COMUFFICIO

VADEMECUM SULLA NORMATIVA EUROPEA DELLA SICUREZZA DIGITALE

Cosa cambia per le aziende con il nuovo regolamento europeo sulla Privacy - GDPR

VADEMECUM SULLA

NORMATIVA EUROPEA SULLA SICUREZZA DIGITALE

Cosa cambia per le aziende con il nuovo regolamento Europeo sulla Privacy General Data Protection Regulation (GDPR)

Sommario

COMUFFICIO

Perché la guida

Gli analisti economici definirebbero "incumbent" (che sta per arrivare) l'effetto del "**pacchetto protezione dati personali"** conseguente ai Regolamenti Europei 679 e 680 del 2016. Si tratta di norme già approvate, ma che diventeranno pienamente obbligatorie (e contestabili) a partire dal **21 maggio 2018**.

E' una data ormai dietro l'angolo che porterà a nuove importanti necessità per tutte le organizzazioni, tanto le aziende private quanto gli Enti Pubblici, **e che apre opportunità di business alle aziende del settore ICT**, sia in termini di hardware, sia di software ma soprattutto di consulenza e di servizi personalizzati.

Il testo impone infatti alle imprese e alle pubbliche amministrazioni una forte e reale responsabilizzazione alla **protezione dei dati personali**.

La responsabilità della protezione non potrà più schermarsi dietro il mero adempimento formale di una firma per presa visione dell'informativa o per il rilascio del consenso al trattamento: il regolamento infatti si fonda su alcuni nuovi principi, quali **la protezione del dato fin dalla progettazione dei sistemi informatici** (**Project by Design**), **la presenza di un Responsabile/Controller, e la verifica continua** dell'utilizzo del sistema da parte dalle risorse interne all'organizzazione.

Appare palese che si parla tanto di integrazione dei sistemi, quanto di formazione del personale, quanto di assistenza (tecnica e formativa) periodica.

In termini sintetici, possiamo dire che il regolamento prevede:

- la **valutazione preventiva** del sistema preesistente e della rilevanza dei dati trattati all'interno dell'azienda, azione da svolgere con un approccio aperto e moderno: ad esempio si cita un recente caso di un artigiano mobiliere che ha subito un attacco a causa del quale gli sono stati rubati dati relativi a elementi d'arredo esclusivi progettati per i clienti finali da alcuni designer internazionali che hanno fatto richiesta di risarcimento per il furto di opera d'ingegno;
- la **definizione di regole interne e di misure di sicurezza** adeguate ed efficaci a protezione dei dati e che siano costantemente riviste e aggiornate;
- la presenza **di un responsabile/Controller** (DPO - Data Protection Officer), previsto come obbligatorio dalla normativa e incaricato di mantenere la compliance ai requisiti della norma.

Ne consegue che il buon fornitore/partner dovrà essere in grado di interloquire col Cliente su temi tra loro diversi ma tutti importanti: capacità di analisi dei processi dell'azienda cliente, conoscenza di elementi di risk management, conoscenza delle soluzioni tecniche per la protezione del sistema, conoscenza di elementi di protezione assicurativa per la tutela del rischio, capacità di formare una figura professionale.

Si tratta evidentemente di un notevole salto di qualità nella relazione col cliente, e proprio questa difficoltà rappresenta la sfida da vincere per conquistare questo importante mercato che si sta aprendo. Per darne una misura, nel 2016 il danno sostenuto dalle aziende italiane per attacchi cyber è stato valutato in 900 milioni di euro, le aziende o Enti che dovranno sottostare alla normativa sono stimate in 4 milioni, e il Sole 24 Ore ha stimato che per il nuovo ruolo di Controller occorreranno tra i 50 e i 140 mila nuovi addetti.

Gli obiettivi che ci siamo posti sono due: aiutare gli Associati ad essere in regola con la normativa, sostenere gli Associati nella loro azione sul mercato della cyber sicurezza.

Adeguarsi al GDPR in 6 passi

1. RACCOGLIERE E MAPPARE I TRATTAMENTI DEI DATI

In questa fase è cruciale identificare la documentazione interna riguardante il trattamento dei Dati personali e creare il Registro delle attività di trattamento (obbligo introdotto dall'art. 30 del GDPR).

Per ogni trattamento dei dati personali bisognerà domandarsi:

CHI	- determina le finalità e le modalità dei trattamenti di dati? - effettua il trattamento dei dati?
QUALI	- tipologie di Dati vengono Trattati? - rischi comporta il trattamento?
DOVE	- vengono custoditi i dati? - vengono (eventualmente traferiti) i dati (UE - extra UE)?
QUANDO	- i dati vengono raccolti?
COME	- viene garantita la protezione dei Dati? - sono minimizzati i rischi di accesso non autorizzato?

