NUOVO REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

Storia della normativa "Privacy" in breve

Legge 675/1996 -sulla protezione dei dati personali. I "dati personali" devono essere trattati seguendo regole ben determinate, con l'obbligo di adozione delle misure di sicurezza.

D.lgs. 196/2003 -Codice della privacy (normativa ancora in vigore). E' stata unificata in un unico testo la normativa e le misure di sicurezza sono previste dall'Allegato B. Il Codice è stato integrato da numerosi provvedimenti del Garante che disciplinato il trattamento in specifici settori di mercato.

Regolamento UE 2016/679 -pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04.05.2016 ed entrato in vigore il 25.05.2016 e **si applicherà in tutti gli Stati Membri a partire dal 25.05.2018**, termine entro il quale le aziende dovranno adeguarsi alla nuova legge sulla privacy. Ricordiamo che i Regolamenti UE sono immediatamente esecutivi, non richiedendo la necessità di recepimento da parte degli Stati Membri, per questo motivo si avrà una maggiore armonizzazione della normativa in materia privacy in tutto il territorio europeo.

Principali novità e cosa resta invariato

Il Regolamento introduce regole più chiare in materia di informativa e consenso, definisce i limiti al trattamento automatizzato dei dati personali, pone le basi per l'esercizio di nuovi diritti, stabilisce criteri rigorosi per il trasferimento dei dati al di fuori dell'UE e per i casi di violazione dei dati personali (**Data Breach**).
Restano sostanzialmente invariati

- Definizione di trattamento e dato personale

- Principi relativi al trattamento dati
- Liceità del trattamento
- Informativa
- Consenso
- Soggetti che effettuano il trattamento

Quali sono gli adempimenti principali in materia di privacy per una azienda rispetto al Codice della Privacy (D.lgs. 196/2003)?

I principali adempimenti sono:

- Informativa agli interessati (dipendenti, clienti, fornitori, ecc.);
- L'acquisizione del consenso degli interessati (se non ricorre una causa di esonero prevista dall'articolo 24 del codice per i dati diversi da quelli sensibili e dall'articolo 26 del codice per i dati sensibili);
- Rispetto della autorizzazione generale del garante per il trattamento dei dati sensibili;
- Applicazione delle misure di sicurezza;
- Designazione di responsabili e incaricati del trattamento;
- Organizzare la propria struttura per agevolare l'esercizio dei diritti dell'interessato;
- Effettuare la notificazione al garante nei casi in cui questa sia prescritta dall'articolo 37 del codice.

Quali sono gli adempimenti principali in materia di privacy per una azienda rispetto al prossimo Regolamento EU 2016/679?

I principali adempimenti sono:

- I principi di base del trattamento, comprese le condizioni relative al consenso, a norma degli articoli 5, 6, 7 e 9;
- Registro dei trattamenti (Art 30);
- Informativa agli interessati (dipendenti, clienti, fornitori, ecc.) (Art. 13-20);
- Valutazione d'impatto sulla protezione dei dati (Art. 35);
- Rispetto della autorizzazione generale del garante per il trattamento dei dati a rischio (Art.36);
- Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita (Art. 25);
- Applicazione delle misure di sicurezza (Art 32);

- Designazione di responsabili del trattamento (Art. 28);
- Organizzare la propria struttura per agevolare l'esercizio dei diritti dell'interessato (Art. 15,21,31,34);
- Designazione del responsabile della protezione dei dati (per autotutela o obbligo) (Art 37-39);
- Effettuare le notifiche al garante nei casi in cui queste siano prescritte dagli articoli 33 e 36 del Regolamento.

Per rispettare la legge sulla privacy come bisogna comportarsi in caso di attività esternalizzate?

