Regolamento privacy: novità e punti fermi della nuova disciplina

di Gianluca Satta (*)

L'articolo si propone di illustrare brevemente le principali novità in materia di protezione dei dati personali introdotte dal Reg. UE 2016/679. Il percorso affronta alcune questioni di carattere generale, dai principi ai presupposti di liceità delle attività di trattamento, fino all'analisi delle principali figure e degli adempimenti privacy, evidenziando, allo stesso tempo, i punti di continuità rispetto alla precedente disciplina in materia.

Introduzione

Questo articolo, il primo di una serie di appuntamenti che accompagneranno il lettore nel corso dei prossimi mesi, intende affrontare la tematica del nuovo Reg. UE 2016/679 ("Regolamento Generale in materia di Protezione dei Dati personali", di seguito anche "RGPD"), attraverso una breve panoramica generale, evidenziando gli aspetti più rilevanti tra le novità introdotte dalla nuova disciplina, che si applicherà a partire dal prossimo 25 maggio 2018. Nei prossimi contributi saranno, invece, affrontati nello specifico alcuni tra gli adempimenti *privacy* più importanti e delicati.

Il Reg. UE 2016/679 e la protezione dei dati personali

La protezione dei dati personali è un diritto pienamente riconosciuto e tutelato all'interno dei Trattati Europei (1). In particolare, il quadro normativo in materia è rappresentato, in primo luogo, dall'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea (2) che, con l'entrata in vigore del Trattato di Lisbona, ha acquisito il medesimo valore giuridico dei trattati europei e, pertanto, pienamente vincolante per l'Unione e per gli Stati membri. Un ulteriore richiamo all'esigenza di garantire un'adeguata protezione dei dati personali a livello europeo, è presente all'art. 16 del Trattato sul Funzionamento dell'Unione Europea (TFUE), che attribuisce al legislatore europeo l'obbligo di introdurre, nell'ambito dell'ordinamento europeo, norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale (3).

Note:

(*) Avvocato in Cagliari, cultore in materia di Diritto dell'Informatica presso l'Università degli Studi di Cagliari

(1) Il diritto alla *privacy*, inteso nella sua accezione moderna, dinamica e attiva, contempla non solo il diritto ad impedire la conoscenza, da parte di estranei, delle informazioni personali (secondo la vecchia impostazione statica e negativa del concetto), ma anche il diritto di ciascun individuo di controllare la raccolta, la classificazione e l'uso di quelle informazioni da parte di chi gestisce le banche dati, nelle quali le stesse sono inserite e conservate.

(2) L'art. 8 della Carta dei Diritti Fondamentali dell'UE, rubricato "Protezione dei dati di carattere personale" recita: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

(3) L'art. 16 TFUE dispone che "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti".

La disciplina europea in materia di protezione dei dati personali, fino all'entrata in vigore del Reg. UE 2016/679 (4), era costituita principalmente dalla Direttiva 95/46/CE (la c.d. Direttiva madre) e dall'insieme degli atti di recepimento di ciascun ordinamento degli Stati membri. In Italia, la Legge 31 dicembre 1996, n. 675 (5) è stato il primo testo normativo adottato in attuazione della Direttiva madre, successivamente abrogato e sostituito dal D.Lgs. 30 giugno 2003, n. 196 (Codice della *privacy*) (6).
Come rilevato dallo stesso legislatore europeo, nella parte dedicata ai "considerando" del nuovo Regolamento, l'insieme delle disposizioni normative, sin qui richiamate, ha contribuito a creare livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, diversi all'interno di ciascun Stato europeo, ostacolando la libera circolazione dei dati personali all'interno dell'Unione. Inoltre, le divergenze nell'attuazione e nell'applicazione della Direttiva 95/46/CE, hanno rappresentato un freno all'esercizio delle attività economiche su scala europea, in grado di falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione.
Per queste ragioni, si è ritenuto necessario intervenire attraverso l'emanazione del Reg. UE 2016/679, optando a favore di una fonte normativa in grado di produrre i propri effetti direttamente all'interno degli ordinamenti degli Stati membri, senza necessità di alcun atto di recepimento.
Il Regolamento, che insieme alla Direttiva UE 2016/680 costituisce il c.d. Pacchetto di protezione dei dati, è entrato in vigore il 24 maggio 2016, quattro anni dopo la sua presentazione ufficiale da parte della Commissione Europea, e si applicherà a partire dal 25 maggio 2018. L'obiettivo del legislatore europeo, infatti, è quello di garantire a tutti i destinatari delle norme del Regolamento (dagli Stati membri, ai privati ed alle Pubbliche amministrazioni) un tempo di due anni, a partire dalla data di entrata in vigore, per l'adeguamento alle nuove disposizioni normative.
Nei prossimi mesi, quindi, tutte le imprese e le Pubbliche amministrazioni dovranno attivarsi per allineare le proprie attività e i processi interni ai nuovi obblighi previsti dal Regolamento Generale.

