario;
b) la capacità di assicurare su base permanente la riservatezza[3], l'integrità[4], la disponibilità[5] e la resilienza[6] 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 (c.d. *business continuity*);
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Come già anticipato, il livello di sicurezza andrà stabilito dopo avere svolto una corretta valutazione dell'impatto ed una analisi dei rischi.

Il trattamento dei dati personali da parte di soggetti sottoposti all'Autorità del titolare o del responsabile deve essere sempre autorizzato e istruito da questi a meno che non ci siano norme (comunitarie o nazionali) che dispongano in maniera diversa.

Il titolare e il responsabile che violano l'obbligo di adozione di misure di sicurezza adeguate sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, comma 4, lettera a)).

5.5. L'obbligatoria notifica all'Autorità di controllo e all'interessato della violazione dei dati

L'art. 33[7] obbliga il titolare del trattamento a notifica la violazione dei dati (c.d. *data breach*) all'Autorità di controllo, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne

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.

3. L'accesso protetto e controllato ai dati, a garanzia della confidenzialità delle informazioni trattate.
4. Intesa quale sicurezza che i dati trattati siano completi e inalterati.
5. Intesa come accessibilità nei tempi e nei luoghi previsti.
6. Con il termine "resilienza" in informatica si intende la capacità di un sistema di adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati. Essa si basa sulla qualità dell'hardware, del software e dell'organizzazione umana.
7. **Art. 33 Notifica di una violazione dei dati personali all'Autorità di controllo**

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 re-

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 (valutazione, peraltro, non necessariamente semplice). Se la notifica è effettuata oltre le 72 ore, il titolare deve motivare il ritardo.

Come accennato in precedenza, per "violazione dei dati personali" si intende, secondo il Regolamento, "*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*".

Il titolare del trattamento deve essere informato della violazione dei dati dal responsabile del trattamento senza ritardo, dopo che questi ne sia venuto a conoscenza.

La notifica prevede il seguente contenuto minimo:
a. l'avvenuta violazione;
b. la comunicazione dei riferimenti e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c. la descrizione delle probabili conseguenze della violazione dei dati personali;
d. la descrizione delle 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.

Il Regolamento prevede tuttavia che, 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.

Tutta la documentazione deve essere opportunamente conservata, in quanto può essere richiesta dall'Autorità Garante al fine di verificare il rispetto delle disposizioni del Regolamento europeo in materia di protezione dei dati personali.

Anche il soggetto interessato ha diritto alla comunicazione tempestiva e chiara della violazione dei dati personali (art. 34[8]); tuttavia, tale obbligo non sorge in capo al titolare se:
1. 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;

---

lative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'Autorità di controllo di verificare il rispetto del presente articolo.

8. **Art. 34 Comunicazione di una violazione dei dati all'interessato**

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.

2. 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;
3. 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.

Il titolare e il responsabile che violano gli obblighi previsti dal regolamento in materia di *data breach* sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83, comma 4, lettera a)).

5.6. La valutazione d'impatto sulla protezione dei dati

L'art. 35[9] obbliga il titolare ad una adeguata valutazione del rischio (intendendo quest'ultimo come il prodotto della frequenza di accadimento e della gravità delle conseguenze, trattamento), tenuto

9. **Art. 35 Valutazione d'impatto sulla protezione dei dati**
1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'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 a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4. L'Autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'Autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.
5. L'Autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'Autorità di controllo comunica tali elenchi al comitato.
6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'Autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.
7. La valutazione contiene almeno: a)una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento; b)una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c)una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d)le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8. Nel valutare l'impatto del trattamento effettuato dai relativi Titolari o Responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.
9. Se del caso, il Titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.
10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il Titolare del trattamento è soggetto una base giuridica, tale diritto disciplini

conto della natura, dell'oggetto, o delle finalità del trattamento, in consultazione con il responsabile.

È necessario, perciò, riferirsi alle normative UNI EN ISO 9001, ISO 31000 e ISO/IEC 27001.

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nel caso di:
1. 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 sugli interessati;
2. trattamento, su larga scala[10], di categorie particolari di dati personali (sensibili o giudiziari);
3. sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il compito è semplificato dal fatto che l'Autorità di controllo provvederà a redigere e pubblicizzare l'elenco dei trattamenti da sottoporre preventivamente ad una valutazione di impatto e l'elenco dei trattamenti esonerati da tale valutazione.

Alla valutazione di impatto del trattamento dei dati possono essere utili i codici di condotta e le opinioni degli interessati o dei loro rappresentanti in merito alla valutazione di impatto.

Per comprensibili motivi di uniformità, la valutazione dovrà contenere almeno:
1. una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
2. una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. una valutazione dei rischi per i diritti e le libertà degli interessati;
4. 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 Regolamento.

È possibile individuare una serie di attività utili ai fini della valutazione del rischio; ad esempio:
1. individuare le possibili situazioni di rischio, avendo riguardo ai tipi di violazione, alle strutture dello studio coinvolte, alla probabilità del verificarsi dell'evento e alla gravità delle conseguenze;
2. individuare ed adottare le contromisure necessarie, sia per ridurre i rischi, sia per intervenire a contenimento delle conseguenze;
3. effettuare un monitoraggio costante ed una verifica periodica;
4. predisporre piani di *disaster recovery*.

L'obbligo di compiere una valutazione di impatto dei rischi connessi al trattamento di dati personali non sorge nell'ipotesi in cui:
a) il trattamento è "*necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*";

---

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.

10. Ci si riferisce a quei trattamenti riguardanti 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.

b) il trattamento di che trattasi "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblic*i poteri di cui è investito il titolare del trattamento*".

Qualora il trattamento effettuato trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il Titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, non si applicano le regole prima indicate per la valutazione dei rischi, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

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.

Il titolare e il responsabile che violano gli obblighi di cui all'art. 35 sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83, comma 4, lettera a)).

5.7. La consultazione preventiva

Nel caso di trattamento da cui potrebbe derivare un rischio elevato, l'art. 36[11] del Regolamento prevede la consultazione preventiva dell'Autorità di controllo da parte del titolare del trattamento, prima di procedere al trattamento dei dati personali; l'Autorità di controllo **s**i esprime entro otto settimane, con possibile proroga di sei settimane.

11. **Art. 36 Consultazione preventiva**
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.

Nell'ambito di tale processo di consultazione, va 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. Inoltre, vanno comunicate all'Autorità di controllo le informazioni relativamente ai seguenti aspetti:
a) gli ambiti di responsabilità del titolare, degli eventuali contitolari e dei responsabili;
b) le misure adottate per garantire e proteggere i diritti e le libertà degli interessati;
c) gli eventuali dati di contatto del titolare;
d) ogni altra richiesta che perviene dall'Autorità di controllo.

Le legislazioni dei singoli Stati membri possono prescrivere che i titolari consultino l'Autorità di controllo per ottenerne l'autorizzazione preliminare al trattamento avente ad oggetto un interesse pubblico come la protezione sociale e la sanità pubblica.

Il titolare e il responsabile che violano gli obblighi di cui all'art. 36 sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83, comma 4, lettera a)).

5.8. La designazione del responsabile della protezione dei dati

Secondo quanto previsto dall'art. 37[12] del Regolamento, deve essere designato un responsabile della protezione (DPO – *data protection officer*), da parte del titolare del trattamento e del responsabile, al fine di vigilare sulla corretta applicazione della normativa in materia di protezione dei dati personali, da parte dell'ente/organizzazione.

Tale figura è obbligatoria:
a) se il trattamento è effettuato da un'Autorità pubblica o da un organismo pubblico, eccettuate le Autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

12. **Art. 37. La designazione del Responsabile della protezione dei dati**
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.

b) se 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;
c) se 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'art. 9 o di dati relativi a condanne penali e a reati di cui all'art. 10.

La scelta sulla figura deve essere basata sulle sue qualità personali e professionali e alle sue conoscenze specialistiche nel campo della protezione dei dati personali; è auspicabile che detta figura abbia una buona conoscenza del funzionamento della organizzazione alla quale appartiene o dalla quale viene designato. Normalmente si tratta di un dipendente ma nulla vieta che possa essere un soggetto esterno[13].

Avendo riguardo ai professionisti, difficilmente si verificherà l'ipotesi di obbligatorietà della nomina di tale figura: per tale motivo, in questa sede, ci limitiamo a rinviare al testo degli art. 37, 38[14] e 39[15].

Il titolare e il responsabile che violano gli obblighi di cui all'art. 37, 38 e 39 sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83, comma 4, lettera a)).

