

Spett.li CLIENTI
Loro Sedi

Oggetto: Circolare n. 7 del 23 maggio 2018
Tutela dei dati personali – Nuova disciplina della *privacy*

Con il **regolamento UE 27.4.2016 n. 679** sono state introdotte importanti **novità in materia di *privacy***.

Tale regolamento che ha ad oggetto la tutela delle persone fisiche relativamente 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**.

A breve il vigente Codice della *privacy* sarà quindi sostituito da un nuovo Decreto Legislativo che costituirà, insieme al Regolamento UE n. 679/2016, la nuova disciplina in materia di *privacy*.

Di seguito viene esposta una sintesi delle principali problematiche che imprese e soggetti pubblici dovranno tenere presenti in vista dell'applicazione della nuova disciplina anche in riferimento ai Provvedimenti ed alle indicazioni emanate dal Garante della *Privacy*.

Oggetto e ambito di applicazione

Le disposizioni contenute nel regolamento UE 679/2016:

- a) si applicano a **tutte le imprese** e le **pubbliche amministrazioni**;
- b) riguardano la **protezione delle persone fisiche** con riferimento:
 - al **trattamento** dei dati personali;
 - alla **libera circolazione** di tali dati;
- c) trovano applicazione con riferimento sia al **trattamento automatizzato** sia a quello **non automatizzato** di dati personali.

Figure professionali

Accanto alle figure professionali già previste, ossia il titolare del trattamento dei dati e il responsabile del trattamento dati è introdotta la **nuova figura del responsabile per la protezione dei dati (RDP)**.

- il **titolare** del trattamento è il soggetto che singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- il **responsabile** del trattamento è il soggetto che tratta i dati personali per conto del titolare del trattamento;
- il **responsabile per la protezione dei dati (RDP)** può essere sia un dipendente della società titolare del trattamento o, in alternativa, un professionista esterno competente in tema di protezione dati. La nomina di tale figura è obbligatoria nei seguenti casi:
 - a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
 - b) se le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala;
 - c) se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

I casi concreti in cui si rende necessaria la nomina dell'RDP non sono di facile individuazione, tuttavia, si può ritenere che tra le aziende private rientrino le seguenti:

- ✓ Istituzioni finanziarie e istituti di credito;
- ✓ Società di recupero crediti;
- ✓ Istituzioni e compagnie assicurative;



- ✓ Aziende sanitarie private – cliniche, poliambulatori, laboratori analisi cliniche e diagnostiche e altri istituti sanitari;
- ✓ Società di servizi / consulenza;
- ✓ Centri elaborazione dati e Internet provider;
- ✓ Società di trasporti, agenzie di viaggio, strutture alberghiere e ricettive in genere;
- ✓ Società commerciali e industriali allorché trattino una mole di dati personali dei propri dipendenti, clienti, fornitori, consulenti esterni, tale da far ritenere soddisfatto uno dei fattori che connota il trattamento su larga scala (dunque, per un'ulteriore esemplificazione: società di produzione e/o trasformazione di prodotti ortofrutticoli con 40 dipendenti, 4 unità locali dislocate sul territorio nazionale e dotate di sistemi di videosorveglianza/controlli accessi);
- ✓ Studi professionali associati, società di revisione, società tra professionisti.

Tra i compiti svolti dall'RDP si evidenziano i seguenti:

- informare e fornire consulenza al titolare e al responsabile del trattamento nonché ai dipendenti che eseguono i trattamenti;
- sorvegliare l'osservanza del Regolamento;
- fornire pareri in merito alla "Valutazione d'impatto sulla protezione dei dati";
- cooperare con l'Autorità di controllo e fungere da punto di contatto con essa.

Adempimenti

In capo al titolare del trattamento e al responsabile del trattamento sono stati: **Indirizzo internet:**

- dettagliati e/o modificati alcuni adempimenti** già previsti, 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.

Modalità di trattamento dei dati

Il trattamento dei dati deve avvenire sulla base di determinati principi stabiliti dal regolamento quali la liceità, la correttezza e la trasparenza nei confronti dell'interessato, la limitazione delle finalità, la minimizzazione dei dati che devono essere adeguati, pertinenti e limitati a quanto necessario, l'integrità e la riservatezza.

Acquisizione del consenso

Per il consenso che deve essere libero, specifico rispetto alle finalità del trattamento e informato, non sono precisate le modalità di espressione.

E' richiesto il consenso "esplicito" solo per categorie particolari di dati e decisioni basate su trattamenti automatizzati.

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.

Informativa

Il contenuto dell'informativa deve essere ben dettagliato.

In particolare, l'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile e deve essere utilizzato un linguaggio chiaro e semplice. Inoltre, deve essere data per iscritto o con "altri mezzi" anche elettronici (ad esempio, nel caso di servizi on line) oppure oralmente se richiesto dall'interessato.

Principio di "accountability"

Viene introdotto il principio della c.d. "responsabilizzazione" (*accountability*) di titolari e responsabili del trattamento, che sono tenuti a mettere in atto misure tecniche e organizzative adeguate per garantire e per dimostrare l'applicazione della normativa in materia di *privacy*.

Pertanto, è il titolare che decide in maniera autonoma modalità, garanzie e limiti del trattamento dei dati personali, nel rispetto del regolamento e di determinati criteri.