Quando si applica il Regolamento europeo

Prima di affrontare nel dettaglio alcuni aspetti peculiari del nuovo assetto normativo offerto dal Regolamento, è bene chiarire i confini applicativi della disciplina, così da eliminare ogni dubbio circa l'estensione materiale (7) e territoriale (8) di queste nuove regole.
In primo luogo, sotto l'aspetto oggettivo, il Regolamento si applica a tutti i trattamenti di dati personali, automatizzati e non, effettuati da soggetti (titolari o responsabili del trattamento) che svolgono le proprie attività nell'Unione, indipendentemente dal luogo in cui sia effettuato il trattamento stesso. Inoltre, la nuova disciplina si estende anche nei confronti dei soggetti non stabiliti nell'Unione che, per offrire beni o fornire servizi o per svolgere attività di monitoraggio di comportamenti, trattano dati personali di interessati che si trovano nel territorio europeo. Il punto di riferimento, quindi, non è più rappresentato esclusivamente dal luogo ove si svolgono le operazioni di trattamento, ovvero dove si trova il soggetto che compie tali attività, bensì dal soggetto a cui i dati personali si riferiscono, ovverosia dall'interessato. Quest'ultimo, infatti, rappresentando la parte debole della catena, costituisce il fulcro attorno al quale ruotano tutte le disposizioni presenti nel Regolamento, anche quelle che ne delineano il profilo applicativo.
Da un punto di vista soggettivo, invece, gli obblighi e i principi si applicano sia ai soggetti privati (persone fisiche e/o giuridiche) sia alle autorità pubbliche (Pubbliche amministrazioni), i quali possono assumere il

Note:
(4) Reg. 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 - RGPD).
(5) Legge n. 675 del 31 dicembre 1996, recante "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" - Pubblicata sulla Gazzetta Ufficiale n. 5 dell'8 gennaio 1997 - Suppl. Ordinario n. 3.
(6) D.Lgs. 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" - Pubblicato sulla Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Suppl. Ordinario n. 123.
(7) Cfr. art. 2 RGPD.
(8) Cfr. art. 3 RGPD.

ruolo di titolari o di responsabili del trattamento (9).
Restano escluse, oltre a tutte le attività di trattamento che non rientrano nel campo di applicazione del diritto dell'Unione, tutti i trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (10).