13. Sul punto si rinvia ai documenti riportati in Appendice.
14. **Art. 38 Posizione del Responsabile della protezione dei dati**
1. Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il Responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
2. Il Titolare e del trattamento e il Responsabile del trattamento sostengono il Responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.
3. Il Titolare del trattamento e il Responsabile del trattamento si assicurano che il Responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il Responsabile della protezione dei dati non è rimosso o penalizzato dal Titolare del trattamento o dal Responsabile del trattamento per l'adempimento dei propri compiti. Il Responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento.
4. Gli interessati possono contattare il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente Regolamento.
5. Il Responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.
6. Il Responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il Titolare del trattamento o il Responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.
15. **Art. 39 Compiti del Responsabile della protezione dei dati**
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.

5.9. Codici di condotta

L'art. 40[16] riserva ai codici di condotta il ruolo di contribuire alla corretta applicazione del regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese.

16. **Art. 40 Codici di condotta**
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 controllo che è competente ai sensi dell'articolo 55 lo sottopone, tramite la procedura di cui all'articolo 63, al comitato, il quale formula un parere sulla conformità al presente Regolamento del progetto di codice, della modifica o della proroga o, nel caso di cui al paragrafo 3 del presente articolo, sulla previsione di adeguate garanzie.
8. Qualora il parere di cui al paragrafo 7 confermi che il progetto di codice di condotta, la modifica o la proroga è conforme al presente Regolamento o, nel caso di cui al paragrafo 3, fornisce adeguate garanzie, il comitato trasmette il suo parere alla Commissione.
9. La Commissione può decidere, mediante atti di esecuzione, che il codice di condotta, la modifica o la proroga approvati, che le sono stati sottoposti ai sensi del paragrafo 8 del presente articolo, hanno validità generale all'interno dell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2.
10. La Commissione provvede a dare un'adeguata pubblicità dei codici approvati per i quali è stata decisa la validità generale ai sensi del paragrafo 9.
11. Il comitato raccoglie in un registro tutti i codici di condotta, le modifiche e le proroghe approvati e li rende pubblici mediante mezzi appropriati.

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 Regolamento.

I codici di condotta contengono anche i meccanismi che consentono 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.

Le associazioni e gli altri organismi 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; quest'ultima 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.

Il controllo sui codici può anche essere svolto da un organismo terzo in possesso del livello adeguato di competenze riguardo al contenuto del codice, accreditato a tal fine dell'Autorità di controllo competente, indipendente[17].

5.10. Le certificazioni

L'art. 42[18] disciplina le certificazioni quali strumenti facoltativi idonei a dimostrare la *compliance* tra il Regolamento comunitario e il trattamento dei dati personali. In sintesi, il meccanismo di cer-

17. **Art. 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.
18. **Art. 42 Certificazione**
1. Gli Stati membri, le Autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente Regolamento dei trattamenti effettuati dai Titolari del

tificazione deve attestare i requisiti minimi per un sistema di gestione della protezione dei dati, in funzione delle specificità dei vari settori di trattamento (pubblico o privato) e delle esigenze delle grandi, medie e piccole imprese.

I requisiti debbono essere verificabili attraverso un sistema di monitoraggio e/o attraverso un sistema di valutazione di terza parte, da parte dell'organismo di certificazione, in possesso del livello adeguato di competenze riguardo alla protezione dei dati, che può rilasciare e rinnovare la certificazione. Il monitoraggio e/o la certificazione, possono essere utilizzati a fini esterni, per scopi di comunicazione, e per la dimostrazione di aver adottato un sistema di gestione per la protezione dei dati.

Come per i codici di condotta, le certificazioni possono essere utilizzati come elementi per dimostrare il rispetto degli obblighi in capo al titolare del trattamento.

Il rilascio di certificazione al titolare o al responsabile fa scattare in capo a questi soggetti l'impegno ad applicare analoghe garanzie in tema di tutela dei diritti degli interessati.

La certificazione viene rilasciata per una durata pari a tre anni ed è rinnovabile, alle stesse condizioni e purché sussistano i requisiti richiesti; se tali requisiti vengono meno, ovviamente la certificazione è revocata.

Il titolare e il responsabile che violano gli obblighi di cui all'art. 42 sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83, comma 4, lettera a)). La violazione degli obblighi di cui all'art. 42 comporta una responsabilità anche in capo agli organismi di certificazione.

---

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.

5.11. Gli organismi di certificazione

L'art. 43[19] prevede il coinvolgimento di organismi di certificazione accreditati per valutare la conformità dei sistemi di protezione dei dati attivati dai titolari o dai responsabili del trattamento soggetti al Regolamento.

La norma indicata come riferimento per l'accreditamento di tali organismi è la EN ISO/IEC 17065:2012, che disciplina il rilascio della certificazione di prodotto, applicabile agli Organismi che effettuano la certificazione di prodotti, processi e servizi.

19. **Art. 42 Organismi di certificazione**
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) 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 paragrafo 1 del presente articolo, se le condizioni per l'accreditamento non sono, o non sono più, rispettate o se le misure adottate da un organismo di certificazione violano il presente Regolamento.
8. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 92 al fine di precisare i requisiti di cui tenere conto per i meccanismi di certificazione della protezione dei dati di cui all'articolo 42, paragrafo 1.
9. La Commissione può adottare atti di esecuzione per stabilire norme tecniche riguardanti i meccanismi di certificazione e i sigilli e marchi di protezione dei dati e le modalità per promuovere e riconoscere tali meccanismi di certificazione, i sigilli e marchi di protezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2. 1. 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).

L'accreditamento agli organismi i certificazione può essere rilasciato dall'Ente unico nazionale di accreditamento (in Italia, dall'Ente Nazionale di Accreditamento – ACCREDIA) o dall'Autorità competente (in l'Italia, l'Autorità Garante per la protezione dei dati personali).

Detti organismi di certificazione, per essere accreditati, devono:
a) dimostrare di essere indipendenti e competenti;
b) di essersi impegnati a rispettare i criteri di cui all'art. 42, par. 5;
c) di avere istituito procedure per il rilascio delle certificazioni;
d) di avere istituito procedure per la gestione dei reclami;
e) avere dimostrato all'Autorità di controllo che non vertono in una situazione di conflitto di interessi.

L'accreditamento degli organi di certificazione deve avvenire in base ai criteri approvati dall'Autorità di controllo competente.

Gli organismi di certificazione sono responsabili della corretta valutazione in merito alle istanze di certificazione, mentre la responsabilità della conformità al Regolamento resta di competenza del titolare e del responsabile del trattamento.

L'organismo di certificazione collabora con l'Autorità di controllo provvedendo a riscontrare le sue richieste in merito ai motivi del rilascio o della revoca della certificazione.

I requisiti richiesti per la concessione dell'accreditamento sono resi pubblici dall'Autorità di controllo. Qualora le condizioni per la concessione dell'accreditamento non sono, o non sono più rispettate, o se le misure di un organismo di certificazione violano il Regolamento, l'Autorità di controllo o l'organismo nazionale di accreditamento revocano l'accreditamento.

Il titolare e il responsabile che violano gli obblighi di cui all'art. 43 sono soggetti a sanzione amministrativa pecuniaria fino a 10.000.000 euro o, per le imprese, fino al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore (art. 83, comma 4, lettera a)). La violazione degli obblighi di cui all'art. 42 comporta una responsabilità anche in capo agli organismi di certificazione.

5.12. Il risarcimento del danno

L'art. 82[20] dispone che chiunque subisca un danno materiale o immateriale a seguito di una violazione del Regolamento ha il diritto ad ottenerne il risarcimento del danno stesso ad opera del

20. **Art. 82 Diritto al risarcimento e responsabilità**
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

titolare o del responsabile; la responsabilità viene meno se il titolare e il responsabile riescono a provare che l'evento dannoso non è in alcun modo loro imputabile.

È prevista la responsabilità in solido in caso di una pluralità di titolari o di responsabili, per l'intero ammontare del danno, con diritto di rivalsa a favore di chi paga per l'intero.

La competenza nell'esercizio delle azioni legali finalizzate ad ottenere il risarcimento dei danni sono delle Autorità giurisdizionali competenti, in base a quanto regolato dal diritto dello Stato membro.

5.13. Le sanzioni

L'art. 83[21] del Regolamento prevede in capo all'Autorità di controllo il potere di imporre sanzioni amministrative per un importo pecuniario massimo predeterminato, tenendo conto, nella deter-

---

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.

