YOUR COMPANY

GDPR

il nuovo regolamento della gestione dei dati personali

Via 123, 45678 Città, Stato
Telefono: 0123 2345 678
E-mail: info@company.com
Sito web : www.company.com

INDICE

CAPITOLO 1

L'evoluzione della Privacy e la gestione dei dati: il GDPR e i riferimenti normativi

GDPR, General Data Protection Regulation, è la sigla che identifica il Regolamento (UE) 2016/679, emanato il 27 aprile 2016, con cui si stabiliscono le norme valide in tutti i paesi dell'Unione Europea, in materia di dati personali.

L'innovazione tecnologica negli ultimi anni ha cambiato tutto: basti pensare all'evoluzione tecnologica di Industry 4.0, Internet of things e la crescente diffusione del commercio elettronico che hanno assegnato un ruolo di primo piano al dato, alla sua acquisizione e alla sua gestione.

I dati acquistano valore in sé e devono essere tutelati per ciò che rappresentano in sé e per il valore che assumono in relazione alle persone cui si riferiscono.

Il dato personale è diventato il fulcro della nuova **Data Economy**, che oggi si basa sulla conoscenza e sull'elaborazione delle informazioni, considerate un potenziale motore per lo sviluppo e una fonte di nuovi business.

L'interessato, soggetto cui si riferiscono i dati personali, è fin da subito considerato il vero protagonista della normativa.

FONTE	DESCRIZIONE
Sito del Garante per la protezione dei dati italiani	www.garanteprivacy.it
Testo del regolamento UE, completo dei riferimenti per ciascun "considerando"; documenti illustrativi di caratere generale; FAQ; il testo tradotto dalle linee guida del WP29	
Pagina web del Gruppo Articolo 29	http://ec.europa.eu/newsroom/article29/news-overviwe.cfm
Contiene le Linee Guida	
Portale della legislazione italiana vigente	www.normattiva.it
Contiene il testo delle leggi e degli atti aventi forza di legge, continuamente aggiornati al testo vigente	
Pagina della Commissione Europea	https://ec.europa.eu.commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
Contiene la Riforma	
Pagina della Commissione Europea	https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisation_en
Contiene l'illustrazione delle novità per Imprese e PA	

CAPITOLO 2

Data Protection
il nuovo processo aziendale

Le nuove regole del GDPR cambiano profondamente l'approccio alla tutela dei dati.

Dalla considerazione di essere un mero insieme di adempimenti, diventa un processo produttivo, che necessita di essere gestito attraverso procedure chiare e definite, tali da richiederne la gestione attraverso un modello organizzativo specifico, innovativo.

La precedente edizione della disciplina, la 196/2003, era incentrata sui diritti dell'interessato: il nuovo regolamento invece conferisce doveri e responsabilità agli interlocutori aziendali, titolare responsabile del trattamento mediante un principio definito Accountability.

Se il Codice in materia di dati personali (D.Lgs. 196/2003) aveva disegnato per i titolari del trattamento un serie di misure minime di sicurezza da adottare, senza le quali erano previste sanzioni, la nuova normativa sposta la scelta e la responsabilità sul tipo e la quantità di misure tecniche e organizzative sia necessario adottare sul titolare del trattamento, che assume l'onere della prova della compliance e ne diventa garante.

La Data Protection non è più solo quindi una materia delegabile a un consulente, a un esperto di tecnologia o a un ufficio legale ma è l'approccio dell'imprenditore, organizzativo e tecnologico che ha importanza, in funzione del fatto che la gestione del processo di Data Protection, per essere gestito al meglio, necessita di un budget.

CAPITOLO 3

Il Data Protection Officer

Accanto ai ruoli classici, individuati dall'edizione precedente della normativa quali titolare, responsabile ed incaricato, nasce la figura del **Data Protection Officer (DPO)** o meglio del **Responsabile della protezione dei dati personali.**

L'obbligatorietà della sua figura in azienda dipende:
• dalla tipologia di soggetto giuridico, privato o Pubblica amministrazione
• dalla quantità di dati personali trattati
• dalla frequenza e dal tipo di dati trattati, sensibili o giudiziari.

Il DPO, interno o un consulente esterno all'azienda, assume il ruolo di Auditor interno dei processi di Data Protection e esterno nei confronti del Garante della Privacy; è il suo primo contatto, infatti, in caso di violazioni rilevate nei trattamenti.

Inutile dire che il DPO riveste un ruolo chiave e per questo deve possedere requisiti di professionalità, conoscenza della normativa e elevata comprensione dei processi IT nonché competenze legali.

Questi i suoi compiti:
• **Informare** e consigliare il titolare o il responsabile del trattamento in merito agli obblighi derivanti dal regolamento europeo e conservare la documentazione relativa a tale attività e alle risposte ricevute.

• **Vigilare** sull'attuazione e sull'applicazione delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la formazione del personale che partecipa ai trattamenti e gli audit connessi.