Diritti degli interessati

Tra i diritti degli interessati sono ora previsti accanto a quelli di accesso, rettifica e di opposizione:

- il **diritto all'oblio** (cancellazione) in forma rafforzata: tale diritto, se esercitato dall'interessato, impone al titolare del trattamento di dar corso alla cancellazione dei suoi dati personali quando non siano più necessari rispetto alle finalità per le quali sono stati raccolti, così come quando abbia ritirato il consenso prestato o qualora i dati siano stati trattati illecitamente;
- il **diritto alla limitazione** al trattamento dei dati;
- il **diritto alla portabilità** dei dati: tale diritto consiste nella possibilità di trasferire i dati personali da un titolare del trattamento ad un altro indicato dall'interessato, senza alcun impedimento.

Registro delle attività di trattamento

È obbligatorio tenere un registro delle operazioni di trattamento, in forma scritta, anche in formato elettronico. Il registro dovrà contenere una descrizione dettagliata delle misure di sicurezza tecniche e organizzative e, su richiesta, dovrà essere messo a disposizione dell'Autorità di controllo.

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. Si rammenta che tra le categorie particolari di dati rientrano quelli attualmente classificati come "sensibili" ossia quei 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.

Valutazione di impatto sulla protezione dei dati (DPIA)

È stato introdotto l'obbligo per il titolare del trattamento dei dati di effettuare una valutazione preliminare d'impatto di quel trattamento sulla protezione dei dati quando si è in presenza di:

- ✓ trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- ✓ trattamenti automatizzati, ivi compresa la profilazione;
- ✓ trattamenti su larga scala di categorie particolari di dati personali, o dei dati relativi a condanne penali e a reati;
- ✓ dati ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico.

La DPIA è un procedimento atto a costruire e dimostrare la conformità dell'azienda al Regolamento, nonché uno strumento di fondamentale importanza messo a disposizione del Titolare del trattamento.

Violazione dei dati

È previsto l'obbligo di 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.

Videosorveglianza

L'installazione di adeguati impianti di video-sorveglianza deve rispettare i principi indicati dal Garante della Privacy e dalla normativa vigente.

Le attuali norme del Governo hanno riformato la disciplina del controllo a distanza dei lavoratori e stabilito che l'installazione degli apparecchi è ammessa solo:

- previo accordo con le rappresentanze sindacali aziendali;
- previa autorizzazione della Direzione Territoriale del Lavoro (D.T.L.), nelle aziende con minori dimensioni, ove mancano le rappresentanze sindacali.

L'accordo con le Rappresentanze sindacali o l'autorizzazione della D.T.L. devono in ogni caso essere preventivi rispetto alla installazione delle apparecchiature.

Si ricorda che la violazione delle norme è punita con sanzioni pecuniarie e costituisce un illecito di natura penale.

Sanzioni

Con il Regolamento Europeo è stato introdotto un nuovo “sistema sanzionatorio” che prevede un aumento delle sanzioni amministrative pecuniarie fino ad un massimo di 20 milioni di Euro o, per le imprese, fino al 4% del fatturato totale annuo dell’esercizio precedente, se superiore.

Conclusioni

A fronte di quanto esposto nella presente circolare, **dal 25.05.2018**, imprese e professionisti dovranno **porre in essere una serie di adempimenti**, differenziati a seconda della tipologia di attività esercitata e della dimensione della realtà aziendale, al fine di adeguarsi alla nuova disciplina sulla *privacy*. In sintesi, quindi, gli step che l’azienda o il professionista possono essere tenuti a seguire consistono:

- a. nella revisione dell’organizzazione interna dell’impresa conformandola al protocollo *privacy*;
- b. nella contrattualizzazione dei rapporti tra Titolare e Responsabile del trattamento dati, specificando le rispettive responsabilità;
- c. nella revisione della modulistica con i clienti/utenti che si realizza con la riformulazione delle informative sulla *privacy* e la raccolta del nuovo consenso al trattamento dati;
- d. nella programmazione e l’attuazione di sistemi di sicurezza nella protezione dei dati;
- e. nella predisposizione della documentazione dimostrativa della propria conformità alle regole previste nel Regolamento;
- f. nella formazione obbligatoria del personale;
- g. nell’eventuale adesione a codici di correttezza e a sistemi di certificazione.

Le modifiche introdotte in materia di *privacy* per le quali si è fornita una breve sintesi con la presente circolare presentano elementi di una certa complessità che possono rendere necessario soprattutto in determinate situazioni l’intervento di un esperto specializzato in materia.

Segnaliamo tuttavia che alcuni clienti ci hanno comunicato di aver ricevuto delle proposte di consulenza da società di servizi per adeguarsi alla normativa sulla *privacy* con tariffe molto elevate. Per evitare costi inutili e adempimenti non obbligatori vi invitiamo a contattare i collaboratori di Studio prima di firmare mandati e/o contratti per questi adempimenti.

Lo Studio rimane disponibile anche a curare i contatti con le Organizzazioni sindacali e/o l’iter presso la Direzione Territoriale del Lavoro (D.T.L.) necessari per l’ottenimento dell’autorizzazione all’utilizzo dei sistemi di videosorveglianza.

Cordiali saluti.

Dott. Vincenzo Bona

Vincenzo Bona