21. **Art. 83 Condizioni generali per infliggere sanzioni amministrative pecuniarie**

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) qualsia-

minazione del *quantum*, delle circostanze del caso (ad esempio, del dolo o della colpa dell'autore; della natura, della gravità e della durata della violazione; della presenza/assenza di misure adottate; ecc.) e della natura di impresa o persona fisica del responsabile. Le sanzioni, peraltro, devono essere effettivamente inflitte, proporzionate e dissuasive.

Per comodità, si ribadisce che si applica la sanzione fino a 10 milioni di euro, o in caso d'impresa, fino al 2% del fatturato annuo mondale dell'esercizio precedente se superiore, la violazione delle prescrizioni degli articoli:

- 8 (consenso dei minori),
- 10 (trattamenti che non richiedono l'identificazione degli interessati),
- 25 (protezione dei dati fin dalla progettazione e protezione per impostazione predefinita),
- 26 (contitolarità del trattamento),
- 27 (nomina rappresentante del titolare non stabilito nell'Unione Europea),
- 28 (responsabile del trattamento),
- 29 (trattamento sotto l'Autorità del titolare o del responsabile del trattamento),
- 30 (registri delle attività del trattamento),
- 31 (cooperazione con l'Autorità di vigilanza),
- 32 (sicurezza del trattamento),
- 33 (notificazione delle violazioni all'Autorità),
- 34 (comunicazioni delle violazioni all'interessato),
- 35 (valutazione d'impatto sulla protezione dei dati),
- 36 (consultazione preventiva dell'Autorità di vigilanza),
- 37 (designazione del responsabile della protezione dei dati),
- 38 (posizione del responsabile della protezione dei dati),
- 39 (compiti del responsabile della protezione dei dati),
- 42 e 43 (certificazione e relativi organismi).

La sanzione sarà pari fino al doppio (ossia, fino a 20 milioni di euro, o in caso d'impresa, fino al 2% del fatturato annuo mondale dell'esercizio precedente se superiore), per la violazione delle prescrizioni in materia di principi base del trattamento, di condizioni per il consenso, di diritto degli interessati, di trasferimento di dati personali all'estero e di mancata ottemperanza ad un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'Autorità di vigilanza.

---

si 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.

Rimane ferma, ovviamente, la punibilità di comportamenti integranti fattispecie di reato: le relative sanzioni penali sono di competenza dei singoli Stati[22].

22. **Art. 84 Sanzioni**
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.

6. L’analisi dei rischi nel trattamento dei dati personali

6.1. Premessa

Analizzare i rischi connessi al trattamento dei dati è un’attività specialistica che richiede il possesso di adeguate nozioni e competenze: di conseguenza, è sconsigliabile al professionista procedere in modo autonomo. In ogni caso, è comunque possibile procedere ad una prima analisi semplificata, che ben può rappresentare la base di partenza per una valutazione ben più ampia ed esaustiva.

Prima di procedere, è necessario ricordare alcuni punti essenziali:
- il rischio è, ai nostri fini, il prodotto della frequenza di accadimento e della gravità delle conseguenze, trattamento;
- poiché i rischi non sono tutti uguali, è necessario prevedere una scala di valori ed associare a rischi maggiori misure sempre più importanti;
- le misure sono rappresentate da quelle azioni che servono a minimizzare i rischi e/o i danni.

6.2. Una possibile matrice dei rischi per gli archivi informatici

Tanto premesso, indichiamo di seguito una matrice dei rischi che, sebbene di impostazione semplice, è comunque efficace nell’evidenziare il metodo da utilizzare nell’analisi da parte del professionista:

PROBLEMA	ELEMENTI DI DEBOLEZZA	DANNI	MISURE
Sottrazione delle credenziali per via telematica	Scarse misure di sicurezza Insufficiente formazione del personale	Accesso illegittimo e conseguente utilizzo di dati da parte di terzi Alterazione e/o distruzione dei dati	Formazione del personale Software ed hardware adeguati Procedure per la corretta conservazione delle password e la relativa modifica periodica
Errore materiale	Insufficiente formazione del personale	Accesso da parte di terzi non autorizzati Alterazione e/o distruzione di dati	Formazione del personale
Virus informatici	Software non aggiornati	Accesso da parte di terzi non autorizzati Alterazione e/o distruzione di dati	Formazione del personale Utilizzo di software periodicamente aggiornati: antivirus, firewall
Hardware e software obsoleti	Scarsa protezione ed efficienza Malfunzionamenti	Problemi di accesso Perdita dei dati	Utilizzo di hardware adeguati e software aggiornati
Accesso fisico da parte di terzi presso lo studio professionale	Scarse misure antiintrusione	Furto dei dati	Installazione misure di sicurezza (ad esempio: videosorveglianza, portoncino di ingresso blindato, finestre con sistema anti-intrusione, sistema di allarme) Regolamentazione degli accessi Utilizzo di armadi blindati/ignifughi
Disastri naturali e/o incidenti		Perdita dei dati	Procedure di *disaster recovery*, sistemi antincendio Utilizzo di armadi blindati/ignifughi
Guasto al sistema elettrico		Accesso impossibile Operatività inibita	Gruppo di continuità

Per ciascuna delle aree di rischio (e per quelle ulteriori eventualmente individuate), il professionista dovrà stimare l'indice di rischio, vale a dire la probabilità di accadimento e l'impatto delle conseguenze. Si può, ad esempio, immaginare di individuare quattro livelli:

- rischio basso,
- rischio medio,
- rischio alto,
- rischio altissimo.

Le misure dovranno essere tanto più importanti quanto maggiore è tale livello di rischio.

Inoltre, periodicamente la matrice andrà verificata e, all'occorrenza, opportunamente implementata.

6.3. Una possibile matrice dei rischi per gli archivi cartacei

Riprendendo la precedente matrice utilizzata per gli archivi informatici, proponiamo una simile per gli archivi cartacei:

PROBLEMA	ELEMENTI DI DEBOLEZZA	DANNI	MISURE
Errore materiale	Insufficiente formazione del personale	Alterazione e/o distruzione di dati	Formazione del personale
Accesso fisico da parte di terzi presso lo studio professionale	Scarse misure antiintrusione	Furto, alterazione e/o distruzione dei dati	Installazione misure di sicurezza (ad esempio: videosorveglianza, portoncino di ingresso blindato, finestre con sistema anti-intrusione, sistema di allarme) Regolamentazione degli accessi Utilizzo di armadi blindati/ignifughi
Disastri naturali e/o incidenti		Perdita dei dati	Procedure di *disaster recovery*, sistemi antincendio Utilizzo di armadi blindati/ignifughi

6.4. Le misure di sicurezza

Le misure di sicurezza possono essere classificate, in ragione della loro natura, in tre categorie:

ORGANIZZATIVE	FISICHE	INFORMATICHE
Nomina del responsabile	Sistemi anti-intrusione, di allarme e vigilanza	Utilizzo di username e password per l'accesso ai computer
Rilascio e revoca dell'autorizzazione, da parte del titolare o del responsabile, agli incaricati del trattamento dei dati	Accesso controllato	Password con caratteristiche di sicurezza (di primo accesso con sostituzione obbligatoria da parte dell'utente, numero minimo di caratteri, presenza di lettere, numeri e simboli, blocco dopo 3 tentativi errati, ecc.)
Previsione di diversi livelli di autorizzazione di accesso ai dati in relazione ai compiti e mansioni assegnate	Gruppo di continuità	Periodica modifica della password ad esempio, ogni 30 giorni) e scadenza dopo non uso prolungato (ad esempio, dopo 90 giorni di inutilizzo)
Verifica periodica delle credenziali di accesso	Sistemi antincendio	Utilizzo di software antivirus, periodicamente aggiornato
Istruzioni scritte per lo svolgimento dei compiti assegnati	Back-up periodico dei dati	Utilizzo di firewall
Verifica della restituzione dei documenti originali al termine delle operazioni affidate	Armadi blindati/ ignifughi	Inibizione di accesso a siti considerati non sicuri
Previsione di regole di custodia dei dati da parte degli incaricati durante le operazioni di trattamento		Utilizzo esclusivo di software con licenza
Identificazione e registrazione accessi dopo l'orario di chiusura degli archivi		
Formazione continua del personale		
Verifiche periodiche		
Certificazioni di qualità		
Adesione a codici di condotta		
Aggiornamento periodico della matrice dei rischi ed eventuale implementazione delle misure		
Regolamento interno di condotta		

Appendice

1. **Linee guida sui responsabili della protezione dei dati**

(a pagina seguente)

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

16/IT
WP 243 rev. 01

Linee guida sui responsabili della protezione dei dati

Adottate il 13 dicembre 2016
Versione emendata e adottata in data 5 aprile 2017

Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e Stato di diritto) della Commissione europea, direzione generale Giustizia e consumatori, B -1049 Bruxelles, Belgio, ufficio MO59 05/35.

