Circolare n° 9 del 04.05.2018

Tutela dei dati personali: la nuova disciplina della privacy prevista dal regolamento UE 679/2016

Con il regolamento UE 27.4.2016 n. 679 sono state introdotte alcune **novità in materia di privacy. Tale regolamento**, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, è entrato in vigore il 24.5.2016, ma **sarà applicabile dal prossimo 25.5.2018.** Nel prosieguo del presente contributo verranno esaminati i principali aspetti della nuova disciplina in materia di tutela dei dati personali (privacy). In particolare, vengono analizzati gli aspetti riguardanti: i) **l'ambito di applicazione della nuova disciplina**; ii) **le figure del titolare, responsabile e incaricato del trattamento dei dat**i; iii) la nuova **figura del responsabile della protezione dei dati**; iv) le **modalità di trattamento dei dati**; v) **l'acquisizione del consenso dell'interessato**; vi) **l'informativa all'interessato**; vii) i **diritti dell'interessato**; viii) le misure di sicurezza; ix) la **valutazione di impatto sulla protezione dei dati; x) la violazione dei dati.**

1) Premessa:

Con il regolamento UE 27.4.2016 n. 679 sono state introdotte alcune **novità in materia di privacy. Tale regolamento**, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, è entrato in vigore il 24.5.2016, ma **sarà applicabile dal prossimo 25.5.2018.**

2) Oggetto e finalità del regolamento

Le disposizioni contenute nel reg. UE 679/2016 riguardano la **protezione delle persone fisiche** (così come per il Codice della privacy, che esclude il trattamento dei dati relativi a persone giuridiche) con riferimento:

- al **trattamento dei dati personali**;
- alla **libera circolazione** di tali dati.

Ambito di applicazione materiale

Il reg. UE 679/2016 trova applicazione con riferimento ai seguenti **trattamenti:**

- **trattamento automatizzato**, in maniera parziale o totale, **di dati personali**;
- **trattamento non automatizzato** di dati personali contenuti in un archivio o destinati ad essere ivi inclusi.

Sono esclusi, in particolare, i **trattamenti di dati personali effettuati** da una persona fisica **per l'esercizio di attività a carattere esclusivamente personale o domestico.**

3) Figure Professionali

Nell'ambito dei **soggetti coinvolti** nel trattamento dei dati personali, il reg. UE 679/2016 continua a prevedere, rispetto al Codice della privacy, le figure del titolare del trattamento dei dati e del responsabile del trattamento dei dati.
Il regolamento, poi, disciplina la nuova figura del **responsabile per la protezione dei dati personali.**

a) Titolare, responsabile e incaricato del trattamento dei dati

Il reg. UE 679/2016 definisce in maniera più precisa **ruoli e compiti del titolare e del responsabile del trattamento dei dati**. Tali qualifiche possono essere assunte da una **persona fisica o giuridica**, **un'autorità pubblica, un servizio o altro organismo**.

Titolare del trattamento
Il titolare del trattamento è il soggetto che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali.**

b) Responsabile del trattamento

Il responsabile del trattamento è il **soggetto che tratta dati personali per conto del titolare del trattamento**. Rispetto al Codice della privacy:

- viene prevista una più **specifica definizione dei rapporti fra titolare e responsabile**, che deve avvenire mediante il ricorso a un contratto (o altro atto giuridico), in forma scritta (anche in formato elettronico), con uno specifico contenuto;
- il responsabile del trattamento **può ricorrere ad un altro responsabile** solo su autorizzazione scritta (specifica o generale) del titolare del trattamento;
- **può essere nominato un sub-responsabile** del trattamento, per specifiche attività di trattamento, nel qual caso occorre definire i rapporti mediante un contratto o altro atto giuridico.

La violazione del regolamento da parte del responsabile del trattamento, determinando finalità e mezzi del trattamento stesso, **comporta l'assunzione diretta della qualifica di titolare del trattamento.**
Il responsabile del trattamento deve **presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate** onde assicurare la conformità del trattamento al regolamento e alla tutela dei diritti dell'interessato.

Aspetti generali:
Il contratto di nomina del responsabile del trattamento deve prevedere:
- la materia disciplinata;
- la durata del trattamento;
- la natura e finalità del trattamento;
- il tipo di dati personali;
- le categorie di interessati;
- gli obblighi e diritti del titolare del trattamento.

