



## **Rivista di diritto amministrativo**

Pubblicata in internet all'indirizzo [www.amministrativamente.com](http://www.amministrativamente.com)

**Diretta da**

Gennaro Terracciano, Gabriella Mazzei

**Direttore Responsabile**

Marco Cardilli

**Coordinamento Editoriale**

Luigi Ferrara, Giuseppe Egidio Iacovino,  
Carlo Rizzo, Francesco Rota, Valerio Sarcone

# FASCICOLO N. 5-6/2018

## estratto

Registrata nel registro della stampa del Tribunale di Roma al n. 16/2009

ISSN 2036-7821

## Comitato scientifico

Salvatore Bonfiglio, Gianfranco D'Alessio, Gianluca Gardini, Francesco Merloni, Giuseppe Palma, Angelo Piazza, Alessandra Pioggia, Antonio Uricchio, Vincenzo Caputi Jambrenghi, Annamaria Angiuli, Helene Puliat, J. Sánchez-Mesa Martínez, AndryMatilla Correa.

## Comitato dei referee

Gaetano Caputi, Marilena Rispoli, Luca Perfetti, Giuseppe Bettoni, Pier Paolo Forte, Ruggiero di Pace, Enrico Carloni, Stefano Gattamelata, Simonetta Pasqua, Guido Clemente di San Luca, Francesco Cardarelli, Anna Corrado, Fabrizio Cerioni, Gaetano Natullo, Paola Saracini, Mario Cerbone, Margherita Interlandi, Bruno Mercurio, Giuseppe Doria, Salvatore Villani.

## Comitato dei Garanti

Domenico Mutino, Mauro Orefice, Stefano Toschei, Giancarlo Laurini, Angelo Mari, Gerardo Mastrandrea, Germana Panzironi, Maurizio Greco, Filippo Patroni Griffi, Vincenzo Schioppa, Michel Sciascia, Raffaello Sestini, Leonardo Spagnoletti, Giuseppe Staglianò, Alfredo Storto, Alessandro Tomassetti, Italo Volpe.

## Comitato editoriale

Laura Albano, Daniela Bolognino, Caterina Bova, Sergio Contessa, Ambrogio De Siano, Fortunato Gambardella, Flavio Genghi, Massimo Pellingra, Stenio Salzano, Francesco Soluri, Giuliano Tagliaventi, Marco Tartaglione, Stefania Terracciano.

# **Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del Data Protection Officer (DPO): incidenza sulla attività della pubblica amministrazione**

**di Adriano Tortora\***

## Sommario

1. Introduzione – 2. I principi introdotti dal Regolamento GDPR – 3. Il Responsabile della protezione dei dati (RPD) – 4. Incidenza del RGPD sulla Pubblica Amministrazione – 5. Conclusioni.

## Abstract

In materia di protezione dei dati personali, il nuovo obiettivo dell'Unione è quello di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, implementando il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati in modo equivalente in tutti gli Stati membri.

E dunque, per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, si è ritenuto necessario (ed opportuno) disciplinare la materia con lo strumento normativo del Regolamento, direttamente applicabile su tutto il territorio europeo, che si propone di introdurre e cristallizzare nuovi principi generali della materia, utili sempre a sopperire l'eventuale carenza (oppure non chiarezza) delle disposizioni adottate a livello nazionale.

\*Avvocato. Docente di diritto amministrativo presso l'Università Unilink.

## 1. Introduzione

In virtù della rapidità dell'evoluzione tecnologica e della globalizzazione, la portata della condivisione e della raccolta di dati personali, negli ultimi decenni, è aumentata in modo significativo.

Per comprendere l'entità di tale fenomeno evolutivo, basti pensare al fatto che la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare enormi quantità di dati personali, come mai in precedenza, nello svolgimento delle loro attività.

Tale evoluzione richiede evidentemente, rispetto al passato, un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che possa consentire lo sviluppo dell'economia digitale in tutto il mercato interno europeo.

In proposito, l'articolo 16, paragrafo 2, TFUE conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati.

Con il Regolamento generale sulla protezione dei dati n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (d'ora in avanti Regolamento GDPR), l'Unione Europea ha ritenuto, appunto, di intervenire sulla materia sul presupposto dichiarato che sia "opportuno, dunque, che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche".

Sebbene, infatti, i suoi obiettivi e principi abbiano innovato con efficacia la materia, la precedente direttiva 95/46/CE (per anni punto di

riferimento della tutela dei dati e della privacy) non

ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche.