Sito Internet: http://ec.europa.eu/justice/data-protection/index_en.htm

IL GRUPPO DI LAVORO SULLA TUTELA DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli Articoli 29 e 30 della stessa,

visto il proprio regolamento,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

Indice

4

1. Introduzione

Il regolamento generale sulla protezione dei dati (RGPD)[1], che esplicherà i propri effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di *compliance* per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (*accountability*). I responsabili della protezione dei dati (RPD) saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del RGPD.

In base al RGPD, alcuni titolari del trattamento e responsabili del trattamento sono tenuti a nominare un RPD[2]. Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali.

Anche ove il regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia gli approcci di questo genere.

La figura del RPD non costituisce una novità assoluta. La direttiva 95/46/CE[3] non prevedeva alcun obbligo di nomina di un RPD, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni.

Ancor prima dell'adozione del RGPD, il Gruppo di lavoro ha sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del RPD possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese[4]. Oltre a favorire l'osservanza attraverso strumenti di *accountability* (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione

[1] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119, 4.5.2016). Il RGPD è rilevante ai fini del SEE e sarà applicabile una volta incorporato nell'Accordo relativo al SEE.

[2] La nomina di un RPD è obbligatoria anche con riguardo alle autorità competenti di cui all'articolo 32 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119, 4.5.2016), alla luce della normativa nazionale di recepimento. Le presenti linee guida guardano con particolare attenzione alla figura del RPD come prevista dal RGPD, ma le indicazioni in esse formulate valgono anche per i RPD previsti dalla direttiva 2016/680 con riferimento alle disposizioni di carattere analogo contenute nei due strumenti.

[3] Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GU L 281, 23.11.95).

[4] Si veda http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

dei dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.

I RPD non rispondono personalmente in caso di inosservanza del RGPD. Quest'ultimo chiarisce che spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, paragrafo 1). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

Inoltre, al titolare del trattamento o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il RPD è preposto. La nomina di un RPD è solo il primo passo, perché il RPD deve disporre anche di autonomia e risorse sufficienti per svolgere in modo efficace i propri compiti.

Il RGPD riconosce nel RPD uno degli elementi chiave all'interno del nuovo sistema di *governance* dei dati, e prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici. Le presenti linee guida intendono fare chiarezza sulle pertinenti disposizioni del regolamento al fine di favorire l'osservanza della normativa da parte di titolari del trattamento e responsabili del trattamento; inoltre, le linee guida vogliono essere di ausilio ai RPD nell'esecuzione dei compiti loro attribuiti. Il presente documento contiene anche alcune raccomandazioni, in termini di migliori prassi, che scaturiscono dall'esperienza accumulata in alcuni Stati membri. Il Gruppo di lavoro monitorerà l'attuazione delle linee guida qui presentate e provvederà alle integrazioni che si riveleranno opportune.

2. Nomina di un RPD

2.1. Nomina obbligatoria

In base all'articolo 37, paragrafo 1, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici[5]:

[5] Si osservi che, in base all'articolo 37, paragrafo 4, il diritto dell'Unione o dello Stato membro può prevedere casi ulteriori di nomina obbligatoria di un RPD.

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico[6];

b) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure

c) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati[7] o[8] di dati personali relativi a condanne penali e reati[9].

Nelle sottosezioni che seguono, il Gruppo di lavoro fornisce indicazioni sui criteri e sulle formulazioni utilizzati all'articolo 37, paragrafo 1.

Tranne quando sia evidente che un soggetto non è tenuto a nominare un RPD, il Gruppo di lavoro raccomanda a titolari del trattamento e responsabili del trattamento di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RPD, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti[10]. Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario, per esempio se i titolari del trattamento o i responsabili del trattamento intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'articolo 37, paragrafo 1.

Se si procede alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli articoli 37-39 per quanto concerne la nomina stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.

Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un RPD e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli

[6] Con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali. V. articolo 32 della direttiva (UE) 2016/680.
[7] Ai sensi dell'articolo 9, si tratta dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell'identificazione univoca di una persona fisica, e di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.
[8] Nel testo in lingua inglese dell'articolo 37, paragrafo 1, lettera c) compare la congiunzione "*and*" (e); si veda il paragrafo 2.1.5 *infra* per maggiori chiarimenti sull'utilizzo della congiunzione "o" anziché "e" nello specifico contesto.
[9] Articolo 10.
[10] Si veda l'articolo 24, paragrafo 1.

interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di responsabile per la protezione dei dati (RPD)[11].

Il RPD viene designato, su base obbligatoria o meno, per tutti i trattamenti svolti dal titolare del trattamento o dal responsabile del trattamento.

2.1.1. "AUTORITÀ PUBBLICA O ORGANISMO PUBBLICO"

Nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il Gruppo di lavoro ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico[12]. In questi casi la nomina di un RPD è obbligatoria.

Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri[13] non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.

In tutti questi casi la situazione in cui versano gli interessati è probabilmente molto simile a quella in cui il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. Più in particolare, i trattamenti perseguono finalità simili e spesso il singolo ha, in modo analogo, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali; pertanto, è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un RPD.

Benché nei casi sopra descritti non sussista l'obbligo di nominare un RPD, il Gruppo di lavoro raccomanda, in termini di buone prassi, che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD. Le attività del RPD nominato nei termini sopra indicati si estendono a tutti i trattamenti svolti, compresi quelli che non sono connessi all'espletamento di funzioni pubbliche o all'esercizio di pubblici poteri quali, per esempio, la gestione di un database del personale.

[11] Queste considerazioni valgono anche per i *chief privacy officers* (CPO) o altri professionisti in materia di privacy già operanti presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel regolamento per quanto riguarda, per esempio, le risorse disponibili o le salvaguardie della loro indipendenza e che, in tal caso, non possono essere considerati e denominati "RPD".
[12] Si vedano, per esempio, le definizioni di "ente pubblico" e "organismo di diritto pubblico" contenute nell'articolo 2, paragrafi 1 e 2, della direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico.
[13] Articolo 6, paragrafo 1, lettera e).

2.1.2. "ATTIVITÀ PRINCIPALI"

L'articolo 37, paragrafo 1, lettere b) e c), del RGPD contiene un riferimento alle "*attività principali del titolare del trattamento o del responsabile del trattamento"*. Nel considerando 97 si afferma che le attività principali di un titolare del trattamento "*riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria*". Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento.

Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un RPD.

A titolo di ulteriore esemplificazione, si può citare il caso di un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L'attività principale dell'impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali. Ne consegue che anche l'impresa in oggetto deve nominare un RPD.

D'altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

2.1.3. "LARGA SCALA"

In base all'articolo 37, paragrafo 1, lettere b) e c), del RGPD, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito[14].

[14] Il considerando in questione vi ricomprende, in particolare, "*trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*".

In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il Gruppo di lavoro intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina di un RPD.

A ogni modo, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile del trattamento specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

D'altro canto, lo stesso considerando prevede in modo specifico che "*Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato*". Si deve tener conto del fatto che il considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che fra tali estremi si colloca un'ampia zona grigia. Inoltre, va sottolineato che il considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un RPD negli stessi identici termini.

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

2.1.4. "MONITORAGGIO REGOLARE E SISTEMATICO"

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "*monitoraggio del comportamento di detti interessati*"[15] ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati[16].

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per

[15] "*Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali*."