Aspetti specifici:
Il contratto deve prevedere che il responsabile del trattamento:
 proceda al trattamento dei dati **solo su istruzione documentata del titolare del trattamento**;
 garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla **riservatezza o abbiano un adeguato obbligo legale di riservatezza**;
 adotti tutte le **misure di sicurezza**;
 assista il titolare, tenuto conto della natura del trattamento e delle informazioni a disposizione, **nel garantire il rispetto degli obblighi per la sicurezza** dei dati personali e per la valutazione d'impatto sulla protezione dei dati e la consultazione preventiva;
 su scelta del titolare del trattamento, **cancelli o restituisca tutti i dati personali** dopo che è terminata la prestazione dei servizi relativi al trattamento, e cancelli le copie esistenti;
 metta a disposizione del titolare del trattamento tutte **le informazioni necessarie per dimostrare il rispetto dei sopra esposti obblighi**, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

c) Responsabile della protezione dei dati

Il reg. UE 679/2016 introduce **la nuova figura professionale del responsabile della protezione dei dati** - RPD (o Data Protection Officer - DPO), di cui si forniscono le principali caratteristiche nella seguente tabella.

Nomina:

La nomina dell'RPD è obbligatoria per:

 tutti i soggetti la cui attività principale consista in trattamenti che, per la loro natura, ambito di applicazione e/o finalità, **richiedono il monitoraggio regolare e sistematico degli interessati** su larga scala;
 tutti i soggetti la cui attività principale consista nel trattamento, su larga scala, di categorie particolari di dati personali (nell'ambito dei quali sono compresi i dati definiti dal Codice della privacy come "**sensibili",** oltre ai nuovi dati genetici e biometrici) e i **dati relativi a condanne penali e reati**

Qualifica e designazione

L'RPD viene designato dal **titolare del trattamento e dal responsabile del trattamento:**
 in **funzione delle qualità professionali** (conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati) e della capacità di assolvere i propri compiti; non sono necessarie attestazioni formali o titoli professionali specifici;
 ricorrendo a un proprio dipendente (RPD interno) o a un soggetto esterno (RPD esterno), in quest'ultimo caso mediante il ricorso ad un contratto di servizi.

Compiti:

L'**RPD** deve svolgere i seguenti compiti minimi:
 informare e fornire consulenza al titolare o al responsabile del trattamento, nonché ai dipendenti, in merito agli obblighi derivanti dal regolamento;
 verificare l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale;
 fungere da punto di contatto con l'autorità di controllo o, eventualmente, consultarla di propria iniziativa.

Nell'esecuzione di tali compiti, l'RPD:
 deve essere "sostenuto", mediante il **rilascio delle risorse necessarie;**
 non deve ricevere alcuna istruzione;
 non è rimosso o penalizzato.

Obblighi:

È **tenuto al segreto o alla riservatezza** in merito all'adempimento dei propri compiti.

Adempimenti:

I dati di contatto del responsabile della protezione dei dati **devono essere pubblicati e comunicati all'autorità di controllo** da parte del titolare del trattamento e dal responsabile del trattamento.

Adempimenti del titolare del trattamento e del responsabile del trattamento

In capo al **titolare del trattamento e al responsabile del trattamento sono stati:**
 dettagliati e/o modificati alcuni adempimenti già previsti dal Codice della privacy, ad esempio in materia di modalità di trattamento dei dati, di acquisizione del consenso e di rilascio dell'informativa;
 introdotti nuovi compiti, fra i quali tenere un registro delle attività di trattamento ed effettuare una valutazione di impatto sulla protezione dei dati.

4) Modalità di trattamento dei dati

Il titolare del trattamento deve previamente **istruire tutti coloro che siano autorizzati ad accedere e trattare i dati personali**, compreso il responsabile del trattamento

Costituiscono **principi generali del trattamento:**
 la liceità, la correttezza e la trasparenza nei confronti dell'interessato;
 la limitazione delle finalità (determinate, esplicite e legittime);
 la minimizzazione dei dati, che devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
 l'esattezza, con aggiornamento dei dati se necessario;

 la limitazione della conservazione;
 l'integrità e la riservatezza;
 la responsabilizzazione del titolare del trattamento, il quale è competente per il rispetto dei principi sopra esposti e sul quale grava l'onore di prova.

Il trattamento è lecito se ricorrono i seguenti presupposti:
 consenso dell'interessato per una o più specifiche finalità;
 adempimento di obblighi contrattuali, di cui l'interessato è parte o di misure precontrattuali;
 obblighi di legge cui è soggetto il titolare del trattamento;
 interesse pubblico o esercizio di pubblici poteri;

Acquisizione del consenso

Come già previsto dal Codice della privacy, il **consenso deve essere libero**, specifico rispetto alle finalità del trattamento (o per finalità compatibili), **informato**
La richiesta di consenso, qualora inserita all'interno di una dichiarazione scritta, deve essere chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato e deve essere resa in forma comprensibile e facilmente accessibile, con linguaggio semplice e chiaro.