La compresenza, inoltre, di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri ha ostacolato la libera circolazione dei dati personali all'interno dell'Unione.

Tale divario creatosi nei livelli di protezione è dovuto alle divergenze realizzate nell'attuare e applicare, a livello nazionale, la direttiva 95/46/CE.

Queste differenze hanno costituito, pertanto, un freno all'esercizio delle attività economiche su scala dell'Unione, falsando la concorrenza e impedendo alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione.

Il nuovo obiettivo dell'Unione è, dunque, quello di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, implementando il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati in modo equivalente in tutti gli Stati membri.

A tal uopo, per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, si è ritenuto necessario (ed opportuno) disciplinare la materia con lo strumento normativo del Regolamento, diret-

tamente applicabile su tutto il territorio europeo.

Solo con tale mezzo, difatti, si possono avere maggiori certezze in termini di garanzia dei diritti e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offrendo alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento, assicurando altresì un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri.

Ovviamente, per il buon funzionamento della nuova disciplina, si sono ritenuti corollari imprescindibili:

- a) la libera circolazione dei dati personali all'interno dell'Unione, non limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- b) l'applicazione delle nuove misure di protezione alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali;
- c) il rafforzamento e la disciplina dettagliata dei diritti degli interessati e degli obblighi di coloro che effettuano e determinano il trattamento dei dati personali;
- d) l'attribuzione di poteri equivalenti per controllare e assicurare il rispetto delle norme di protezione dei dati personali e sanzioni equivalenti per le violazioni negli Stati membri;
- e) la neutralità della protezione delle persone fisiche sotto il profilo tecnologico (non dovrebbe dipendere dalle tecniche impiegate e dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio).

## 2. I principi introdotti dal regolamento gdpr

Alla luce dei suddetti ambiziosi obiettivi ed in considerazione delle nuove pratiche tecnologiche che intende disciplinare, il nuovo Regolamento si propone di introdurre e cristallizzare nuovi principi generali della materia, utili sempre a sopperire l'eventuale carenza (oppure non chiarezza) delle disposizioni adottate a livello nazionale.

Esso ha iniziato ad esplicare i propri effetti a partire dal 25 maggio 2018.

### 2.1. Principi applicabili al trattamento dei dati

All'art. 5 il Regolamento si preoccupa, sin da subito, di definire i principi-guida che devono sovrintendere a tutta l'attività di trattamento dei dati personali.

Innanzitutto si enuncia il principio di «liceità, correttezza e trasparenza», secondo cui i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

Specificazione del primo è il successivo criterio di "limitazione delle finalità" per cui i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati con modalità che non siano incompatibili con tali finalità.

Sul punto si precisa che un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o affini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali.

In relazione al profilo temporale, si enuncia il principio di "limitazione della conservazione", secondo il quale 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. Anche in questo caso i dati personali possono essere conservati per periodi più

lunghe a condizione che siano trattate esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal medesimo regolamento.

Sempre nella medesima ottica di limitazione si pone l'ulteriore principio di "minimizzazione dei dati" in virtù del quale essi devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Attinente ad un profilo prettamente qualitativo, è il principio dell' "esattezza" che impone di adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

Da ultimo si precisa che i dati debbano essere trattati con mezzi e modi che ne preservino l' "integrità e riservatezza", in modo cioè che venga garantita un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

## 2.1 Fondamenti di liceità del trattamento

In linea con la disciplina italiana dettata dal vigente Codice della privacy (D.L.vo 196/2003), il regolamento conferma che ogni trattamento di dati deve trovare fondamento in un' idonea base giuridica.

I fondamenti di liceità del trattamento sono indicati all'art. 6 del regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal Codice privacy - d.lgs. 196/2003.

In particolare si prevede che 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 (questa condizione non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti).

Sebbene in linea di principio, come detto, le suddette condizioni corrispondono a quella già individuate dalla precedente disciplina, numerose sono però le innovazioni introdotte dal Regolamento GDPR.

### 2.1.1 Il Consenso

Quanto al requisito del "Consenso", rispetto alla previgente disciplina, il Regolamento si preoccupa di precisare che in presenza di "dati sensibili" (art. 9) e/o di trattamenti automatizzati (art. 22), esso deve essere "esplicito".