I principi generali e i presupposti di liceità del trattamento

I principi e i presupposti di liceità del trattamento costituiscono i due principali binari che guidano l'attività di trattamento dei dati personali e dettano i confini entro i quali questa può muoversi.
I principi generali, già presenti nella disciplina della Direttiva 95/46/CE e nel Codice della *privacy* (11), sono degli enunciati che contengono le norme fondamentali che i titolari devono rispettare per il trattamento dei dati personali; inoltre, la loro corretta interpretazione ed applicazione, spesso, consente di risolvere molte questioni di carattere pratico che emergono nell'ambito delle attività di trattamento dati.
Rispetto alla precedente disciplina applicabile, il nuovo Regolamento ha ampliato e rafforzato la protezione dei dati personali e, parallelamente, anche le norme che dettano i principi generali sono stati modificati, attraverso una formulazione più esplicita e completa, e resi maggiormente coerenti con l'intenzione di garantire una tutela più efficace.
In particolare, il primo e più importante principio, che determina e delimita l'attività del trattamento, è quello di "limitazione della finalità", in base al quale i dati personali devono essere "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità" (12). Pertanto, in base a questo principio, rimasto pressoché identico alla precedente formulazione, ogni attività di trattamento è consentita solo se è ancorata ad una finalità (scopo); prima di procedere al trattamento, quindi, ciascun titolare deve individuare la finalità che intende perseguire.
Una volta individuati quali dati personali è possibile trattare in relazione alla finalità, è necessario determinare la misura entro la quale può effettuarsi il trattamento dei dati, attraverso l'applicazione del principio di "minimizzazione dei dati", in base al quale i dati personali oggetto di trattamento devono essere "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (13).
Un ulteriore importante principio è quello di "limitazione della conservazione", secondo il quale i dati personali 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" (14).
Infine, tra i principi generali sanciti dal Regolamento si colloca anche il nuovo paradigma della "*data protection by design and by default*" che ha assorbito il "principio di necessità" già previsto nel Codice della *privacy* (15). In forza di questo nuovo approccio alla

Note:
(9) Per trattamento si intende "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". In termini più sintetici, è possibile considerare trattamento ogni operazione che implica un semplice contatto con un dato personale.
(10) Sul punto, si veda il par. 2, lett. c) dell'art. 2 RGPD. In particolare, non è agevole tracciare i confini di una tale disposizione limitativa del campo di applicazione, se non altro perché occorrerebbe verificare di volta in volta se l'attività sottesa al trattamento (o meglio, la finalità che si intende perseguire con il trattamento di quei particolari dati personali) sia a carattere personale o domestico. In questa sede ci si limiterà ad esemplificare il caso, certamente escluso dall'ambito di applicazione delle norme del Regolamento, dei dati personali presenti nella rubrica del proprio *smartphone* rappresentati dal nome, dal cognome e dal numero di telefono dei propri amici e parenti; la raccolta, la memorizzazione nel telefono, la visualizzazione, e l'utilizzo di tali dati, costituiscono attività di trattamento eseguite per finalità esclusivamente personale o domestica. A dimostrazione della difficoltà di inquadramento dell'esclusione in esame, lo stesso non potrebbe dirsi per i dati personali presenti nella rubrica e riferiti a clienti o dipendenti, in quanto connessi con l'attività commerciale o professionale.
(11) Rispettivamente, l'art. 6 della Direttiva 95/46/CE e l'art. 11 del D.Lgs. 30 giugno 2003, n. 196.
(12) Art. 5, par. 1, lett. b), RGPD.
(13) Art. 5, par. 1, lett. c), RGPD.
(14) Art. 5, par. 1, lett. d), RGPD.
(15) Tale principio, sancito all'art. 3 del D.Lgs. 30 giugno 2003, n. 196, disponeva che "I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione dei dati personali e dei dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

privacy, infatti, il titolare del trattamento è tenuto ad adottare "misure tecniche e organizzative adeguate, quali la pseudonimizzazione (16), volte ad attuare in modo efficace i principi di protezione dei dati", sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, "e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati". Inoltre, il titolare deve garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari, con riferimento alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità, per ogni specifica finalità del trattamento (17).

