Circolare n°: 15/2018

Oggetto: ***La nuova regolamentazione in materia di privacy***

Sommario: A partire dal prossimo 25 maggio entrerà in vigore il nuovo Regolamento UE 2016/679 che andrà a sostituire l'attuale normativa vigente in materia di Privacy disciplinata dal Dlgs n° 196/2003.

Il regolamento sarà immediatamente applicabile senza necessità di ulteriori provvedimenti di recepimento da parte dell'Autorità nazionale.

Contenuto:

Il nuovo regolamento introduce regole più chiare in materia di informativa e consenso, garantendo una maggiore armonizzazione delle norme a livello europeo, sebbene ogni paese membro possa integrarne i contenuti.

Il Garante della Privacy potrà, infatti, disciplinare particolare aspetti afferenti al trattamento dei dati personali in alcuni ambiti, e definire in modo più dettagliato gli obblighi per le PMI.

Le misure più innovative riguardano: la nomina di un **Responsabile della protezione dei dati**, soggetto a cui sono attribuite funzioni di controllo, consultazione e informazione della nuova disciplina e l'istituzione del **Registro dei trattamenti**.

Con la presente circolare vengono evidenziati le principali novità introdotte dal nuovo regolamento. L'applicazione e l'interpretazione del regolamento sono sottoposte a periodici aggiornamenti da parte del Garante, in particolare per quanto concerne la sua attuazione verso le PMI. Seguiranno pertanto ulteriori approfondimenti.

Indice:

AMBITO DI APPLICAZIONE:

Il regolamento garantisce una migliore efficacia delle norme relative alla **tutela delle persone fisiche**, con riguardo sia al trattamento sia alla protezione dei dati personali[1].

Il regolamento trova inoltre applicazione con riferimento all'ambito delle attività commerciali e professionali; non è quindi oggetto di applicazione il trattamento dei dati effettuato da una persona fisica in ambito personale o domestico.

Il principio cardine della nuova normativa è quello della "**accountability**" (responsabilizzazione): i titolari del trattamento dei dati devono essere responsabilizzati, dimostrando di adottare approcci e politiche di privacy adeguate e in conformità con il Regolamento, nonché misure che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

PRINICIPALI NOVITA':

Si riepilogano in breve le prioritarie novità introdotte dal nuovo regolamento:

Consenso: per i dati "sensibili[2]" il consenso deve essere esplicito; non deve essere necessariamente documentato per iscritto, anche se quest'ultima è modalità idonea a configurare l'inequivocabilità del consenso;

Contenuto informativo: i contenuti dell'informativa sono più ampi rispetto a quelli previsti dal Codice della Privacy. In particolare, il titolare deve sempre specificare i dati di contatto del **RPD-DPO** (**Responsabile della protezione dei dati - Data Protection Officer**), ove esistente e solo se previsto, la base giuridica del trattamento, l'interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.

[1] Per dato personale si intende le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica.
[2] Quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale.

Il regolamento prevede inoltre che il titolare specifichi 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.

Modalità dell'informativa

L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile.

L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online) anche se sono ammessi "altri mezzi" (anche oralmente).

Diritto di accesso e cancellazione (oblio)

Il diritto di accesso prevede, in ogni caso, il diritto di ricevere una copia dei dati personali oggetto di trattamento. Il titolare del trattamento non è tenuto a fornire le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi.

Il diritto "all'oblio" consiste nel diritto alla cancellazione dei propri dati personali. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi qualsiasi copia o riproduzione.

RESPONSABILE DEI DATI:

La novità più rilevante riguarda la nomina del **responsabile della protezione dei dati personali**[3], ossia un soggetto designato dal titolare o dal responsabile del trattamento per assolvere funzioni di supporto, controllo, consultive, formative e informative in

[3] Nel dettaglio il responsabile della protezione dei dati dovrà: a) sorvegliare l'osservanza del regolamento; b) collaborare con il titolare/responsabile nel condurre una valutazione di impatto sulla protezione dei dati (DPIA); c) informare e sensibilizzare il titolare, e il responsabile del trattamento, nonché i dipendenti, riguardo gli obblighi derivanti dal regolamento; d) cooperare con il Garante e fungere da punto di contatto per il Garante; e) supportare il titolare o il responsabile con riguardo alla tenuta di un registro delle attività di trattamento.

relazione all'applicazione del Regolamento. Rimangono invariate le figure già previste dal Codice Privacy, del **titolare del trattamento** dei dati e del **responsabile del trattamento**[4]**.**

Per la nomina del **responsabile della protezione dei dati personali**, non è richiesta l'iscrizione in appostiti albi o elenchi; il soggetto deve tuttavia possedere un'approfondita conoscenza della normativa e della prassi in materia di privacy, nonché delle norme e delle procedure amministrative che disciplinano lo specifico settore di appartenenza.

Il ruolo può essere ricoperto da:

- **un dipendente** del titolare o del responsabile al trattamento dei dati;
- in alternativa da **soggetti esterni,** a condizione che garantiscono l'effettivo assolvimento dei compiti attribuiti dal Regolamento.

La designazione può essere fatta mediante atto specifico di nomina, o nel caso di soggetti esterni, tramite contratto di servizi.

Entrambi gli atti, da predisporre in forma scritta, dovranno indicare i compiti attribuiti, le risorse messe a disposizione per lo svolgimento dell'incarico, e ogni altra informazione utile in rapporto al contesto.