2. INDIVIDUARE LA PROPRIETA' DEI DATI

In questa fase sarà utile verificare che:

- i Dati raccolti siano strettamente necessari per le finalità perseguite dall'azienda
- sussista una base giuridica per il trattamento dei Dati, sia stato dato consenso al trattamento in modo chiaro e indiscutibile
- sia garantito il diritto all'accesso, rettifica, portabilità e revoca del consenso al trattamento
- sia garantito il *diritto all'oblio* (ottenere la cancellazione di dati non più necessari alle finalità)
- siano rispettate le disposizioni in materia di sicurezza

3. DESIGNARE IL DATA PROTECTION OFFICER (DPO), PER CHI E' OBBLIGATORIA QUESTA FIGURA?

In questa fase, in presenza delle condizioni previste dal Regolamento, è fondamentale nominare il DPO ossia il soggetto che assume la funzione di informazione, consulenza e controllo della gestione dei Dati. E' richiesta una persona che "*abbia conoscenza della Normativa e delle pratiche in materia di protezione di dati nel controllo del rispetto del Regolamento"* e che:

- Sensibilizzi sull'impatto del trattamento dei Dati
- Monitori la conformità dell'azienda al GDPR

IMPORTANTE → *il DPO non è mai responsabile della conformità del trattamento dei Dati ma la responsabilità resta in capo al Titolare o al Responsabile del Trattamento.*

4. ORGANIZZARE I PROCESSI INTERNI

In questa fase bisogna riorganizzare e implementare i processi interni all'impresa circa il trattamento dei Dati considerando i potenziali *Data Breach mediante:*

- Piani di formazione dei dipendenti
- Creare un modello per gestire i reclami e le richieste degli interessati
- Creare un modello per notificare eventuali violazioni alle autorità competenti entro 72 ore

5. GESTIONE DEI RISCHI

In questa fase è importante mantenere correttamente tenuto il Registro dei trattamenti (art. 30 GDPR). Se i dati presentino un elevato rischio per i diritti e le libertà dell'interessato è fondamentale effettuare una apposita valutazione dell'impatto sulla protezione dei dati (DPIA - Data Protection Impact Assessment).

6. DOCUMENTARE LA CONFORMITA'

In questa fase va redatto un documento di rendicontazione delle attività svolte e il relativo piano di rimedi in uso e in implementazione per contrastare i profili di rischio emersi. Dare visibilità a: aver reso idonea l'informativa alla raccolta Dati, l'ottenimento del consenso, la nomina del responsabile, la conformità alle richieste del Regolamento.

Come è cambiata la normativa sul rischio informatico e cosa comporta per le aziende

La strategia della commissione europea sulla data protection:

- Direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione
- Miglioramento degli strumenti di contrasto al cyber crime tramite il ravvicinamento della normativa penale degli Stati Membri
- Miglioramento della collaborazione transfrontaliera tra autorità
- Creazione di un sistema efficace di monitoraggio e raccolta di dati statistici sui reati informatici
- Creazione dell'European Cyber Crime Center

A chi si applica

A tutti i soggetti, inclusi gli Enti Pubblici.
La condizione è quella del trattamento di dati personali relativi a persone fisiche.
Si supera anche la riduzione effettuata dalla Manovra Monti del 2011, che aveva portato ad escludere i dati se relativi alle persone giuridiche.

Cosa cambia rispetto al D. Lgs. 196/2003 e chi effettuerà i controlli

Mantiene tutti gli obblighi della 196, ma ne aggiunge altri con una logica nuova e del tutto diversa.
Il criterio è quello di dimostrare di essere a conoscenza del potenziale rischio e di aver attivato delle azioni **specifiche, reali, dimostrabili** per evitarlo.
Vengono ora **valutati in particolare il progetto e la sua realizzazione.**
Il controllo della compliance alla normativa è stato affidato alla **Guardia di Finanza**.

Qualche esempio pratico

Il fornitore di software di **CRM** ha, già ora, due obblighi:

1. fornire un sw che sia già compatibile con la nuova normativa;
2. ricontrattualizzare **l'assistenza ai CRM** già forniti ponendosi nelle regole dei rapporti di subfornitura previsti dalla norma.
   Nei servizi che prevedono una **subfornitura** (es. cloud) deve essere indicata tutta la filiera di subfornitura con obbligo di notifica in caso di cambiamento del subfornitore e possibilità di rescissione del contratto da parte del cliente finale.
   Per tutti i servizi che prevedono un **data retention** deve essere indicata la **expiry date**, ovvero la data in cui i dati inutilizzati verranno distrutti.

Misure da adottare

Misure di sicurezza da adottare sulla base di una valutazione di impatto in materia di privacy

- Tutelare **l'integrità dei dati e la riservatezza, nonché l'integrità dei sistemi**;
- Garantire la capacità di disaster recovery;
- Prevedere delle misure di sicurezza aggiuntive in caso di dati sensibili;
- Provare e verificare le policy e procedure di sicurezza;
- **Predisporre un PROJECT BY DESIGN dell'azienda e designare, ove obbligatorio, un Responsabile/Controller dal 21 maggio 2018**

Sanzioni

Sanzioni amministrative comminate nei casi di mancata predisposizione e adesione al Project By Design

Sanzioni fino **a 20.000.000,00 oppure al 4% del fatturato mondiale di gruppo**, nel caso siano violati:

- Principi relativi al trattamento ed al consenso;
- Disposizioni relative ai diritti dell'interessato;
- Disposizioni in materia di trasferimento dati;
- Violazione di ordine di cessazione del trattamento.