Prima ancora di procedere all'adempimento degli obblighi *privacy*, qualunque attività di trattamento deve essere sempre preceduta, non solo dalla valutazione sul rispetto dei principi generali, ma anche dall'osservanza dei presupposti di liceità, che potrebbero definirsi come le condizioni in presenza delle quali il trattamento dei dati personali è considerato lecito.

Il presupposto di liceità per eccellenza è rappresentato dal consenso dell'interessato (sempre preceduto dall'informativa), ma non è l'unica base giuridica che giustifica e rende lecito il trattamento dei dati. L'art. 6 del Regolamento, infatti, prevede una serie di casi in cui il trattamento dei dati può essere effettuato anche senza il consenso dell'interessato a condizione che il trattamento sia necessario: all'esecuzione di misure precontrattuali o di un contratto di cui l'interessato è parte; per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento e, infine, 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 (18).

Sostanzialmente, per quanto concerne i presupposti di liceità del trattamento non vi sono particolari novità rispetto alla precedente disciplina prevista dall'art. 24 del Codice *privacy*, se non nel fatto che in caso di trattamento necessario per il perseguimento del legittimo interesse del titolare, il bilanciamento degli interessi non è più effettuato dall'Autorità Garante all'interno di un provvedimento, ma è compito del titolare stesso, in ragione del principio di responsabilizzazione, eseguire il bilanciamento dei propri interessi con gli interessi, i diritti e le libertà dell'interessato.

Per quanto concerne, invece, altre categorie particolari di dati personali (19) l'art. 9 RGPD, a differenza della precedente impostazione normativa del Codice *privacy*, prevede un divieto generale di trattamento, salvo i casi in cui ricorrono determinate condizioni, tra cui il consenso esplicito dell'interessato (20).

Note:

(16) L'art. 4 RGPD definisce la pseudonimizzazione come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile". Il richiamo alla pseudonimizzazione è meramente esemplificativo e non esaustivo. In ogni caso, tale modalità di trattamento non va confusa con l'anonimizzazione del dato che si ottiene rendendo impossibile l'identificazione o l'identificabilità dell'interessato.

(17) L'art. 25 RGPD prevede, inoltre, che il principio della "*data protection by design and by default*" sia attuato "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".

(18) Alla luce di quanto rilevato, si badi che, la richiesta del consenso pur in presenza di una condizione che permette il trattamento in sua assenza, oltre che non essere corretto, potrebbe comportare delle problematiche sul piano giuridico. Infatti, il titolare potrebbe ritrovarsi dinnanzi all'eventualità di non poter procedere al trattamento in quanto ha ottenuto il diniego dell'interessato, pur in presenza di un obbligo di legge o di un obbligo contrattuale nei confronti dello stesso interessato che gli impone di procedere. Per evitare situazioni così paradossali, è necessario valutare bene l'opportunità di procedere al trattamento sulla base del consenso o di altra base giuridica diversa.

(19) Il riferimento è alla "vecchia" categoria dei dati "sensibili". Il Regolamento non prevede più tale denominazione, pur mantenendo un regime di protezione speciale per queste tipologie di dati. Rientrano nell'ambito di questa categoria di dati (definita anche "dati particolarmente sensibili"): i 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.

(20) Le altre condizioni sono elencate dall'art. 9, par. 2, RGPD.

L'organizzazione interna e i principali adempimenti privacy

Senza dubbio, le più significative e rilevanti novità in materia sono previste dalle norme che disciplinano i soggetti del trattamento e la loro organizzazione, nonché quelle che prevedono gli adempimenti obbligatori in materia di trattamento dei dati personali. In questa sede, per ragioni di brevità, ci si limiterà ad esporre in modo molto sintetico le principali differenze rispetto alla precedente disciplina.

In primo luogo, nel Regolamento si è mantenuta l'organizzazione di tipo gerarchico-piramidale dei soggetti del trattamento (Tavola1).