Dal successivo art. 7, si comprende che esso non debba necessariamente avere forma scritta o essere "documentato per iscritto", essendo invece imprescindibile l'attestazione della sua inequivocabilità. In proposito nel primo comma del suddetto art. 7 è previsto che "il titolare del trat-

tamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali".

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando linguaggio semplice e chiaro.

Il rispetto delle suddette regole è previsto dal regolamento a pena di invalidità del consenso stesso.

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.

L'interessato dovrà, inoltre, essere preventivamente informato di tale potere di revoca e del fatto che la revoca deve avvenire nelle stesse modalità (e con la stessa facilità) con cui si è prestato il consenso.

Nel valutare se il consenso sia stato liberamente prestato, si deve tenere 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.

Con riferimento al consenso raccolto prima del 25 maggio 2018, il Garante per la protezione dei dati personali ha precisato che "Il consenso raccolto precedentemente al 25 maggio 2018 resta valido se ha tutte le caratteristiche sopra individuate. In caso contrario, è opportuno adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati secondo quanto prescrive il regolamento, se si vuole continuare a fare ricorso a tale base giuridica. In particolare, occorre verificare che la richiesta di consenso sia chiaramente distinguibile da altre

richieste o dichiarazioni rivolte all'interessato (art. 7.2), per esempio all'interno di moduli. Prestare attenzione alla formula utilizzata per chiedere il consenso: deve essere comprensibile, semplice, chiara (art. 7.2). I soggetti pubblici non devono, di regola, chiedere il consenso per il trattamento dei dati personali (si vedano considerando 43, art. 9, altre disposizioni del Codice: artt. 18, 20)".

### 2.1.2 Interesse vitale di un terzo

In mancanza delle altre condizioni di liceità di cui all'art. 6, il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica.

Come detto, si tenga presente che il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica può avere luogo unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica.

Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

In virtù della nuova linea di "responsabilizzazione" che pervade l'intero Regolamento GDPR, il bilanciamento tra il legittimo interesse del titolare o del terzo e diritti (e libertà) dell'interessato non spetta all'Autorità ma è compito dello stesso titolare.

Al fine di procedere al suddetto bilanciamento si dovrà tenere presente che i legittimi interessi di un titolare del trattamento, compresi quelli di un titolare del trattamento a cui i dati perso-

nali possono essere comunicati, o di terzi possono costituire una base giuridica del trattamento medesimo, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento.

Per meglio comprendere tale concetto, il Regolamento offre, al considerando n. 47, alcuni criteri ed esempi che consentano altresì di effettuare il bilanciamento: "Ad esempio, potrebbero sussistere tali legittimi interessi quando esista una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è un cliente o è alle dipendenze del titolare del trattamento. In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali. Posto che spetta al legislatore prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali, la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti. Costituisce parimenti legittimo interesse del titolare del trattamento interessato trattare dati personali strettamente necessari a fini di prevenzione delle frodi. Può essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto".

Tali criteri sembrano porsi, in realtà, in linea di continuità con quelli enunciati dal Garante per

la Protezione dei dati personali in materia di "Trattamento dei dati personali e videosorveglianza" e di "Utilizzo di un sistema informatico antifrode nell'ambito delle transazioni di commercio elettronico effettuate attraverso il sito web aziendale".

### 2.1.3 Esecuzione di un contratto e adempimento di un obbligo legale

Entrambi i suddetti requisiti si riferiscono alla presenza di un'obbligazione che può essere di natura convenzionale oppure di natura legale.

Nel primo caso, il trattamento dovrebbe essere considerato lecito se è necessario nell'ambito di un contratto o ai fini della conclusione di un contratto.

Nel secondo caso, il trattamento dovrebbe essere considerato lecito se è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.

Il regolamento non impone, tuttavia, che vi sia un atto legislativo specifico per ogni singolo trattamento.

Un atto legislativo può essere sufficiente come base per più trattamenti effettuati conformemente a un obbligo legale cui è soggetto il titolare del trattamento o se il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri.

Dovrebbe altresì spettare al diritto dell'Unione o degli Stati membri stabilire la finalità del trattamento e se il titolare del trattamento che esegue un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri debba essere una pubblica autorità o altra persona fisica o giuridica di diritto pubblico o, qualora sia nel pubblico interesse, anche per finalità inerenti alla salute, quali la sanità pubblica e la protezione sociale e la gestione dei servizi di assistenza sanitaria, di diritto privato, quale un'associazione professionale.