• **Verificare** l'attuazione e l'applicazione del Regolamento europeo; la

sicurezza dei dati; il riscontro alle richieste degli interessati di esercitare i diritti riconosciuti dal Regolamento.

•**Garantire** la conservazione della documentazione relativa ai trattamenti effettuati dal titolare.

•**Controllare** che le violazioni dei dati personali siano documentate, notificate e comunicate.

•**Controllare** che il titolare o il responsabile del trattamento effettui la valutazione d'impatto sulla protezione dei dati e richieda l'autorizzazione preventiva o la consultazione preventiva nei casi previsti.

•**Fungere** da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

•**Controllare** che sia dato seguito alle richieste del Garante per la protezione dei dati personali e, nell'ambito delle sue competenze, cooperare di propria iniziativa o su richiesta dell'Autorità.

CAPITOLO 4

Il trattamento dei dati: consensato, espresso e libero

Il consenso dovrebbe essere espresso mediante "un'azione positiva inequivocabile con la quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare che i dati personali che lo riguardano siano oggetto di trattamento, ad esempio mediante dichiarazione scritta, anche elettronica, o orale."

Recita così il Considerando 25 del nuovo regolamento europeo.

Il **trattamento** dei dati da parte dell'interessato, può essere effettuato attraverso la richiesta del **consenso.**

Il consenso può essere raccolto anche in modo elettronico o orale ma deve essere libero da eventuali conseguenze negative, informato in modo trasparente e semplice, specifico per lo scopo per cui viene richiesto.

Il consenso al trattamento dei dati personali deve essere espresso con azioni positive inequivocabili: il legislatore in questo modo ha definitivamente fatto decadere il consenso tacito passivo o pre-confezionato.

La richiesta per la raccolta è necessario sia chiara, concisa e non disturbare il servizio per il quale il consenso è espresso.

Sono fatti salvi i casi di legittimo interesse per i quali il legislatore fornirà spiegazioni e casistiche più dettagliate.

CAPITOLO 5

L'informativa il documento di trasparenza e correttezza tra l'azienda e l'interessato

L'Informativa è a tutti gli effetti uno strumento di informazione e non più un atto dovuto.

E' il documento di valore in cui vengono indicate tutte le informazioni al trattamento richiesto e **suggella il patto di chiarezza e correttezza tra l'azienda e l'interessato, qualunque sia la tipologia di interlocutore: fornitore, cliente, collaboratore, dipendente.**

E' evidente che debba essere formulata con un linguaggio chiaro, conciso e semplice anche con l'ausilio di icone standard e esaustive.

Il legislatore ha previsto la comunicazione dell'informativa in varie forme in funzione dei canali di comunicazione di cui l'azienda fa uso:

• per il **sito web,** canali social e mobile: l'informativa è resa in forma scritta, anche con mezzi elettronici

• per le **attività di Customer Care** e promozione telefonica: in forma orale, solo se richiesto dall'interessato e se la sua identità è comprovata.

CAPITOLO 6

Il DIPIA
per l'analisi del rischio e il Registro dei trattamenti

E' il nuovo strumento il **Data Protection Impact Assessment (DPIA),** il documento in cui vengono valutati e riepilogati i rischi derivanti dal trattamento dei dati in azienda e i possibili impatti sugli interessati in relazione ai propri diritti e libertà.

La predisposizione del DIPIA è necessaria fin dalla progettazione del nuovo processo di Data Protection.

Può essere redatto anche grazie all'ausilio di programmi informatici specifici che definiscono la sicurezza delle reti aziendali, inclusi i dispositivi infrastrutturali di conservazione dei dati aziendali, in modalità on-premise o in modalità As a Service (Cloud), da attacchi cyber, protagonisti ormai degli articoli di cronaca negli ultimi mesi, anche a danno dei massimi organismi di sicurezza.

Il processo prevede tre distinte fasi da svolgersi periodicamente:
1. Analisi dei rischi
2. Definizione della lista delle criticità
3. Definizione del programma di intervento.

Il DIPIA si configura perciò agli occhi del Legislatore come un piano di autovalutazione e di consapevolezza dei rischi circa il trattamento dei dati può cagionare a terzi.

Nel caso in cui, dal DIPIA emergesse un elevato indice di rischio, il titolare avrebbe la facoltà di richiedere un consulto da parte dell'autorità Garante in riferimento alle attività di trattamento in oggetto.

I trattamenti in corso devono essere comunicati all'autorità garante, attraverso il Registro del trattamento, che deve essere esibito su richiesta. A carico del titolare del trattamento è infatti in capo l'onere della prova della conformità dell'azienda alle disposizione di legge, condiviso dal responsabile del trattamento nel caso in cui venga eseguito per conto del titolare.

Sono esonerate dall'obbligo di redazione del registro del trattamento "le imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati, o i dati personali relativi a condanne penali e a reati".

Il registro deve contenere:

• il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati

•le finalità del trattamento

•le categorie di interessati e delle categorie di dati personali

• I destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali.

• se applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale, e la documentazione delle garanzie adeguate

• i termini ultimi previsti per la cancellazione delle diverse categorie di dati

• una descrizione generale delle misure di sicurezza tecniche e organizzative.