Il Garante prescrive di disciplinare i rapporti tra titolare del trattamento e soggetto esterno cui sia stata affidata una porzione di attività necessitante il trattamento dei dati personali. Il soggetto esterno (impresa, consulente) deve assumersi l'impegno di garantire un adeguato trattamento dei dati. Questo significa per esempio che il soggetto esterno cui sia stato affidato l'incarico di trattare i dati deve assumersi precisi impegni su base contrattuale. In proposito il Garante ha fornito alcuni suggerimenti ad hoc per la costruzione delle clausole contrattuali. Il soggetto esterno deve, tra l'altro, assumersi l'impegno di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali. Inoltre il soggetto esterno deve obbligarsi ad adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere. Visto che il soggetto esterno si obbliga a eseguire le istruzioni del titolare, è coerente prevedere un obbligo di report a carico del service e del consulente esterno. Questi devono assumere l'obbligo di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.

Cosa si intende per Valutazione d'impatto sulla protezione dei dati?

Con il Nuovo Regolamento Europeo: si effettua una valutazione degli impatti privacy analizzando i rischi, definendo i "gap" (distanze) rispetto alla corretta gestione dei rischi, stabilendo un piano per colmarli e controllando annualmente gli effetti degli interventi per ridurre i rischi.
Il nuovo documento quasi sicuramente si chiamerà Privacy Impact Assessment (PIA).

Cosa si intende per Accountability?

Con il Nuovo Regolamento Europeo è stato introdotto il principio di **accountability** (responsabilità verificabile), tutti i soggetti che partecipano al trattamento dati devono essere consci e responsabili e devono tenere documentazione di tutti i trattamenti effettuati. Chi non documenta, è soggetto a possibili sanzioni, ciò a

prescindere dall'utilizzo che si fa dei dati, è sufficiente non avere i documenti per essere perseguibili.

Come deve essere redatta l'informativa?

Con il Nuovo regolamento Europeo l'informativa deve essere leggibile, comunicativa, accessibile, concisa e scritta con linguaggio chiaro e semplice con un numero limitato di riferimenti normativi. Deve essere fornita per iscritto (oralmente va bene solo se l'interessato è d'accordo e la sua identità deve comunque essere comprovata con altri mezzi).

L'informativa agli interessati è un atto con cui chi tratta i dati altrui, si identifica e rende noto agli interessati le caratteristiche del trattamento, illustrando i diritti riconosciuti dalla legge. È un atto che deve precedere il trattamento, privo di particolari formalità, ma deve essere idoneo allo scopo perseguito. L'adempimento è a carico sia di soggetti privati sia di soggetti pubblici.

Nell'informativa devono essere indicati i soggetti o le categorie di soggetti che possono venire a conoscenza dei dati personali in qualità di responsabili o incaricati. L'informativa può essere fornita oralmente o per iscritto (necessariamente per iscritto per gli enti pubblici nei modelli di dichiarazioni sostitutive).

Deve contenere:

- le finalità, la durata e le modalità del trattamento cui sono destinati i dati;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- i diritti dell'interessato;
- gli estremi identificativi del titolare e, se designati, del suo rappresentante nel territorio dello stato del responsabile.

Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Se è stato designato un responsabile esso sarà indicato come referente dell'interessato per l'esercizio dei suoi diritti.

Come deve essere redatto il Registro dei Trattamenti?

Per le imprese o organizzazioni con più di 250 dipendenti è previsto un duplice obbligo documentale: quello del **Registro delle attività di trattamento** che deve essere redatto (anche in formato elettronico) sia dal titolare che dal responsabile del trattamento e va esibito su richiesta al Garante.
L'obbligo di tenuta del Registro delle attività di trattamento si applica anche ad imprese con meno di 250 dipendenti se il trattamento:
a) presenta un rischio per i diritti e le libertà delle persone;
b) non è occasionale ed include dati personali sensibili, sanitari, sulla vita o sull'orientamento sessuale, genetici, biometrici, relativi a condanne penali e a reati.

Tale documento deve contenere le seguenti informazioni:

a) Nome e dati di contatto del titolare del trattamento, e ove applicabile del contitolare, del rappresentante del titolare e del responsabile della protezione dati;
b) Finalità del trattamento;
c) Descrizione delle categorie di interessati e delle categorie di dati personali;
d) Le categorie di destinatari a cui i dati sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) Ove applicabile, i trasferimenti di dati personali verso un paese terzo od una organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e la documentazione delle garanzie adeguate;
f) Ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative

Chi è il Data Protection Officer (DPO)?