Categorie particolari di dati personali

Sono inclusi nella nuova definizione di "categorie particolari di dati" quelli attualmente previsti dal Codice della privacy **come dati "sensibili**", quindi i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oltre ai dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
In tale categoria sono inclusi i nuovi riferimenti ai **dati genetici e dati biometrici** intesi a identificare in modo univoco una persona fisica.
Per il trattamento dei suddetti dati è, in generale, prescritto il divieto generale di trattamento.

Processi decisionali automatizzati

Il trattamento è vietato **salvo l'acquisizione del consenso "esplicito" dell'interessato** o nei casi in cui tali operazioni siano necessarie per l'esecuzione di un contratto con l'interessato o sia autorizzata dal diritto dell'Unione o del singolo Stato membro.
Rimane comunque **l'obbligo di apprestare garanzie adeguate ad assicurare il rispetto dei diritti dell'interessato,** riguardanti la specifica informazione all'interessato, nonché di esprimere la propria opinione e di contestare la decisione.
Nell'informativa **devono essere esplicitate le modalità e le finalità della profilazione.**

5) Informativa

Il reg. UE 679/2016 riprende, rispetto al Codice della privacy , **l'obbligo di informativa**, distinto sempre rispetto alla raccolta dei dati presso l'interessato o meno, prevedendo però un **contenuto maggiormente dettagliato**.

Contenuto dell'informativa

Informativa per il trattamento di dati raccolti presso l'interessato

Occorre rendere noto:
 l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
 i **dati di contatto** del responsabile della protezione dei dati, se nominato;
 le **finalità del trattamento** cui sono destinati i dati personali e la base giuridica del trattamento;
 i legittimi interessi perseguiti dal titolare del trattamento o da terzi, qualora costituisca la base giuridica del trattamento;
 gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
 il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
 l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento **l'accesso ai dati personali e la rettifica** o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
 l'esistenza del diritto di revocare il consenso in qualsiasi momento;

Informativa per il trattamento di dati non ottenuti presso l'interessato

Occorre rendere noto **le informazioni di cui sopra** (con esclusione del riferimento alla comunicazione dei dati personali come obbligo legale o contrattuale), con l'aggiunta:
 delle **categorie di dati personali** oggetto di trattamento;
 della **fonte da cui hanno origine i dati personali** e, se del caso, dell'eventualità che i dati provengano da fonti accessibili al pubblico.

6) Diritti degli interessati

Nell'ambito dei **diritti previsti in capo all'interessato**, vengono ripresi, rispetto al Codice della privacy, oltre all'informativa sul trattamento dei dati personali, i seguenti:

 diritto di accesso;
 diritto di rettifica;
 diritto di cancellazione (diritto all'oblio in forma rafforzata);
 diritto di opposizione.

Modalità per l'esercizio dei diritti

Quanto alle modalità per l'esercizio dei diritti, rispetto al Codice della privacy:
 il termine per la risposta all'interessato è, per tutti i diritti, di **un mese dal ricevimento della richiesta**, estendibile fino a due mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato, anche in caso di diniego;

 il riscontro alle richieste presentate dagli interessati **deve avvenire in forma scritta**, anche elettronica;
 in generale **le informazioni vanno rese in maniera gratuita**; spetta al titolare, però, stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato qualora si tratti di richieste manifestamente infondate o eccessive, anche ripetitive, e, nell'ambito del diritto di accesso, nel caso di richiesta di più copie dei dati personali (tenuto conto dei costi amministrativi sostenuti).

7) Registro delle attività di trattamento

titolari e i responsabili del trattamento **devono tenere un registro delle operazioni di trattamento**, in forma scritta, anche in formato elettronico. **Sono escluse** da tale obbligo le **imprese o le organizzazioni con meno di 250 dipendenti**, salvo che il trattamento:
 possa presentare un rischio per i diritti e le libertà dell'interessato;
 non sia occasionale;
 includa il trattamento di categorie particolari di dati o di dati personali relativi a condanne penali e a reati.

Contenuto del registro

Titolare del trattamento:

 Nome e dati di contatto del titolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
 finalità del trattamento;
 categorie di interessati e categorie di dati personali;
 categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
 trasferimenti dei dati personali verso un Paese terzo o un'organizzazione internazionale, compresa l'identificazione del Paese terzo o dell'organizzazione interna-azionale e la documentazione delle garanzie adeguate;
 termini ultimi previsti per la cancellazione delle diverse categorie di dati (ove possibile);
 descrizione generale delle misure di sicurezza tecniche e organizzative (ove possibile).