## 2.2. L'informativa ed il suo contenuto

In un'ottica di implementazione della tutela del soggetto interessato, gli artt. 13 e 14 del Regolamento hanno elencato in maniera tassativa quelli che devono necessariamente essere i contenuti dell'informativa che il titolare dei dati deve fornire al soggetto interessato, aggiungendo nuovi obblighi rispetto al passato.

Dovranno essere, oggi, oggetto di necessaria informazione:

- 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.

Particolarmente innovativi ed incisivi sono gli obblighi per il titolare di indicare la base giuridica del trattamento e specificare i dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente.

Il regolamento prevede anche ulteriori informazioni in quanto "necessarie per garantire un

trattamento corretto e trasparente": in particolare, il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Inoltre, se il trattamento comporta processi decisionali automatizzati (anch'essa profilazione), l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

Quanto alle modalità con cui deve essere resa l'informativa, l'art. 12 del Regolamento prevede che essa debba essere fornita "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".

Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito web. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online.

Dato che i minori meritano una protezione specifica, quando il trattamento dei dati riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente.

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.

Anche con riferimento all'informativa, è necessario che i titolari dei dati verificano la corrispondenza delle informative utilizzate a tutti i criteri introdotti dal Regolamento, con particolare attenzione ai nuovi contenuti obbligatori e alle prescritte modalità di redazione della stessa.

Con riferimento a quasi tutte le innovazioni introdotte dal Regolamento in relazione all'informativa, il Garante per la protezione dei dati personali ritiene estensibili in via analogica le considerazioni svolte, in passato, sui precedenti strumenti normativi.

### 2.3 Diritti degli interessati

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

Principio cardine è quello per cui il titolare del trattamento deve agevolare l'esercizio dei diritti dell'interessato e non può rifiutare di soddisfare la richiesta dell'interessato al fine di esercitare i suoi diritti, salvo che il titolare del trattamento dimostri che non è in grado di identificare l'interessato.

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

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

In vista dell'imminente operatività del Regolamento GDPR è opportuno che i titolari di trattamento adottino le misure tecniche e organizzative eventualmente necessarie per favorire l'esercizio dei diritti e il riscontro alle richieste presentate dagli interessati, che – a differenza

di quanto attualmente previsto – dovrà avere per impostazione predefinita forma scritta (anche elettronica).

A tal uopo potranno risultare utili le indicazioni fornite, nel corso degli anni, dal Garante per la protezione dei dati personali con riguardo all'intelligibilità del riscontro fornito agli interessati e alla completezza del riscontro stesso.

Pur essendo l'esercizio dei diritti, in linea di principio, gratuito, da ultimo si deve rendere conto della possibilità per il titolare dei dati di stabilire l'ammontare di un eventuale contributo da pretendere dall'interessato, là dove quest'ultimo avanzi richieste totalmente infondate o eccessive.

#### 2.3.1 Diritto di accesso

Diritto imprescindibile dell'interessato è quello di accesso ai propri dati, oggetto di trattamento. Costui ha il diritto inoltre 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.

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 del Regolamento, relative al trasferimento.

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.

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

### 2.3.2 Diritto all'oblio

In considerazione della enorme rilevanza che la questione del diritto all'oblio ha assunto negli ultimi anni, a causa della persistenza delle informazioni sul web e sui social network, anche oltre la morte del soggetto interessato, il Legislatore Europeo ha voluto esplicitare alcuni concetti e regole, dedicandovi un apposito articolo del Regolamento.

Ai sensi dell'art. 17, infatti, viene espressamente previsto che 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.

Il titolare del trattamento, dunque, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1 dell'art. 17, 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.

Sono escluse dalle suddette regole le situazioni in cui sia necessario mantenere le suddette informazioni:

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 del Regolamento;

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.

E' possibile rinvenire la ratio di tale disposizione nel Considerando n. 65 del Regolamento, in cui si chiarisce che "Un interessato dovrebbe avere il diritto di ottenere la rettifica dei dati personali che la riguardano e il «diritto all'oblio» se la conservazione di tali dati viola il presente regolamento o il diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento. In particolare, l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in particolare rilevante se l'interessato ha prestato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal tratta-

to, e vuole successivamente eliminare tale tipo di dati personali, in particolare da internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non sia più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria"

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

### 2.3.3 Diritto di limitazione del trattamento

In linea con il diritto "al blocco" del trattamento dei dati, previsto in Italia dall'art. 7, comma 3, lett. a) del Codice della Privacy, il Legislatore Europeo ha ritenuto di rinforzare tale disciplina ampliando le ipotesi in cui l'interessato al trat-

tamento dei dati abbia il diritto di pretenderne la limitazione.