[16] Si osservi che il considerando 24 riguarda l'applicazione extraterritoriale del RGPD; inoltre, vi è una differenza fra l'espressione "*monitoraggio del loro comportamento*" (articolo 3, paragrafo 2, lettera b)) e "*monitoraggio regolare e sistematico degli interessati*" (articolo 37, paragrafo 1, lettera b)), per cui le due espressioni potrebbero ben riferirsi a concetti distinti.

finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

2.1.5. CATEGORIE PARTICOLARI DI DATI E DATI RELATIVI A CONDANNE PENALI E A REATI

Le disposizioni dell'articolo 37, paragrafo 1, lettera c), riguardano il trattamento di categorie particolari di dati ai sensi dell'articolo 9 *e* di dati personali relativi a condanne penali e a reati di cui all'articolo 10. Nonostante l'utilizzo della congiunzione "e" nel testo, non vi sono motivazioni sistematiche che impongano l'applicazione simultanea dei due criteri. Pertanto, il testo deve essere interpretato come se recasse la congiunzione "o". [NdT: il testo italiano del regolamento reca già la congiunzione "o"]

2.2. RPD del responsabile del trattamento

Per quanto riguarda la nomina di un RPD, l'articolo 37 non distingue fra titolari del trattamento [17] e responsabili del trattamento[18] in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro a dover nominare un RPD; questi ultimi saranno poi tenuti alla reciproca collaborazione.

Vale la pena di evidenziare che anche qualora il titolare del trattamento sia tenuto, in base ai criteri suddetti, a nominare un RPD, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi.

Alcuni esempi:

- Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oltre all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte

[17] Ai sensi della definizione contenuta all'articolo 4, punto 7, il titolare del trattamento è la persona o l'organismo che determina le finalità e i mezzi del trattamento.
[18] Ai sensi della definizione contenuta all'articolo 4, punto 8, il responsabile del trattamento è la persona o l'organismo che tratta dati personali per conto del titolare del trattamento.

dall'azienda e dai clienti non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata di attività. Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare, svolge, nel suo complesso, trattamenti su larga scala. Ne deriva che il responsabile del trattamento deve nominare un RPD ai sensi dell'articolo 37, paragrafo 1, lettera b); al contempo, l'azienda in quanto tale non è soggetta all'obbligo di nomina del RPD.

- Un'azienda di medie dimensioni che produce rivestimenti in ceramica incarica un responsabile esterno della gestione dei servizi di salute occupazionale; tale responsabile ha un numero elevato di clienti con caratteristiche analoghe. Il responsabile del trattamento è tenuto a nominare un RPD ai sensi dell'articolo 37, paragrafo 1, lettera b), poiché svolge trattamenti su larga scala. Tuttavia, l'azienda non è tenuta necessariamente allo stesso adempimento.

Il RPD nominato da un soggetto responsabile del trattamento vigila anche sulle attività svolte da tale soggetto quando operi in qualità di autonomo titolare del trattamento – per esempio, rispetto ai dati concernenti il personale, le risorse informatiche, la logistica.

2.3. Designazione di un unico RPD per più organismi

L'articolo 37, paragrafo 2, consente a un gruppo imprenditoriale di nominare un unico RPD a condizione che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati[19], l'autorità di controllo[20] e i soggetti interni all'organismo o all'ente, visto che uno dei compiti del RPD consiste nell' "*informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento*"[21].

Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD[22].

Il RPD, se necessario con il supporto di un *team* di collaboratori, deve essere in grado di comunicare con gli interessati[23] in modo efficiente e di collaborare[24] con le autorità di

[19] V. articolo 38, paragrafo 4: "*Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento*."
[20] V. articolo 39, paragrafo 1, lettera e): "*fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione*."
[21] Articolo 39, paragrafo 1, lettera a).
[22] V. anche paragrafo 2.6 *infra*.
[23] V. articolo 12, paragrafo 1: "*Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.*"

controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

Ai sensi dell'articolo 37, paragrafo 3, è ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare del trattamento o il responsabile del trattamento deve assicurarsi che un unico RPD, se necessario supportato da un *team* di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

2.4. Accessibilità e localizzazione del RPD

Ai sensi dell'articolo 4 [sic] del RGPD, l'accessibilità del RPD deve essere effettivamente tale. Per garantire tale accessibilità, il Gruppo di lavoro raccomanda che il RPD sia localizzato nel territorio dell'Unione europea, indipendentemente dal fatto che il titolare del trattamento o il responsabile del trattamento siano stabiliti nell'UE.

Tuttavia, non si può escludere che, in alcuni casi ove il titolare del trattamento o il responsabile del trattamento non sono stabiliti nell'UE[25], un RPD sia in grado di svolgere i propri compiti con maggiore efficacia operando al di fuori del territorio dell'UE.

2.5. Conoscenze e competenze del RPD

In base all'articolo 37, paragrafo 5, il RPD "*è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39*". Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

- **Conoscenze specialistiche**

Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a

[24] V. articolo 39, paragrafo 1, lettera d: "*cooperare con l'autorità di controllo.*"
[25] V. articolo 3 del RGPD per quanto concerne l'ambito territoriale di applicazione.

trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del RPD, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi.

- **Qualità professionali**

L'articolo 37, paragrafo 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un RPD; tuttavia, sono pertinenti al riguardo la conoscenza da parte del RPD della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del RGPD. Proficua anche la promozione di una formazione adeguata e continua rivolta ai RPD da parte delle Autorità di controllo.

E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento; inoltre, il RPD dovrebbe avere buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

- **Capacità di assolvere i propri compiti**

Per capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del RPD, sia quanto dipende dalla posizione del RPD all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il RPD dovrebbe perseguire in via primaria l'osservanza delle disposizioni del RGPD. Il RPD svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento[26], i diritti degli interessati[27], la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita[28], i registri delle attività di trattamento[29], la sicurezza dei trattamenti[30] e la notifica e comunicazione delle violazioni di dati personali[31].

- **RPD sulla base di un contratto di servizi**

[26] Capo II
[27] Capo III
[28] Articolo 25.
[29] Articolo 30.
[30] Articolo 32.
[31] Articoli 33 e 34.

La funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale RPD soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 del RGPD; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Pari importanza riveste il fatto che ciascuno dei soggetti in questione goda delle tutele previste dal RGPD: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto RPD, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di RPD. Al contempo, si potranno associare le competenze e le capacità individuali affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.

Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il *team* RPD, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del *team* RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

2.6. Pubblicazione e comunicazione dei dati di contatto del RPD

L'articolo 37, settimo paragrafo, del RGPD impone al titolare del trattamento o al responsabile del trattamento

- di pubblicare i dati di contatto del RPD, e
- di comunicare i dati di contatto del RPD alle pertinenti autorità di controllo.

Queste disposizioni mirano a garantire che tanto gli interessati (all'interno o all'esterno dell'ente/organismo titolare o responsabile del trattamento) quanto le autorità di controllo possano contattare il RPD in modo facile e diretto senza doversi rivolgere a un'altra struttura operante presso il titolare/responsabile del trattamento. Anche la confidenzialità riveste pari importanza; per esempio, i dipendenti possono essere riluttanti a presentare reclami al RPD se non viene garantita la confidenzialità delle loro comunicazioni. Il RPD è tenuto a osservare le norme in materia di segreto o confidenzialità nello svolgimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5).

I dati di contatto del RPD dovrebbero comprendere tutte le informazioni che consentono agli interessati e all'autorità di controllo di raggiungere facilmente il RPD stesso: recapito postale, numero telefonico dedicato e/o indirizzo dedicato di posta elettronica. Se opportuno, per facilitare la comunicazione con il pubblico, si potrebbero indicare anche canali ulteriori: una

hotline dedicata, un modulo specifico per contattare il RPD pubblicato sul sito del titolare/responsabile del trattamento.

In base all'articolo 37, settimo paragrafo, del RGPD non è necessario pubblicare anche il nominativo del RPD. Seppure ciò rappresenti con ogni probabilità di una buona prassi, spetta al titolare del trattamento o al responsabile del trattamento e allo stesso RPD stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze[32]. Tuttavia, comunicare il nominativo del RPD all'autorità di controllo è fondamentale affinché il RPD funga da punto di contatto fra il singolo ente o organismo e l'autorità di controllo stessa (articolo 39, paragrafo 1, lettera e)).

In termini di buone prassi, il Gruppo di lavoro raccomanda, inoltre, che il titolare/responsabile del trattamento comunichi ai dipendenti il nominativo e i dati di contatto del RPD. Per esempio, queste informazioni (nominativo e dati di contatto) potrebbero essere pubblicate sulla intranet del titolare/responsabile del trattamento, inserite nell'elenco telefonico interno e nei diversi organigrammi della struttura.

3. Posizione del RPD

3.1. Coinvolgimento del RPD in tutte le questioni riguardanti la protezione dei dati personali

Ai sensi dell'articolo 38 del RGPD, il titolare del trattamento e il responsabile del trattamento assicurano che il RPD sia "*tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*".