In cima all'organizzazione si trova il "titolare del trattamento" (o *data controller*) (21) il quale ha il compito di determinare le finalità e i mezzi del trattamento, nonché di adottare tutti gli adempimenti previsti dalla normativa *privacy*. Il titolare conserva in capo alla propria persona la responsabilità generale per qualsiasi trattamento di dati personali che quest'ultimo effettua direttamente o che altri effettuano per suo conto. Allo stesso tempo, in forza del nuovo principio di responsabilizzazione (detto anche principio di *accountability*), il titolare del trattamento è tenuto a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento (22). Si tratta di una grande novità in materia di protezione dei dati personali, in quanto ai titolari viene affidato 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.

Proseguendo nella definizione delle figure, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, questi si definiscono "contitolari" e il loro rapporto è regolato dall'art. 26 RGPD.

Nell'ambito dei suoi ampi poteri organizzativi, il titolare può delegare una parte delle proprie funzioni e compiti a soggetti diversi, che prendono il nome di "responsabile del trattamento" (o *data processor*). A differenza del passato, l'art. 28 RGPD impone regole più precise per la sua designazione. In particolare, la nomina deve essere effettuata, nel rispetto della forma scritta (anche elettronica), mediante contratto o altro atto giuridico idoneo a vincolare il responsabile al titolare del trattamento (23). Inoltre, se previsto nell'atto di nomina, il responsabile può nominare, a sua volta, altri soggetti responsabili del trattamento (che, per comodità, possono definirsi "*sub*-responsabili").

Alla base della piramide, sebbene il nuovo Regolamento non preveda istituzionalmente la loro figura, vi sono i c.d. incaricati del trattamento, ovverosia tutti i soggetti autorizzati ad effettuare operazioni di trattamento su istruzione e sotto la diretta autorità del titolare o di un responsabile dallo stesso nominato (24). L'amministratore di sistema è una figura la cui nomina è obbligatoria, ed è prevista dal Provvedimento Generale dell'Autorità Garante del 27 novembre 2008 (25). In forza del citato provvedimento, all'amministratore

Note:

(21) L'art. 4, par. 1, n. 7, RGPD, definisce il titolare del trattamento: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

(22) L'adozione di tali misure deve essere calibrata tenendo conto di altri fattori quali: la natura, l'ambito di applicazione, il contesto e le finalità del trattamento, nonché il rischio per i diritti e le libertà delle persone fisiche.

(23) Il legislatore europeo, alla luce dell'importanza del rapporto tra titolare e responsabile del trattamento, all'art. 28, par. 3, RGPD ha dettato regole precise anche in merito al contenuto dell'atto di designazione.

(24) La presenza di soggetti, diversi dal titolare e dal responsabile del trattamento, si evince chiaramente dalla lettura dell'intero impianto normativo e, in particolare, dall'art. 29 RGPD, il quale dispone che "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". Non essendo contrario al dettato normativo, per comodità e per un senso di continuità con la precedente impostazione, questi soggetti possono essere definiti ancora "incaricati del trattamento". Inoltre, alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento, che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del Regolamento nella sua interezza, si ritiene opportuno che titolari e responsabili del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni, anche attraverso gli interventi del Garante.

Tavola 1 - Organizzazione gerarchica dei soggetti del trattamento

di sistema è delegata la gestione e la manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi *software* complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. Nell'ambito delle nuove disposizioni del Regolamento, la nomina dell'amministratore di sistema da parte del titolare del trattamento non può che rappresentare una forma di misura organizzativa adeguata per l'adozione di tutte le misure tecniche e informatiche a tutela dei dati personali, nel pieno rispetto del principio di responsabilizzazione (26).

Il *Data Protection Officer* (Responsabile della Protezione dei Dati - RPD) (27), al contrario delle precedenti figure, deve necessariamente essere collocato al di fuori dell'organizzazione gerarchico-piramidale, alla luce delle funzioni di controllo e di sorveglianza sull'osservanza del Regolamento, nonché dell'indipendenza e dell'assenza di conflitti di interesse, previste dalla normativa, che ne caratterizzano la posizione.