Le nuove modalità di limitazione, reputate più efficaci, consistono essenzialmente nel trasferimento temporaneo dei dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati da un sito web.

Quanto agli archivi automatizzati, la limitazione del trattamento dei dati personali dovrebbe in linea di massima, essere assicurata mediante dispositivi tecnici in modo tale che i dati personali non siano sottoposti a ulteriori trattamenti e non possano più essere modificati. Il sistema dovrebbe indicare chiaramente che il trattamento dei dati personali è stato limitato.

In particolare, ai sensi dell'art. 18 del Regolamento, 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, del Regolamento in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Se il trattamento è limitato a norma del paragrafo 1 dell'art. 18, tali dati personali sono trat-

tati, 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.

L'interessato che ottiene la limitazione del trattamento dovrà, inoltre, essere informato dal titolare del trattamento prima che detta limitazione sia revocata.

### 2.3.4 Diritto alla portabilità dei dati

Mutuandolo da altri settori legati alla tutela dei consumatori, l'articolo 20 del Regolamento introduce il nuovo diritto alla portabilità dei dati, che per molti aspetti si differenzia dal diritto di accesso pur essendo a quest'ultimo strettamente connesso.

Il diritto alla portabilità dei dati permette agli interessati di ricevere i dati personali da loro forniti al titolare del trattamento, in un formato strutturato, di uso comune e leggibile meccanicamente, e di trasmetterli a un diverso titolare. L'obiettivo ultimo è accrescere il controllo degli interessati sui propri dati personali.

Consentendo la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, il diritto alla portabilità rappresenta anche uno strumento importante a supporto della libera circolazione dei dati personali nell'UE e in favore della concorrenza fra titolari. Questo nuovo diritto faciliterà il passaggio da un fornitore di servizi all'altro e potrà, quindi, favorire la creazione di nuovi servizi nel quadro della strategia per il mercato unico digitale.

Secondo la nuova disciplina, 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.

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

La scelta di limitare alle suddette ipotesi, i casi di portabilità dei dati, con conseguente obbligo per i titolari del trattamento di sviluppare formati interoperabili, nasce proprio dalla volontà del legislatore di implementare tale pratica e non creare particolari aggravii.

Non si applica, dunque, qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto.

Per sua stessa natura, tale diritto non può essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche.

Non dovrebbe pertanto applicarsi anche quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Da ultimo, qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non dovrebbe pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del presente regolamento.

Inoltre, si tenga presente che le modalità di esercizio del diritto in questione non dovrebbero pregiudicare il diritto dell'interessato di ottenere

la cancellazione dei dati personali e le limitazioni di tale diritto e non dovrebbero segnatamente implicare la cancellazione dei dati personali riguardanti l'interessato forniti da quest'ultimo per l'esecuzione di un contratto, nella misura in cui e fintantoché i dati personali siano necessari all'esecuzione di tale contratto.

### 2.3 Principio di responsabilizzazione

Al secondo comma dell'art. 5 del Regolamento viene esplicitato il principio fondamentale dell'intera riforma, quello della Responsabilizzazione (accountability, nell'accezione inglese).

Si afferma chiaramente, infatti, che "Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di dimostrarlo («responsabilizzazione»)»".

Al considerando n. 74 viene altresì spiegato che "È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche".

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Si è ritenuto, infatti, che un approccio standardizzato (e uguale per tutti) avrebbe il solo effetto di costringere i responsabili del trattamento

all'interno di strutture inadatte rivelandosi quindi fallimentare.

Le misure specifiche da applicare devono essere determinate in funzione dei fatti e delle circostanze di ciascun caso specifico, con particolare attenzione al rischio inerente al trattamento e al tipo di dati: per fare ciò si è ritenuto di delegarle ad un soggetto che, essendo a stretto contatto con l'ente titolare, non si limiti semplicemente ad applicarle, ma dovrà altresì individuarle.

Il regolamento pone con forza l'accento sul fatto che la "responsabilizzazione" si sostanzia nell'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare la sua applicazione.