Il titolare o il responsabile che abbiano designato un RDP resta in ogni caso responsabile dell'osservanza della normativa in materia di protezione dei dati.

Il nominativo del responsabile e i relativi dati di contatto vanno altresì comunicati all'Autorità di controllo, utilizzando il modello disponibile sul sito del Garante della Privacy.

SOGGETTI OBBLIGATI:

Sono obbligati alla designazione del **responsabile della protezione dei dati personali**:

a) le amministrazioni e gli enti pubblici, fatta eccezione per le autorità giudiziarie;

[4] Soggetto che tratta i dati per conto del titolare.

b) tutti i soggetti la cui attività principale consiste in trattamenti che, per la loro natura, il loro oggetto o le loro finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) tutti i soggetti la cui attività principale consiste nel trattamento, su larga scala, di dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici.

A titolo esemplificativo rientrano nelle categorie sopraindicate: istituti di credito, imprese assicurative, sistemi di informazione creditizia, società finanziarie, società di revisione contabile, società di recupero crediti, partiti e movimenti politici, associazioni di categoria, agenzie interinali e di somministrazione del lavoro e ricerca, società che forniscono servizi informatici, società call center, aziende ospedaliere, e altri.

Nei casi diversi da quelli evidenziati la designazione non è obbligatoria.

A titolo esemplificativo **la designazione del RPD non è obbligatoria** in relazione ai trattamenti effettuati da:

1. liberi professionisti in forma individuale;
2. agenti e rappresentanti e mediatori operanti non su larga scala;
3. imprese individuali o familiari;
4. piccole e medie imprese, con riferimento ai trattamenti dei dati personali connessi alla gestione dei rapporti con fornitori e dipendenti.

N.B: anche laddove la nomina del RDP non sia obbligatoria, è possibile comunque procedere alla sua designazione su base volontaria.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO:

Ulteriore strumento utile ad incentivare il rispetto delle finalità e dei parametri del regolamento è l'introduzione del **registro delle attività di trattamento**.

Si tratta di un documento in cui il titolare deve tenere traccia dettagliata delle attività compiute con dati relativi a dipendenti, fornitori, partner e soprattutto clienti (indicando in particolare le finalità del trattamento, le categorie dei dati e degli interessati, gli eventuali trasferimenti verso paesi terzi dei dati raccolti e le misure di sicurezza adottate).

La tenuta del registro si applica alle imprese e organizzazioni con più di 250 dipendenti, a meno che il trattamento non sia occasionale o ad alto rischio, o includa particolari categorie di dati (ad esempio i dati sensibili).

Accanto al registro, i titolari dovranno svolgere una serie di attività preventive (dimostrabili) idonee a mitigare i rischi inerenti al trattamento. In particolare dovrà essere svolta una **valutazione d'impatto** (o DPIA) che non è obbligatoria in ogni caso.

L'obbligatorietà scatta nei seguenti casi:

a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su trattamenti automatizzati;
b) trattamento su larga scala (es. ospedale) di categorie particolari di dati personali o relativi a condanne penali;
c) sorveglianza su larga scala di una zona accessibile al pubblico.

A titolo esemplificativo è probabile che venga richiesta una **valutazione d'impatto** per i seguenti trattamenti: monitoraggio sistematico delle attività dei dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, la raccolta di dati pubblici dei media sociali per la generazione di profili, etc…

SANZIONI:

Il quadro sanzionatorio previsto per le violazioni del nuovo regolamento da parte delle PMI è graduato in funzione:

- della gravità del fatto compiuto;
- della dimensione dell'azienda;
- del danno effettivamente arrecato;
- della buona condotta tenuta dall'azienda in fase di adozione e rispetto degli adempimenti;
- del fatturato realizzato.

Tuttavia nei casi di violazioni non significative dei diritti degli interessati, il Garante della Privacy potrà adottare, in prima battuta, una diffida in alternativa alla sanzione pecuniaria.

E' plausibile ritenere che la transizione dal vecchio codice alle nuove norme sia accompagnata, da parte del Garante della Privacy, da una definizione puntuale del quadro sanzionatorio per le PMI.

CONSIGLI OPERATIVI:

Per le imprese e per i professionisti l'impatto del Regolamento UE sulla protezione dei dati n. 2016/679, andrà ad interessare soprattutto le **modalità di raccolta e trattamento dei dati personali.**

In particolare dovranno essere osservati i principi base individuati dal GDPR:

a. liceità, correttezza e trasparenza del trattamento;
b. limitazione delle finalità: i dati dovranno essere raccolti per finalità esplicite e legittime e trattati in modo che non sia incompatibile con altre finalità;
c. esattezza: i dati devono essere esatti e se necessario aggiornati;
d. conservazione dei dati in una forma che ne consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattate.

E' pertanto opportuno, sulla base dei chiarimenti forniti dal Garante, che i t**itolari del trattamento** verifichino la rispondenza delle **informative** attualmente adottate ai nuovi criteri (sopra esposti), in modo da garantirne la conformità al regolamento.

Lo Studio è disponibile, ove richiesto, a segnalare Società specializzate sul tema privacy con cui collabora.

Restiamo a disposizione per informazioni, chiarimenti e assistenza.

Cordiali saluti

Studio Brunello e Partner
Dr. Fabio Pavan