E' essenziale che il RPD, o il suo *team* di collaboratori, sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il RPD vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare del trattamento ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni[33]. Assicurare il tempestivo e immediato coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura

[32] Si osservi che l'articolo 33, paragrafo 3, lettera b), ove sono indicate le informazioni da fornire all'autorità di controllo e agli interessati in caso di violazione dei dati personali, prevede, a differenza dell'articolo 37, paragrafo 7, che tali informazioni comprendano anche il nominativo (e non solo le informazioni di contatto) del RPD.
[33] Articolo 35, paragrafo 2.

suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.

Ciò significa che occorrerà garantire, per esempio:

- che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il Gruppo di lavoro raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD;
- che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Ove opportuno, il titolare del trattamento o il responsabile del trattamento potrebbero mettere a punto linee guida ovvero programmazioni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria del RPD.

3.2. Risorse necessarie

L'articolo 38, paragrafo 2, del RGPD obbliga il titolare del trattamento o il responsabile del trattamento a sostenere il RPD "*fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*". Ciò si traduce, in modo particolare, nelle indicazioni seguenti:

- supporto attivo delle funzioni del RPD da parte del *senior management* (per esempio, a livello del consiglio di amministrazione);
- tempo sufficiente per l'espletamento dei compiti affidati al RPD. Ciò riveste particolare importanza se viene designato un RPD interno con un contratto part-time, oppure se il RPD esterno si occupa di protezione dati oltre a svolgere altre incombenze. In caso contrario, il rischio è che le attività cui il RPD è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità. E' fondamentale disporre di tempo sufficiente da dedicare allo svolgimento dei compiti previsti per il RPD; una prassi da raccomandare consiste nel definire la percentuale del tempo lavorativo destinata alle attività di RPD quando quest'ultimo svolga anche altre funzioni. Un'altra buona prassi consiste nello stabilire il tempo necessario per adempiere alle relative incombenze, definire il livello di priorità spettante a tale incombenze, e prevedere che il RPD stesso (ovvero l'azienda/l'organismo titolare o responsabile) rediga un piano di lavoro;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;

- comunicazione ufficiale della nomina del RPD a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/dell'organismo;
- accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al RPD supporto, informazioni e input essenziali;
- formazione permanente. I RPD devono avere la possibilità di curare il proprio aggiornamento con riguardo agli sviluppi nel settore della protezione dati. Ciò mira, in ultima analisi, a consentire un incremento continuo del livello di competenze proprio dei RPD, che dovrebbero essere incoraggiati a partecipare a corsi di formazione su materie attinenti alla protezione dei dati e ad altre occasioni di professionalizzazione (forum in materia di privacy, workshop, ecc.);
- alla luce delle dimensioni e della struttura della singola azienda/del singolo organismo, può risultare necessario costituire un ufficio o un gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale). In casi del genere, è opportuno definire con precisione la struttura interna del gruppo di lavoro nonché i compiti e le responsabilità individuali. Analogamente, se la funzione di RPD viene esercitata da un fornitore di servizi esterno all'azienda/all'organismo, potrà aversi la costituzione di un gruppo di lavoro formato da soggetti operanti per conto di tale fornitore e incaricati di svolgere le funzioni di RPD sotto la direzione di un responsabile che funga da contatto per il cliente.

In linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.

3.3. Istruzioni e [significato di] "adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente"

L'articolo 38, paragrafo 3, fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile del trattamento. In particolare, questi ultimi sono tenuti ad assicurare che il RPD "*non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti*". Il considerando 97 aggiunge che i RPD "*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente*".

Ciò significa che il RPD, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Tuttavia, l'autonomia del RPD non significa che quest'ultimo disponga di un margine decisionale superiore al perimetro dei compiti fissati nell'articolo 39.

Il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza[34]. Se il titolare del trattamento o il responsabile del trattamento assumono decisioni incompatibili con il RGPD e le indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al più alto livello del management e ai decisori. Al riguardo, l'articolo 38, paragrafo 3, prevede che il RPD "riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nel quadro della sue funzioni di informazione e consulenza a favore del titolare del trattamento o del responsabile del trattamento. Un altro esempio di tale rapporto diretto consiste nella redazione di una relazione annuale delle attività svolte dal RPD da sottoporre al vertice gerarchico.

3.4. Rimozione o penalizzazioni in rapporto all'adempimento dei compiti di RPD

L'articolo 38, paragrafo 3, prevede che il RPD "*non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti*".

Questa prescrizione mira a potenziare l'autonomia del RPD e ad assicurarne l'indipendenza nell'adempimento dei compiti assegnatigli, attraverso la previsione di un'adeguata tutela.

Il divieto di penalizzazioni menzionato nel RGPD si applica solo con riguardo a quelle penalizzazioni eventualmente derivanti dallo svolgimento dei compiti propri del RPD. Per esempio, un RPD può ritenere che un determinato trattamento comporti un rischio elevato e quindi raccomandare al titolare del trattamento o al responsabile del trattamento di condurre una valutazione di impatto, ma questi ultimi non concordano con la valutazione del RPD. In casi del genere non è ammissibile che il RPD sia rimosso dall'incarico per avere formulato la raccomandazione in oggetto.

Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta. Per esempio, potrebbero consistere nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al RPD in rapporto alle attività da questi svolte.

[34] Articolo 5, paragrafo 2.

Viceversa, e conformemente alle normali regole di gestione applicabili a ogni altro dipendente o fornitore soggetto alla disciplina del rispettivo contratto nazionale ovvero alle norme di diritto penale e del lavoro, sarebbe legittimamente possibile interrompere il rapporto con il RPD per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche.

In questo ambito va rilevato che il RGPD non specifica le modalità e la tempistica riferite alla cessazione del rapporto di lavoro del RPD o alla sua sostituzione. Tuttavia, quanto maggiore è la stabilità del contratto stipulato con il RPD e maggiori le tutele previste contro l'ingiusto licenziamento, tanto maggiore sarà la probabilità che l'azione del RPD si svolga in modo indipendente. Il Gruppo di lavoro vede, quindi, con favore ogni iniziativa assunta in tal senso dai titolari del trattamento e responsabili del trattamento.

3.5. Conflitto di interessi

In base all'articolo 38, paragrafo 6, al RPD è consentito di "*svolgere altri compiti e funzioni*", ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che "*tali compiti e funzioni non diano adito a un conflitto di interessi*".

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un RPD può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi. Ciò significa, in modo particolare, che un RPD non può rivestire, all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.

A seconda delle attività, delle dimensioni e della struttura organizzativa del titolare del trattamento o del responsabile del trattamento, si possono indicare le seguenti buone prassi:

- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di RPD;

- redigere regole interne a tale scopo onde evitare conflitti di interessi;
- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;
- dichiarare che il RPD non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di RPD, al fine di sensibilizzare rispetto al requisito in questione;
- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale RPD ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da prevenire conflitti di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il RPD sia designato fra soggetti interni o esterni all'organizzazione.

4. Compiti del RPD

4.1. Sorvegliare l'osservanza del RGPD

L'articolo 39, paragrafo 1, lettera b), affida al RPD, fra gli altri, il compito di sorvegliare l'osservanza del RGPD. Nel considerando 97 si specifica che il titolare del trattamento o il responsabile del trattamento dovrebbe essere "*assistito [dal RPD] nel controllo del rispetto a livello interno del presente regolamento*".

Fanno parte di questi compiti di controllo svolti dal RPD, in particolare,

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità,
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Il controllo del rispetto del regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza. Il RGPD chiarisce che spetta al titolare, e non al RPD, "*mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*" (articolo 24, paragrafo 1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del RPD.

4.2. Il ruolo del RPD nella valutazione di impatto sulla protezione dei dati

In base all'articolo 35, paragrafo 1, spetta al titolare del trattamento, e non al RPD, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo

inglese). Tuttavia, il RPD svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o *data protection by design*), l'articolo 35, paragrafo 2, prevede in modo specifico che il titolare "*si consulta*" con il RPD quando svolge una DPIA. A sua volta, l'articolo 39, paragrafo 1, lettera c) affida al RPD il compito di "*fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35*".

Il Gruppo di lavoro raccomanda che il titolare del trattamento si consulti con il RPD, fra l'altro, sulle seguenti tematiche[35]:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD.

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni[36].

Inoltre, il Gruppo di lavoro raccomanda che il titolare del trattamento definisca con chiarezza, per esempio nel contratto stipulato con il RPD, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa, i compiti specificamente affidati al RPD e i rispettivi ambiti, con particolare riguardo alla conduzione della DPIA.

