Guida al GDPR

Guida al Nuovo Regolamento Europeo in materia di protezione dei dati personali

10 punti da conoscere sulla nuova normativa
5 step per arrivare preparati al 25 maggio 2018

A cura della dott.ssa Gabriella Cigliano e dell'ing. Gaetano De Rosa

GIDIERRE enterprise

Scopo

Scopo della presente guida è quello di guidare il lettore alla comprensione degli obblighi a cui le imprese e gli enti pubblici devono ottemperare con l'entrata in vigore del nuovo regolamento, ovvero, entro il 25 maggio 2018.

In maniera sintetica saranno descritte le novità introdotte dal nuovo Regolamento Europeo 2016/679 e saranno proposti suggerimenti per un'agevole gestione della tematica Privacy.

Sperando di aver fornito un utile strumento informativo vi auguriamo una buona lettura.

dott.ssa Gabriella Cigliano

ing. Gaetano De Rosa

Indice

Introduzione

L’avvento delle nuove tecnologie e la possibilità di disporre di grandi database hanno fortemente facilitato la raccolta di dati e la loro elaborazione. In un contesto dominato, perciò, dai **Big Data** è diventato prioritario prevenire eventuali violazioni degli archivi aziendali acquisendo le giuste competenze per poterli gestire.

Il presidente della commissione europea, Jean-Claude Junckers, ha dichiarato che l'aumento della diffusione delle tecnologie digitali, negli ultimi anni, non sempre è andato di pari passo con un graduale irrobustimento delle difese dei dati. Nel corso del 2016, infatti, **l'80% dell'imprese europee ha subito almeno una violazione di sicurezza informatica (Data Breach)** e si contano circa 4.000 episodi di **cyber crime**.

Per regolamentare un settore diventato sempre più cruciale nel quadro economico, nell’aprile del 2016 il Parlamento Europeo ha emanato un **nuovo Regolamento sulla tutela dei dati personali**, con regole standard da applicare in tutti i Paesi Membri dell’Unione. L’obiettivo di tale regolamento è quello di **massimizzare la protezione della privacy**, ma anche di favorire un clima di maggiore **sicurezza e libertà**, volto a promuovere lo sviluppo della nuova **economia digitale**.

Cos'è il GDPR?

Il GDPR (General Data Protection Regulation) è il nuovo Regolamento europeo 2016/679 emanato nell'aprile 2016 che impone a tutti i paesi dell'Unione Europea regole precise in materia di protezione dei dati personali.

Il GDPR segna l'inizio di una nuova epoca nelle norme che tutelano la privacy della persona fisica. Il focus si sposta dai titolari dei diritti, soggetti cui si riferiscono i dati, ai dati stessi che, in quanto tali, acquistano valore in sé. I dati non sono più mero argomento giuridico ma strategia di una nuova economia basata sull'utilizzo dei dati: la **Data Economy**.

È indispensabile, pertanto, regolamentare l'utilizzo di tali dati, abolendo barriere e differenze normative tra i membri dell'UE.

Il regolamento introduce nuovi obblighi e diritti che, se non rispettati, possono diventare un rischio per le imprese sia dal punto di vista economico (sanzioni, in caso di inadempienza, che arrivano a 20 milioni di euro o fino al 4% del fatturato dell'impresa) sia in termini di immagine.

Cosa cambia in 10 punti:

Entro il 25 maggio 2018 tutte le imprese e gli enti pubblici dovranno riorganizzare il sistema di gestione del trattamento dei dati.

Con l'introduzione del regolamento europeo **la privacy diventa un processo aziendale** da gestire con precise procedure.

Quali, dunque, i principali cambiamenti?

01 Cambia il **raggio di applicabilità**: il GDPR si applica a tutte le società che trattano i dati personali degli interessati residenti nell'Unione, indipendentemente dal fatto che il trattamento avvenga nell'UE o meno.

02 Viene introdotta la **privacy by design**: l'inclusione della protezione dei dati diventa parte integrante dei processi aziendali. Questo significa, ad esempio, includere i principi di privacy nei futuri contratti ed attuare una revisione di quelli già in essere.