Sanzioni **aggiuntive** fino **al 2% del fatturato mondiale di gruppo**, nel caso siano violate le norme relative a:

- Notifica Data Breach alle Autorità competenti;

Notifica Data Breach agli Interessati;**La notifica verso le Autorità competenti e gli Interessati deve essere effettuata entro le 72 ore dal momento in cui si scopre l'attacco informatico.**

In termini minimi il regolamento prevede:

a) una valutazione preventiva della rilevanza dei dati (un laboratorio di analisi cliniche o uno studio legale avranno una situazione più delicata rispetto ad una sartoria o un retail);
b) la definizione di regole interne e di misure di sicurezza adeguate ed efficaci a protezione dei dati e che siano costantemente riviste e aggiornate;
c) la conformità delle attività ai principi alle disposizioni del regolamento europeo, compresa l'efficacia delle misure e le modalità di avviso in caso di attacco ai dati;
d) l'esistenza, seppure non sempre obbligatoria, di un Responsabile o (DPO - Data Protection Officer) incaricato di mantenere la compliance ai requisiti della norma;
e) l'obbligo del titolare o del DPO di tenuta di un **registro delle attività** di trattamento effettuate sotto la propria responsabilità, con relativa descrizione delle misure di sicurezza;
f) la possibile adesione a **codici di condotta** o a un **meccanismo di certificazione** quale elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

COMUFFICIO

Check List verso il GDPR

L'elenco di controllo ha lo scopo di avvicinare le aziende al traguardo del GDPR evidenziando eventuali criticità di base nel sistema aziendale.

Dati Personali raccolti da cittadini UE

1. Quali sono i dati personali che vengono raccolti?
2. Dove vengono memorizzati i Dati Personali?
3. I Dati Personali vengono trasmessi? Se sì, come? Vengono trasmessi extra UE?
4. Quali sono le procedure di Conservazione dei Dati Personali?
5. Chi si occupa della custodia dei Dati Personali?

Procedure per il Consenso alla raccolta Dati Personali

1. Il consenso viene richiesto in modo esplicito e con termini inequivocabili?
2. Viene evidenziato in modo chiaro il responsabile del trattamento e il responsabile della protezione?
3. I tempi di memorizzazione del dato sono esplicitati?
4. E' che gli interessati hanno diritto ad accedere ai loro Dati personali, correggerli, richiederne l'eliminazione?
5. L'eventuale trasferimento dei dati extra UE è comunicato in modo chiaro?
6. Si evidenzia quali sono le conseguenze nel caso si decidesse di non fornire Dati personali?
7. Il ritiro del consenso è facile da effettuare come la concessione?
8. Come fanno gli interessati ad accedere ai propri Dati Personali?
9. E' normato l'invio dell'informazione in caso di violazione dei Dati Personali?

Procedute per la manutenzione dei registri dei dati e le policy per l'elaborazione dei dati

1. I consensi vengono registrati?
2. Viene tenuta una registrazione del trattamento dei Dati Personali?
3. Che livello di sicurezza hanno le registrazioni dei Dati Personali?
4. Vengono aggiornate le procedure che descrivono l'elaborazione dei Dati Personali?
5. C'è un rappresentante nella UE per eventuali titolari non UE?
6. Se le elaborazioni dei dati sono esternalizzate il contratto è conforme col GDPR?
7. Che controllo viene effettuato per l'accesso a server o edifici ove sono contenuti i dati?
8. Sono effettuate azioni preventive contro la vulnerabilità o gli incidenti che possono mettere a rischio i dati?
9. Esiste una procedura per inviare notifiche di Data Breach entro 72 ore?
10. C'è una procedura per valutare la possibilità di operazioni a rischio?
11. Viene compilato un registro delle modificazioni delle procedure?
12. Vi è un responsabile della protezione dei Dati Personali?

Comportamento degli operatori

1. E' svolta formazione e sensibilizzazione del personale?
2. Esiste un disciplinare interno, una lettera di incarico di trattamento dei dati?
3. Vengono eseguiti backup dei dati? Chi ne è responsabile?
4. Viene garantita la Business Continuity?
5. Le credenziali di accesso ai sistemi sono in possesso esclusivo dell'incaricato
6. E' stabilità una dimensione delle credenziali di accesso?
7. Vengono disattivati profili inutilizzati o relativi a rapporti cessati?
8. Sono presenti antivirus, anti-malware? Vengono regolarmente aggiornati?
9. Sono presenti firewall?
10. I dati sono contenuti in locali o in spazi non accessibin funzione della tipologia del dato?
11. Vengono monitorati logon sospetti?
12.

Comufficio è a disposizione per ulteriori chiarimenti.