Responsabile del trattamento

 Nome e dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
 categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
 categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di Paesi terzi od organizzazioni internazionali;
 trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale,
 descrizione generale delle misure di sicurezza tecniche e organizzative (ove possibile).

Misure di sicurezza adeguate

Rispetto al Codice della privacy**, non ci sono più le misure minime di sicurezza,** ma è il titolare del trattamento (e il responsabile) a dover adottare misure tecniche e organizzative "adeguate" al fine di "garantire un livello di sicurezza adeguato al rischio" del trattamento

Sarà, quindi, il titolare a valutare le misure necessarie, caso per caso, rispetto ad una serie di elementi, di seguito indicati:
- stato dell'arte;
- costi di attuazione;
- natura, oggetto, contesto e finalità del trattamento;
- rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche

8) Valutazione di impatto sulla protezione dei dati

La valutazione di **impatto sulla protezione dei dati** (DPIA) costituisce un ulteriore adempimento derivante dal principio introdotto della responsabilizzazione dei **titolari nei confronti dei trattamenti da questi effettuati**.
La valutazione, da effettuare ex ante al trattamento ad opera del titolare del trattamento consultandosi con il responsabile della protezione dei dati personali, **ricorre come obbligo in caso di trattamento molto rischioso per i diritti e le libertà delle persone fisiche**. Ciò può derivare da vari elementi, come, ad esempio, l'uso di nuove tecnologie, ovvero **in considerazione di altre caratteristiche** (natura, oggetto, contesto, finalità) del trattamento.

La Dpia può essere effettuata sia dal titolare dei dati sia da soggetti interni o esterni all'organizzazione. La responsabilità resta comunque al titolare del trattamento.
Non c'è l'obbligo di redigere il documento, invece, se i trattamenti dei dati personali: non presentano rischi rilevanti per i diritti e le libertà delle persone:
Non è prevista una metodologia uniforme di redazione del documento. Spetta al titolare scegliere quella che risulta conforme al Regolamento europeo
Alla luce delle sanzioni previste per la violazione della normativa, però (fino a 10 milioni di euro o al 2% del fatturato globale aziendale), indipendentemente dall'obbligatorietà o meno della valutazione di impatto privacy, è sempre preferibile adottare la procedura, perché questa aiuta ad assumere le misure di sicurezza necessarie.

9) Violazioni dei dati ("data breach")

Rispetto al Codice della privacy, viene prevista **la notifica da parte del titolare del trattamento di ogni violazione dei dati trattati all'autorità competente entro 72 ore dal momento in cui ne venga a conoscenza** (e comunque senza ingiustificato ritardo) e, in casi gravi, anche all'interessato. Tale adempimento è necessario solo se si ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati

10) Sanzioni

Si rende noto che le sanzioni previste per le imprese inadempienti sono molto significative, e variano nel rapporto all'inadempimento o all'irregolarità accertata, e possono raggiungere il 4% del fatturato annuo.

11) Conclusioni

Quanto sopra illustrato è un cambiamento importante che interesserà profondamente aziende di ogni tipo e di ogni dimensione.
Il GDPR ha un ambito di applicazione più ampio di quanto potrebbe sembrare a prima vista.
La norma evidenzia come fondamentali le misure di sicurezza informatica invitando quindi l'uso di strumenti conformi. L'ambito d'intervento principale sarà quindi proprio quello informatico. I processi utilizzati dovranno garantire un livello di protezione molto alto e dovranno essi stessi essere conformi alla legge.
L'ammodernamento della legislazione in tema di privacy e l'adempimento del GDPR non sarà di facile adozione ma necessario. Nel breve periodo ogni azienda dovrà quindi sollecitarsi ad adottare le misure più adeguate al raggiungimento degli obiettivi di conformità per non incorrere in pesanti sanzioni e procedimenti penali, anche questi rivisti dal nuovo regolamento, con conseguenti perdite in termini economici e di reputazione

Pensando di fare cosa gradita, vi segnaliamo che il nostro Studio si avvale sul tema Privacy del supporto di una struttura esterna e in grado di accompagnare le aziende nel processo di adeguamento al nuovo regolamento europeo. La clientela eventualmente interessata può contattare lo Studio per informazioni.

Rimaniamo a disposizione e porgiamo distinti saluti

Dott. Marco Folicaldi

20010 Arluno (MI) I C.so XXVI Aprile 123 I tel: 02 901.21.41 I fax: 02 901.71.99
marcofolicaldi@studiofolicaldi.it