Con il Nuovo Regolamento Europeo tutti gli enti pubblici e le aziende il cui core business coinvolge trattamenti di natura rischiosa devono istituire un responsabile per la protezione dei dati.
Il DPO sarà una figura manageriale con rinnovo periodico, sarà referente del Garante e dovrà avere requisiti e competenze elevate. Il DPO potrà essere sia un dipendente che un collaboratore esterno con regolare contratto.
Un gruppo di imprese può nominare un unico DPO.
Il DPO deve:

- Informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento.

- Sorvegliare l'osservanza del regolamento.
- Fornire se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati.
- Cooperare con l'autorità di controllo.
- Fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Che cosa è una banca dati?

È considerata una "banca di dati" qualsiasi complesso organizzato di informazioni riguardanti persone fisiche identificate o identificabili; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Cos'è un "databreach" e quali adempimenti se si verificasse?

I dati personali conservati, trasmessi o trattati da aziende e pubbliche amministrazioni possono essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Si tratta di situazioni che possono comportare pericoli significativi per la privacy degli interessati cui si riferiscono i dati. Il garante ha redatto una pagina apposita che riassume adempimenti in merito: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5033588

Quali sanzioni sono previste?

Dal punto di vista civilistico, viene confermata la responsabilità risarcitoria per il cd. "danno da trattamento", codificata all'art. 82 del Nuovo Regolamento Europeo, che così recita:
"Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento". Il titolare del trattamento o il responsabile è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
Per quanto riguarda l'applicazione delle nuove sanzioni amministrative pecuniarie da parte delle Autorità di Controllo, l'art. 83 del Regolamento stabilisce:

- Sanzioni amministrative pecuniarie **fino a 10.000.000 Euro** o, per le imprese, **fino al 2% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, nel caso di violazione di determinati obblighi posti dal Regolamento.
- Sanzioni amministrative pecuniarie **fino a 20.000.000 Euro** o, per le imprese, **fino al 4% del fatturato mondiale totale annuo** dell'esercizio precedente, se superiore, nel caso degli obblighi più stringenti posti dal Regolamento (anche nel semplice caso di inosservanza degli ordini del Garante) .
- Con riferimento alle sanzioni penali, invece, come è noto il Diritto dell'Unione Europea non può prevederne, essendo **la materia penale di stretta competenza nazionale.**

Ci sono indicazioni del Garante sull'approccio al GDPR?

Il Garante ha stilato e mantiene una guida all'applicazione:
http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

Dove trovo il regolamento?

Il Regolamento, composto da 99 articoli e 173 considerando (chiarimenti) è pubblicato a questo indirizzo:
http://www.garanteprivacy.it/garante/document?ID=6264597
Riferimenti generali del garante:
http://www.garanteprivacy.it/regolamentoue

Conclusioni

Dal D.lgs. 196 al GDPR sono trascorsi 13 anni. Nel 2003 **Facebook** non era ancora nato, i Social Media praticamente non esistevano, il Web era agli albori e, soprattutto, il **Cybercrime** era ben lontano dalle dimensioni assunte negli ultimi anni.

Per questi motivi, **il GDPR è molto orientato alla SICUREZZA DEI DATI, piuttosto che alla pura PRIVACY**

Il nuovo GDPR è scritto secondo una logica di diritto anglosassone: si parla di **PRINCIPI** (Protezione adeguata) e non impone regole.

La protezione dei dati deve essere pensata già in fase di progettazione (Privacybydesign).
Le aziende dovranno **adottare policy di SICUREZZA INFORMATICA** per non subire DataBreach e le conseguenti sanzioni.

Quindi uno dei principali obiettivi del GDPR è quello di sensibilizzare le aziende verso politiche di CyberSecurity più attente ed efficaci, sia nel loro interesse che di quello dei cittadini dell'Unione Europea.

Grazie per aver letto l'eBook. Resta sintonizzato.

Via Lambruschini, 6 - 06018 Trestina
Città di Castello - Perugia - Italy
Telefono 075 8642475
Email: info@zpu.it
Web www.zeropuntouno.it