03 Viene introdotto un **approccio meno formale e più sostanziale**: l'informativa diventa breve, priva di riferimenti normativi, dalla forma concisa e con un linguaggio semplice e chiaro. Essa dovrà obbligatoriamente contenere alcuni elementi quali, ad esempio, la fonte dei dati, il tempo di conservazione previsto ed il titolare del trattamento.

04 Cambia il **consenso al trattamento** dei dati personali: attraverso una manifestazione di volontà esplicita, specifica, informata ed inequivocabile, l'interessato manifesta il proprio assenso a che i dati personali che lo riguardano siano oggetto di trattamento.

05 Viene introdotto il **Documento di valutazione di impatto del trattamento dei dati** (**DPIA – Data Protection Impact Assessment**): all'interno del documento vengono analizzati gli aspetti di gestione, legali ed informatici attraverso tre fasi:

1. Analisi dei rischi;
2. Redazione di una gap list;
3. Creazione di un programma di intervento.

La criticità rispetto alla normativa precedente è data dalla maggiore responsabilizzazione del titolare: non vengono, infatti, indicate misure minime di sicurezza ma la scelta del tipo di gestione è lasciata alla valutazione soggettiva del Titolare del Trattamento (principio di Accountability). Il regolamento pone l'accento sull'adozione di comportamenti proattivi da parte di titolari e responsabili.

06 Viene introdotta la figura del **DPO - Data Privacy Officer** (il Responsabile per la Protezione dei dati personali): la nuova figura deve avere competenze tecniche, giuridiche ed informatiche. Il DPO deve essere nominato dal Titolare del Trattamento (nei casi previsti dal regolamento) ed il suo principale compito sarà quello di valutare e gestire il trattamento di dati personali nel rispetto delle normative privacy europee e nazionali.

07 Viene abolito l'obbligo di notificazione all'autorità Garante per la protezione dei dati personali (con un risparmio per le imprese, di circa 130 milioni di euro all'anno) e al suo posto viene introdotto il **Registro dei Trattamenti**. Tale registro (obbligatorio per aziende con più di 250 dipendenti o nel caso del trattamento di dati particolarmente sensibili) serve a documentare e provare la conformità del trattamento e deve essere messo a disposizione dell'autorità di controllo in caso di verifica.

08 Vengono fissati **nuovi diritti**: il titolare del trattamento deve garantire all'interessato i diritti all'**accesso,** alla **rettifica,** all'**integrazione,** all'**oblio** e alla **portabilità** dei propri dati personali. L'interessato ha il diritto di accedere ai propri dati, di chiedere di rettificarli ed integrarli qualora essi siano inesatti o incompleti. Il diritto all'oblio permette al soggetto di ottenere la cancellazione di dati personali e il divieto di un'ulteriore diffusione di tali dati. L'interessato può, inoltre, richiedere che i suoi dati siano trasferiti da un sistema di trattamento elettronico ad un altro e ottenere tali dati in un formato elettronico che sia di uso comune e che ne consenta, dunque, l'utilizzo (diritto di portabilità).

09 Viene introdotta la **Data Breach Notification**: l'obbligo di segnalare al Garante della Privacy le violazioni di dati, entro 72 ore dal momento in cui se ne è venuti a conoscenza. Per «violazione dei dati personali» si intende un'azione che comporti accidentalmente o in modo illecito la distruzione, la perdita (*Availability breach*), la modifica (*Integrity Breach)*, la divulgazione non autorizzata o l'accesso ai dati personali (*Confidentiality breach*). Nell'eventualità di accadimento di un data breach, il titolare del trattamento deve dimostrare di aver messo in atto le opportune precauzioni. Secondo uno studio di Accenture, **l'Italia** risulta essere **nella Top Ten dei paesi più colpiti da crimini informatici.**

10 Vengono aumentate le **sanzioni** rispetto alle normative precedenti: in caso di violazione, tali sanzioni possono arrivare a 20 milioni di euro o fino al 4% del fatturato annuo dell'impresa.