A tal proposito, il Regolamento individua i criteri generali ai quali il titolare del trattamento dovrà uniformare la sua attività.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design", ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanzialmente in una serie di attività specifiche e dimostrabili.

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 dovrà

mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento.

Dette misure dovranno essere riesaminate e aggiornate qualora necessario.

Di fondamentale importanza in tale attività sarà la fase di valutazione del rischio inerente al trattamento.

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (si vedano artt. 35-36) tenendo conto dei rischi noti e evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano, come la notifica preventiva dei trattamenti all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del

titolare/responsabile e, appunto, di effettuazione di valutazioni di impatto in piena autonomia con eventuale successiva consultazione dell'Autorità, tranne alcune specifiche situazioni di trattamento (vedi art. 36, paragrafo 5 del regolamento). Peraltro, alle autorità di controllo, e in particolare al "Comitato europeo della protezione dei dati" (l'erede dell'attuale Gruppo "Articolo 29") spetterà un ruolo fondamentale al fine di garantire uniformità di approccio e fornire ausili interpretativi analitici: il Comitato è chiamato, infatti, a produrre linee-guida e altri documenti di indirizzo su queste e altre tematiche connesse, anche per garantire quegli adattamenti che si renderanno necessari alla luce dello sviluppo delle tecnologie e dei sistemi di trattamento dati.

#### 2.4 Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5 del Regolamento), devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art. 30.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico – indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali.

Per tale motivo, il Garante della Privacy invita tutti i titolari di trattamento e i responsabili, a prescindere dalle dimensioni

dell'organizzazione, a compiere i passi necessari per dotarsi di tale registro e, in ogni caso, a compiere un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche – ove già non condotta.

I contenuti del registro sono fissati, come detto, nell'art. 30; tuttavia, niente vieta a un titolare o responsabile di inserire ulteriori informazioni se lo riterrà opportuno proprio nell'ottica della complessiva valutazione di impatto dei trattamenti svolti.

#### 3. IL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

Espressione del suddetto approccio responsabilizzante del Regolamento è altresì la previsione della designazione di un "responsabile della protezione dati" (RPD ovvero DPO se si utilizza l'acronimo inglese Data Protection Officer).

Il responsabile della protezione dei dati è sicuramente il fulcro del descritto nuovo quadro giuridico in molti ambiti, avendo come principale obiettivo quello di facilitare l'osservanza delle disposizioni del RGPD.

In base al RGPD, alcuni titolari del trattamento e responsabili del trattamento sono obbligati a nominare un RPD.

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 nelle ipotesi in cui il regolamento non imponga espressamente la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria.

Come detto, infatti, questa figura rappresenta un elemento fondante ai fini della responsabilizzazione, facilitando l'osservanza della normativa e aumentando il margine competitivo

delle imprese: ciò in quanto, oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), essa potrà fungere 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 delle disposizioni del Regolamento, spettando al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento siano conformi alle disposizioni del regolamento stesso (articolo 24, paragrafo 1).

Inoltre, al titolare del trattamento o al responsabile del trattamento spetta il compito fondamentale di garantire l'autonomia del RPD consentendogli altresì, attraverso risorse adeguate, di svolgere in modo efficace i compiti cui è preposto.

### 3.1 I soggetti obbligati

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

- a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- 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 o di dati personali relativi a condanne penali e reati.

Anche qualora si proceda alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli articoli 37-39 del Regolamento per quanto concerne la nomina

stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.

#### 3.1 Definizione di Autorità pubblica o organismo pubblico.

Risulta di fondamentale importanza, per comprendere chi dovrà assolvere all'onere di nominare un Responsabile della Protezione dei dati, definire il contenuto dell'unica categoria obbligatoria alla sua nomina a prescindere dalla tipologia di attività esercitata: l'Autorità pubblica o gli organismi pubblici.

Dal momento che nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Si dovrà necessariamente ricorrere ad una nozione conforme al diritto nazionale.

Di conseguenza, 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.

In realtà, il compito di definire questa categoria diventa più oneroso, dal momento che lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri non sono proprie esclusivamente delle autorità pubbliche e degli 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, come ha chiarito il "Gruppo di lavoro articolo 29 per la protezione dei dati", "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".

In altre parole, 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.

In proposito, bisogna ricordare come 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.