4.3. Cooperazione con l'autorità di controllo e funzione di punto di contatto

In base all'articolo 39, paragrafo 1, lettere d) ed e), il RPD deve "cooperare con l'autorità di controllo" e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al

[35] I compiti del RPD sono elencati all'articolo 39, paragrafo 1, ove si specifica che il RPD deve svolgere "*almeno*" i compiti in questione. Ne deriva che niente vieta al titolare di assegnare al RPD compiti ulteriori rispetto a quelli espressamente menzionati all'articolo 39, paragrafo 1, ovvero di specificare ulteriormente i suddetti compiti.

[36] L'articolo 24, paragrafo 1, prevede che "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire,* ***ed essere in grado di dimostrare****, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".*

trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".

Questi compiti attengono al ruolo di "facilitatore" attribuito al RPD e già menzionato nell'introduzione alle presenti linee guida. Il RPD funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuitile dall'articolo 57 nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'articolo 58. Si è già rilevato che il RPD è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5); tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il RPD di contattare e chiedere lumi all'autorità di controllo. L'articolo 39, paragrafo 1, prevede che il RPD possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

4.4. Approccio basato sul rischio

In base all'articolo 39, paragrafo 2, il RPD deve "*considera[re] debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo*".

Si tratta di una disposizione di portata generale e ispirata a criteri di buon senso, verosimilmente applicabile sotto molti riguardi all'attività quotidiana del RPD. In sostanza, si chiede al RPD di definire un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati. Seppure ciò non significhi che il RPD debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, di fatto la disposizione segnala l'opportunità di dedicare attenzione prioritaria agli ambiti che presentino rischi più elevati.

Attraverso questo approccio selettivo e pragmatico, il RPD dovrebbe essere più facilmente in grado di consigliare al titolare quale metodologia seguire nel condurre una DPIA, a quali settori riservare un audit interno o esterno in tema di protezione dei dati, quali attività di formazione interna prevedere per il personale o gli amministratori che trattino dati personali, e a quali trattamenti dedicare maggiori risorse e tempo.

4.5. Il ruolo del RPD nella tenuta del registro delle attività di trattamento

L'articolo 30, primo e paragrafo 2, prevede che sia il titolare del trattamento o il responsabile del trattamento, e non il RPD, a "*ten[ere] un registro delle attività di trattamento svolte sotto la propria responsabilità*" ovvero "*un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento*".

Nella realtà, sono spesso i RPD a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE[37].

L'articolo 39, paragrafo 1, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, niente vieta al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento.

In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'articolo 30 deve essere considerato anche uno strumento che consente al titolare del trattamento e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione.

[37] Si veda l'articolo 24, paragrafo 1, lettera d), del regolamento (CE) 45/2001.

5. ALLEGATO ALLE LINEE GUIDA SUL RPD – INDICAZIONI ESSENZIALI

L'allegato intende rispondere, in forma sintetica e semplificata, ad alcune delle domande fondamentali rispetto al nuovo obbligo di designazione di un RPD fissato nel regolamento generale sulla protezione dei dati

Designazione del RPD

1. Chi è tenuto a designare un RPD?

La designazione di un RPD è obbligatoria:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
- se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Si tenga presente che la designazione obbligatoria di un RPD può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'UE. Inoltre, anche ove la designazione di un RPD non sia obbligatoria, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia un approccio di questo genere. Qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria.

Fonte: articolo 37(1) RGPD

2. Cosa significa "attività principali"?

Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare del trattamento o del responsabile del trattamento. Per esempio, il trattamento di dati relativi alla salute (come le cartelle sanitarie dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un RPD.

D'altra parte, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale ovvero dispongono di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o

perfino essenziali sono considerate solitamente di natura accessoria e non vengono annoverate fra le attività principali.

Fonte: articolo 37, paragrafo 1, lettere b) e c) RGPD

3. Cosa significa "su larga scala"?

Il regolamento non definisce cosa rappresenti un trattamento "su larga scala". Il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di *fast food*;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Fonte: articolo 37, paragrafo 1, lettere b) e c), RGPD

4. Cosa significa “monitoraggio regolare e sistematico”?

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all’interno del RGPD; tuttavia, esso comprende senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Non si tratta, però, di un concetto riferito esclusivamente all’ambiente online.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull’analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell’ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

L’aggettivo “regolare” ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L’aggettivo “sistematico” ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell’ambito di un progetto complessivo di raccolta di dati;
- svolto nell’ambito di una strategia.

Fonte*: *articolo 37, paragrafo 1, lettera b), RGPD

5. E’ ammessa la designazione congiunta di uno stesso RPD da parte di più soggetti? E a quali condizioni?

Sì. Un gruppo imprenditoriale può nominare un unico RPD a condizione che quest’ultimo sia “*facilmente raggiungibile da ciascuno stabilimento*”. Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati, l’autorità di controllo e i soggetti interni all’organismo o all’ente. Allo scopo di assicurare la raggiungibilità del RPD,

interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD. Il RPD, supportato da un apposito *team* se necessario, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.

È ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare del trattamento o il responsabile del trattamento deve assicurarsi che un unico RPD, se necessario supportato da un *team* di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici

Fonte: articolo 37, paragrafi 2) e 3), RGPD

6. Dove dovrebbe collocarsi il RPD?

Per garantire l'accessibilità del RPD, il Gruppo di lavoro raccomanda la sua collocazione nel territorio dell'Unione europea, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile nell'UE. Tuttavia, non si può escludere che un RPD sia in grado di adempiere ai propri compiti con maggiore efficacia operando al di fuori dell'UE in alcuni casi ove titolare del trattamento o responsabile del trattamento non sono stabiliti nel territorio dell'Unione europea.

7. Si può designare un RPD esterno?

Sì. Il RPD può far parte del personale del titolare del trattamento o del responsabile del trattamento (RPD interno) ovvero "*assolvere i suoi compiti in base a un contratto di servizi*". In quest'ultimo caso il RPD sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.
Se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un *team* operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale RPD soddisfi tutti i requisiti applicabili come fissati nel RGPD.
Per favorire efficienza e correttezza e prevenire conflitti di interesse a carico dei componenti il *team*, le linee guida raccomandano di procedere a una chiara ripartizione dei compiti nel *team* del RPD esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

30

Fonte: articolo 37, paragrafo 6, RGPD

8. Quali sono le qualità professionali che un RPD deve possedere?

Il RPD "*è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i [rispettivi] compiti*".

Il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto.

Fra le competenze e conoscenze specialistiche pertinenti rientrano le seguenti:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del RGPD;
- familiarità con le operazioni di trattamento svolte;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile:
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

Fonte: articolo 37, paragrafo 5, RGPD

Posizione del RPD

9. Quali sono le risorse che titolare del trattamento o responsabile del trattamento dovrebbero mettere a disposizione del RPD?

Il RPD deve disporre delle risorse necessarie per assolvere i propri compiti.

A seconda della natura dei trattamenti, e delle attività e dimensioni della struttura del titolare del trattamento o del responsabile del trattamento, il RPD dovrebbe poter contare sulle seguenti risorse:

- supporto attivo della funzione di RPD da parte del *senior management;*

- tempo sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della designazione del RPD a tutto il personale;
- accesso garantito ad altri servizi all'interno della struttura del titolare/del responsabile del trattamento in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

Fonte: articolo 38, paragrafo 2, RGPD

10. Quali sono le garanzie che possono consentire al RPD di operare con indipendenza? Cosa significa "conflitto di interessi"?

Vi sono numerose garanzie che possono consentire al RPD di operare in modo indipendente:

- nessuna istruzione da parte del titolare del trattamento o del responsabile del trattamento per quanto riguarda lo svolgimento dei compiti affidati al RPD;
- nessuna penalizzazione o rimozione dall'incarico in rapporto allo svolgimento dei compiti affidati al RPD;
- nessun conflitto di interessi con eventuali ulteriori compiti e funzioni.

Gli "altri compiti e funzioni" del RPD non devono comportare conflitti di interessi. Ciò significa, in primo luogo, che il RPD non può rivestire, all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.

A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione con riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare del trattamento o il responsabile del trattamento in un giudizio che tocchi problematiche di protezione dei dati.

Fonte: articolo 38, paragrafi 3 e 6, RGPD

Compiti del RPD

11. Che cosa si intende per "sorvegliare l'osservanza"

Fanno parte di questi compiti di controllo del RPD, in particolare,

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità, e
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare del trattamento o responsabile del trattamento.