GDPR:
Un'opportunità per le aziende

Il GDPR è stato approvato non soltanto per ragioni legislative ma anche per creare un **clima favorevole allo sviluppo dell'economia digitale** e per promuovere **libertà e sicurezza**.

La protezione dei dati personali costituisce per le imprese un vero e proprio **asset competitivo** da poter sfruttare quale vantaggio commerciale. Il nuovo regolamento rappresenta, di fatto, un'opportunità prima che un adempimento.

Esso offre, innanzitutto, un vantaggio tecnico quale la possibilità di rafforzare le misure di protezione atte a contenere il **cyber risk**.

Divenendo, il trattamento dei dati, parte integrante dei processi aziendali, si semplifica la realizzazione dei progetti favorendo una **riduzione dei tempi** attesi per la loro realizzazione.

Ma c'è un terzo elemento che vale la pena sottolineare: i **benefici in termini di immagine** che ne derivano.
Conformandosi ai principi del GDPR, l'azienda dimostra il suo impegno ed interesse ad incrementare la tutela di chiunque sia venuto in contatto con essa, con conseguente impatto positivo sulla sua reputazione. **Trasmettere un senso di sicurezza** a clienti e partner stimola una maggiore **fiducia**, soprattutto adesso che i consumatori stanno diventando sempre più restii e preoccupati a rilasciare i propri dati personali.

5 step
per arrivare preparati
al 25 maggio 2018

Entro il 25 maggio 2018, **ogni azienda dovrà aver adeguato la gestione e protezione dei dati trattati**. Inoltre, dovrà documentare e tenere sotto controllo il processo di gestione delle informazioni così da essere sempre conforme al GDPR.

D'accordo col principio di **data protection by default**, ogni impresa dovrà aggiornare costantemente i dati, conservarli solo nel lasso di tempo necessario e cancellarli, dietro richiesta; inoltre, dovrà poter dimostrare che l'utilizzo di tali dati avviene solo per gli scopi per i quali è stata autorizzata dall'interessato.
Diventa altresì importante crittografare i dati posseduti (anche quelli conservati nei vari supporti di memoria) così da porli al sicuro in caso di furto/smarrimento e le email contenenti dati confidenziali.

Il **trattamento dei dati diventa** un vero e proprio **processo produttivo** da gestire con gli altri processi aziendali. Ne derivano diverse attività da svolgere, tra cui, investire sulla formazione del proprio personale.

Sulla base dei 10 punti analizzati, possiamo riassumere in 5 passi le azioni da intraprendere in vista dell'entrata in vigore del GDPR:

STEP 1 **Analizzare i dati trattati in azienda:** Quali dati personali sono in possesso dell'azienda? Da dove provengono? Chi li gestisce? Dove e come vengono trattati?

É importante fare un inventario delle proprie informative e verificare come cambiarle in funzione dei nuovi obblighi (scelta strategica per evitare di investire tempo e danaro in soluzioni non applicabili alla propria azienda). Completata la mappatura delle proprie banche dati, tramite una **Gap Analisys,** individuare le lacune e ripensare i processi di trattamento dei dati per adeguare le procedure alle disposizioni del GDPR.

STEP 2 Nominare, nei casi previsti, il **DPO** (Data Privacy Officer).

STEP 3 Eseguire la valutazione **DPIA**; questa fase è cruciale, anche quando non obbligatoria, per non incorrere in spiacevoli sanzioni, individuando le misure opportune per la mitigazione del rischio.

STEP 4 Istituire e gestire il **Registro dei Trattamenti** (nei casi previsti).

STEP 5 Definire un **piano di Audit periodici** per testare la validità delle soluzioni adottate a valle della DPIA. In tale piano devono essere comprese **simulazioni di data breach** per testare la robustezza delle misure preventive e protettive.

GIDIERRE enterprise

Gidierre Enterprise S.r.l. Unipersonale
Sede legale: Via della Porta n°10 66040 Pizzoferrato (CH)
Sede operativa: Via don Biagio Iorio n°18 80026 Casoria (NA)
Tel. 081/5739710 – info@gidierre.it
P.iva 02433750698