CAPITOLO 7

La violazione delle regole. Cosa fare in caso succeda

La violazione delle norme del nuovo regolamento GDPR, in ragione del principio di responsabilizzazione dei referenti aziendali sulla protezione dei dati, prevede un sistema sanzionatorio amministrativo articolato.

Le conseguenze economiche sono molto elevate, in funzione del tipo di violazione, ma con possibilità da parte del Garante di adeguarle ai casi concreti.

Le sanzioni si diversificano in funzione del tipo di violazione:

Per le violazioni di obblighi del titolare e del responsabile, dell'organismo di certificazione e dell'organismo di controllo:

• Fino a € 10.000.000 o il 2% del fatturato dell'impresa o del gruppo di imprese

Per le violazioni dei diritti degli interessati e delle condizioni di trattamento

• Fino a € 20.000.000 o il 4% del fatturato dell'impresa o del gruppo di imprese

In sede civilistica esiste comunque sempre il sistema sanzionatorio da parte dell'interessato che può, in casi di comprovata violazione dei suoi diritti e libertà, rivolgersi giudizialmente alle Autorità competenti per richiedere il risarcimento del danno.

CAPITOLO 8

La violazione dei dati. Cosa fare in caso succeda

Le violazioni, contemplate negli artt. 33 e 34, che citano:

"la «violazione dei dati personali» è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

La violazione dei dati, qualunque sia stata la causa che l'ha originata, se ha comportato un rischio per i diritti individuali dell'interessato e la sua libertà, deve essere segnalata senza esitazione, sia all'Autorità di controllo entro 72 ore dall'accadimento e sia all'interessato.

L'obbligo di segnalazione prende il nome di **Data Breach** notification e il mancato rispetto di questo obbligo comporta sanzioni penali.

La notifica di violazione al Garante deve contenere:

• **descrizione della natura della violazione**, compresi, se possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione

• **comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati** o di altro punto di contatto presso cui ottenere più informazioni

• **descrizione delle conseguenze della violazione** dei dati personali

• **descrizione delle misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

La notifica tardiva al Garante, oltre le 72 ore, è sempre possibile ma è necessario fornire le motivazioni del ritardo.

Sarà poi l'Autorità a valutare se la violazione vada notificata anche agli interessati.

CAPITOLO 9

I diritti dell'interessato: trasparenza, portabilità, oblio, limitazione del trattamento

I diritti degli interessati sono disciplinati agli artt. da 12 a 23, per la maggior parte già contemplati nella normativa del 2013.

Le novità del nuovo regolamento GDPR:

• **diritto alla trasparenza**
precisa i tempi (30 giorni) e modalità di risposta alle richieste, che devono essere esposte con linguaggio semplice e chiaro, motivazioni esplicite e modalità di tutela in caso di mancate risposte

• **diritto alla portabilità dei dati**
permette agli interessati di ottenere e riutilizzare i propri dati per i propri scopi e attraverso servizi diversi, facilitando la circolazione, la copia e il trasferimento dei dati da un sistema informatico ad altri

• **diritto all'oblio o cancellazione dei dati**
riguarda i casi di trattamento di dati non necessari, di revoca del consenso di opposizione di obbligo legale alla cancellazione, includendo il diritto alla deindicizzazione dai risultati dei motori di ricerca.

• **diritto alla limitazione del trattamento**
si applica al blocco del trattamento in caso di contestazione dell'esattezza dei dati

• **diritto di opposizione al trattamento,**
si applica al trattamento dei dati basati su legittimo interesse

• **diritti relativi alle decisioni automatizzate e alla profilazione**
consiste nel diritto all'intervento umano per contestare la decisione e esprimere la propria opinione

Esercitare i diritti di accesso, modifica, integrazione e cancellazione dei dati personali è sempre possibile. Oggi le procedure per l'esercizio dei propri diritti sono state rese più semplici dal legislatore, che ha posto in capo al titolare l'onere di dare esecuzione alle richieste, gratuitamente, con linguaggio semplice e in tempi brevi, anche con l'ausilio si mezzi elettronici.

CAPITOLO 10

Privacy by design e Privacy by default: LESS IS MORE

I due concetti sono la massima espressione dello spirito del GDPR, ovvero il principio di minimizzazione dell'uso dei dati oggetto di trattamento: i dati devono essere pertinenti, adeguati e limitati nel tempo, in funzione dello scopo per cui sono raccolti.

Si indica con **Privacy by design** la progettazione della tutela sin dall'origine della raccolta per considerarne la protezione in tutto il ciclo di vita del dato.

Privacy by default significa che occorre prevenire raccolte di dati non necessari per le finalità perseguite, evitando di acquisire informazioni eccedenti rispetto agli obiettivi dichiarati nell'informativa.

GRAZIE

YOUR COMPANY

Via 123, 45678 Città, Stato
Telefono: 0123 2345 678
E-mail: info@company.com
Sito web : www.company.com