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

#### **4. Incidenza del rgpd sulla pubblica amministrazione**

Visti e chiariti gli obblighi nascenti dal Regolamento RGPD per tutti gli Enti che trattano dati di terzi ed i particolari oneri previsti in capo agli Enti incaricati di funzioni pubbliche o che esercitano pubblici poteri (ad esempio con rife-

rimento alla nomina di un Responsabile per la protezione dati), si possono analizzare ed individuare nello specifico gli adempimenti che graveranno, sin dal 25 maggio 2018, su tutte le Pubbliche Amministrazioni.

Diventa prioritario, dunque, per ciascuna amministrazione o organismo pubblico definire internamente quale sia l'ufficio che si occupi stabilmente dell'adeguamento al GDPR, poi definire il DPO, la trasparenza del responsabile trattamento e le altre misure viste.

Gli adempimenti e le attività previste in capo a tali Enti sono sicuramente assai pregnanti in virtù delle particolari categorie di dati che trattano gli uffici pubblici (si pensi, ad esempio, ai dati sanitari, a quelli dei servizi sociali o dei tributi).

Per questo motivo, risulta essenziale per ogni Amministrazione pubblica individuare internamente quale sia l'ufficio che si occupi stabilmente dell'adeguamento al GDPR, in generale, degli adempimenti da questo previsti (dalla revisione delle informative alla istituzione e tenuta del registro delle attività di trattamento).

Successivamente dovrà:

- pianificare quanto prima un percorso ed un piano di formazione;
- stabilire aree di priorità di intervento;
- accantonare adeguate risorse in sede di approvazione di bilancio;
- prevedere risorse specifiche per la formazione del RPD;
- integrare la protezione dei dati con la digitalizzazione dei processi, con la riforma del Codice di Amministrazione digitale, con i codici di comportamento degli enti e con le ultime recenti novità normative in materia di trasparenza, prevenzione della corruzione, Foia e whistleblowing.

Inoltre, uno dei basilari nuovi adempimenti sarà quello dell'adozione (e dell'aggiornamento

continuo) di un registro delle attività di trattamento in cui riportare:

1. il nome e i dati di contatto del titolare del trattamento e del DPO;
2. le finalità del trattamento;
3. una descrizione delle categorie di interessati e delle categorie di dati personali;
4. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
5. i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
6. una descrizione generale delle misure di sicurezza tecniche e organizzative adottate dall'amministrazione.

#### 4.1. Individuazione e nomina del RPD

Come già accennato, tutte le Amministrazioni pubbliche saranno obbligate ad individuare e nominare un Responsabile della protezione dei dati personali.

E' bene subito specificare che il RPD può essere interno o esterno.

Nel primo caso, anche per salvaguardare la sua autonomia, non potrà coincidere con chi – all'interno dell'ente – definisce, anche in parte, le politiche di protezione dei dati personali.

Nel caso di DPO esterno, che dovrà stipulare un vero e proprio contratto di servizi con l'ente, il soggetto incaricato dovrà essere scelto all'esito di una procedura selettiva (in cui prevedere l'individuazione precisa dei requisiti di partecipazione e delle caratteristiche di esecuzione della prestazione).

Si tratta di una figura che deve possedere dei requisiti specifici e deve occuparsi prevalentemente di informare e fornire consulenza sulla corretta applicazione della normativa, curando con particolare attenzione la formazione del personale.

#### 4.1.1. 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.

Di seguito si riportano le indicazioni fornite per la scelta del RPD dal "Gruppo di Lavoro Articolo 29 per la protezione dei dati".

##### 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 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. Profi-

cua 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<sup>26</sup>, i diritti degli interessati<sup>27</sup>, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita<sup>28</sup>, i registri delle attività di trattamento<sup>29</sup>, la sicurezza dei trattamenti<sup>30</sup> e la notifica e comunicazione delle violazioni di dati personali.

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: un'A 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. 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.

#### **4.1.2 RPD esterno sulla base di un contratto di servizi**

La funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all’organismo o all’azienda titolare/responsabile del trattamento.

In tal caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale RPD soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 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 pre-

vedere che sia un solo soggetto a fungere da contatto principale e “incaricato” per ciascun utente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

#### **5. Conclusioni**

Sulla scorta delle svolte argomentazioni, si ritiene prioritario per ogni P.A., in considerazione della moltitudine di dati che si trovano a gestire, adattare la propria organizzazione alle prescrizioni contenute nel Regolamento GDPR, provvedendo sin da subito a nominare un RPD, eventualmente anche esterno, attraverso un contratto di servizi.