Fonte: articolo 39, paragrafo 1, lettera b), RGPD

12. Il RPD è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati?

No, il RPD non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

13. Quale ruolo spetta al RPD con riguardo alla valutazione di impatto sulla protezione dei dati e alla tenuta del registro dei trattamenti?

Per quanto concerne la valutazione di impatto sulla protezione dei dati, il titolare del trattamento o il responsabile del trattamento dovrebbero consultarsi con il RPD, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

Per quanto riguarda il registro dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare del trattamento o sul responsabile del trattamento, e non sul RPD. Cionondimeno, niente vieta

al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento.

Fonte: articolo 39, paragrafo 1, lettera c) e articolo 30, RGPD

Fatto a Bruxelles, il 13 dicembre 2016

Per il Gruppo di lavoro,
La presidente
Isabelle FALQUE-PIERROTIN

Versione emendata e adottata in data 5 aprile 2017

Per il Gruppo di lavoro
La presidente
Isabelle FALQUE-PIERROTIN

34

2. Nuove FAQ presenti sul sito del Garante della Privacy sul Responsabile della Protezione dei Dati (RPD) in ambito privato

(in aggiunta a quelle adottate dal Gruppo Art. 29 in Allegato alle Linee guida sul RPD)

1. Chi è il responsabile della protezione dei dati personali (RPD) e quali sono i suoi compiti?

Il responsabile della protezione dei dati personali (anche conosciuto con la dizione in lingua inglese data protection officer – DPO) è una figura prevista dall'art. 37 del Regolamento (UE) 2016/679. Si tratta di un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del Regolamento medesimo. Coopera con l'Autorità (e proprio per questo, il suo nominativo va comunicato al Garante; v. faq 6) e costituisce il punto di contatto, anche rispetto agli interessati, per le questioni connesse al trattamento dei dati personali (artt. 38 e 39 del Regolamento).

2. Quali requisiti deve possedere il responsabile della protezione dei dati personali?

Il responsabile della protezione dei dati personali, al quale non sono richieste specifiche attestazioni formali o l'iscrizione in appositi albi, deve possedere un'approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento.

Deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza (considerando 97 del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici.

Il responsabile della protezione dei dati personali deve poter disporre, infine, di risorse (personale, locali, attrezzature, ecc.) necessarie per l'espletamento dei propri compiti.

3. Chi sono i soggetti privati obbligati alla sua designazione?

Sono tenuti alla designazione del responsabile della protezione dei dati personali il titolare e il responsabile del trattamento che rientrino nei casi previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679. Si tratta di soggetti le cui principali attività (in primis, le attività c.d. di "core business") consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o in trattamenti su larga scala di categorie particolari di dati personali o di dati relative a condanne penali e a reati (per quanto attiene alle nozioni di "monitoraggio regolare e sistematico" e di "larga scala", v. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243). Il diritto dell'Unione o degli Stati membri può prevedere ulteriori casi di designazione obbligatoria del responsabile della protezione dei dati (art. 37, par. 4).

Ricorrendo i suddetti presupposti, sono tenuti alla nomina, a titolo esemplificativo e non esaustivo: istituti di credito; imprese assicurative; sistemi di informazione creditizia; società finanziarie; società di informazioni commerciali; società di revisione contabile; società di recupero crediti; istituti di vigilanza; partiti e movimenti politici; sindacati; caf e patronati; società operanti nel settore delle "utilities" (telecomunicazioni, distribuzione di energia elettrica o gas); imprese di sommi-

nistrazione di lavoro e ricerca del personale; società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, terme, laboratori di analisi mediche e centri di riabilitazione; società di call center; società che forniscono servizi informatici; società che erogano servizi televisivi a pagamento.

4. Chi sono i soggetti per i quali non è obbligatoria la designazione del responsabile della protezione dei dati personali?

Nei casi diversi da quelli previsti dall'art. 37, par. 1, lett. b) e c), del Regolamento (UE) 2016/679, la designazione del responsabile del trattamento non è obbligatoria (ad esempio, in relazione a trattamenti effettuati da liberi professionisti operanti in forma individuale; agenti, rappresentanti e mediatori operanti non su larga scala; imprese individuali o familiari; piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti: v. anche considerando 97 del Regolamento, in relazione alla definizione di attività "accessoria").

In ogni caso, resta comunque raccomandata, anche alla luce del principio di "accountability" che permea il Regolamento, la designazione di tale figura (v., in proposito, le menzionate linee guida), i cui criteri di nomina, in tale evenienza, rimangono gli stessi sopra indicati.

5. È possibile nominare un unico responsabile della protezione dei dati personali nell'ambito di un gruppo imprenditoriale?

Il Regolamento (UE) 2016/679 prevede che un gruppo imprenditoriale (v. definizione di cui all'art. 4, n. 19) possa designare un unico responsabile della protezione dei dati personali, purché tale responsabile sia facilmente raggiungibile da ciascuno stabilimento (sul concetto di "raggiungibilità", v. punto 2.3 delle linee guida in precedenza menzionate). Inoltre, dovrà essere in grado di comunicare in modo efficace con gli interessati e di collaborare con le autorità di controllo.

6. Il responsabile della protezione dei dati personali deve essere un soggetto interno o può essere anche un soggetto esterno? Quali sono le modalità per la sua designazione?

Il ruolo di responsabile della protezione dei dati personali può essere ricoperto da un dipendente del titolare o del responsabile (non in conflitto di interessi) che conosca la realtà operativa in cui avvengono i trattamenti; l'incarico può essere anche affidato a soggetti esterni, a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento (UE) 2016/679 assegna a tale figura. Il responsabile della protezione dei dati scelto all'interno andrà nominato mediante specifico atto di designazione, mentre quello scelto all'esterno, che dovrà avere le medesime prerogative e tutele di quello interno, dovrà operare in base a un contratto di servizi. Tali atti, da redigere in forma scritta, dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

Nell'esecuzione dei propri compiti, il responsabile della protezione dei dati personali (interno o esterno) dovrà ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Il titolare o il responsabile del trattamento che abbia designato un responsabile per la protezione dei dati personali resta comunque pienamente responsabile dell'osservanza della normativa in materia di protezione dei dati e deve essere in grado di dimostrarla (art. 5, par. 2, del Regolamento; v. anche i punti 3.2 e 3.3. delle linee guida sopra richiamate).

I dati di contatto del responsabile designato dovranno essere infine pubblicati dal titolare o responsabile del trattamento. Non è necessario – anche se potrebbe rappresentare una buona

prassi – pubblicare anche il nominativo del responsabile della protezione dei dati: spetta al titolare o al responsabile e allo stesso responsabile della protezione dei dati, valutare se, in base alle specifiche circostanze, possa trattarsi di un'informazione utile o necessaria. Il nominativo del responsabile della protezione dei dati e i relativi dati di contatto vanno invece comunicati all'Autorità di controllo. A tal fine, allo stato, è possibile utilizzare il modello di cui al seguente link: http://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/7322292

7. Il ruolo di responsabile della protezione dei dati personali è compatibile con altri incarichi?

Si, a condizione che non sia in conflitto di interessi. In tale prospettiva, appare preferibile evitare di assegnare il ruolo di responsabile della protezione dei dati personali a soggetti con incarichi di alta direzione (amministratore delegato; membro del consiglio di amministrazione; direttore generale; ecc.), ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità e alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria, responsabile IT ecc.). Da valutare, in assenza di conflitti di interesse e in base al contesto di riferimento, l'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio, il responsabile della funzione legale).

8. Il responsabile della protezione dei dati personali è una persona fisica o può essere anche un soggetto diverso?

Il Regolamento (UE) 2016/679 prevede espressamente che il responsabile della protezione dei dati personali possa essere un "dipendente" del titolare o del responsabile del trattamento (art. 37, par. 6, del Regolamento); ovviamente, nelle realtà organizzative di medie e grandi dimensioni, il responsabile della protezione dei dati personali, da individuarsi comunque in una persona fisica, potrà essere supportato anche da un apposito ufficio dotato delle competenze necessarie ai fini dell'assolvimento dei propri compiti.

Qualora il responsabile della protezione dei dati personali sia individuato in un soggetto esterno, quest'ultimo potrà essere anche una persona giuridica (v. il punto 2.4 delle suddette Linee guida).

Si raccomanda, in ogni caso, di procedere a una chiara ripartizione di competenze, individuando una sola persona fisica atta a fungere da punto di contatto con gli interessati e l'Autorità di controllo.