Le vere novità introdotte dalla disciplina del Regolamento *privacy*, sebbene in parte coinvolgano anche l'aspetto organizzativo interno (come nel caso della figura del *Data Protection Officer*), riguardano principalmente gli adempimenti del titolare del trattamento.

Come si evince dalla Tavola 2, nel nuovo

Note:

(25) Provv. Gen. 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008 - modificato il 25 giugno 2009).

(26) Sull'obbligatorietà o meno della figura dell'amministratore di sistema, si dovrà attendere l'esito delle modifiche del Codice della *privacy* ad opera dei Decreti delegati in forza dell'art. 13, Legge 25 ottobre 2017, n. 163. Infatti, qualora sia abrogato l'art. 154 del Codice, il Provvedimento Generale emanato dall'Autorità Garante perderà la sua efficacia e, conseguentemente, la figura dell'amministratore di sistema non sarà più obbligatoria. Tuttavia, fino a che non si avranno certezze sull'esito delle modifiche in via di approvazione, la nomina dell'amministratore di sistema permane obbligatoria.

(27) Tale figura non va confusa con il responsabile del trattamento.

Tavola 2 - Adempimenti privacy: cosa cambia rispetto al passato

Adempimenti privacy: cosa cambia rispetto al passato

Adempimento	Codice (D. Lgs. 196/2003)	RGPD (Reg. UE 2016/679)
Notifica dei trattamenti	SI	NO
Data breach + Registro violazioni	NO	SI
Informativa	SI	SI
Consenso	SI	SI
Registro dei trattamenti	NO	SI
Codice di condotta	NO	SI
Valutazioni di impatto	SI	SI *(codificata)*
Consultazione preventiva	SI	SI
Data protection by design and by default	NO	SI
DPO (Data Protection Officer)	NO	SI

Regolamento scompare l'obbligo di procedere alla notifica dei trattamenti. Senza entrare nel merito della disciplina di ciascun adempimento *privacy*, in linea di massima è possibile affermare che l'obbligo di notifica è stato sostituito, oggi, dall'obbligo di tenuta del registro dei trattamenti (28), accompagnato dall'obbligo di effettuare una valutazione di impatto quando il trattamento presenti dei rischi elevati per i diritti e le libertà delle persone fisiche coinvolte. Nel Regolamento, invece, si parla di obbligo di notifica a proposito delle violazioni dei dati personali, il c.d. *data breach*. In forza di tale adempimento, il titolare che subisce una violazione dei dati personali (29) è tenuto a notificare l'accaduto all'autorità di controllo nonché a tenere un registro nel quale deve annotarvi tutte le violazioni subite (se del caso, anche quelle non oggetto di notificazione).
Infine, per quanto riguarda gli adempimenti verso l'interessato, all'informativa e al consenso si aggiunge l'obbligo di comunicare all'interessato la violazione dei dati personali (c.d. *data breach* nei confronti dell'interessato), nonché tutti gli adempimenti funzionali a garantire l'esercizio dei diritti da parte dello stesso, ivi compresi le novità assolute rappresentate dal diritto all'oblio e dal diritto alla portabilità dei dati personali.

Note:
(28) Il registro dei trattamenti (art. 30 RGPD), sebbene rappresenti un adempimento nuovo, la sua struttura e il suo contenuto richiamano alla mente il Documento Programmatico sulla Sicurezza (DPS) previsto dall'allegato B al Codice della *privacy*, la cui obbligatorietà è venuta meno a partire dal 2012. In un certo senso, il registro dei trattamenti, al pari del vecchio DPS, costituisce un documento riepilogativo dei trattamenti e delle misure di sicurezza, tecniche e organizzative adottate.
(29) Per violazione dei dati personali, ai sensi dell'art. 4, par. 1, n. 12), si intende: "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".