ansap
associazione nazionale sindacale
attivita' produttive

# GDPR: cosa devono fare le aziende per mettersi in regola?

**Quando e per chi è valido il GDPR?**

è stato redatto nel **2016** sotto il nome di regolamento per la privacy e sarà attivo il **25 maggio 2018**.

Gli effetti però saranno validi in modo **retroattivo** quindi tutte le regole dovranno essere aggiornate anche per i dati storicizzati.

# Gli attori interessati sono 4:

**Data subject** ovvero i proprietari dei dati ovvero i consumatori (e non le persone giuridiche come le aziende)

**Data controller** ovvero le aziende che usano i dati per i loro scopi

**Data Processor** ovvero i servizi che collezionano i dati che le aziende usano come facebook o google analytics

**Data Protection officer** ovvero la persona che si occuperà di questa normativa e di farla rispettare all'interno dell'aziena

Il GDPR rappresenta indubbiamente un grosso cambiamento per tutte le aziende che per varie finalità e con diverse modalità raccolgono i dati di clienti, prospect o fornitori.

La buona notizia è che **sparisce l'obbligo di notificazione al Garante** di specifici trattamenti dei dati. E, di conseguenza, diremo addio agli oneri amministrativi e finanziari che quest'obbligo comportava (spese, queste, che incidevano soprattutto per le piccole e medie imprese).

L’obbligo di notificazione non scompare del tutto, bensì viene sostituito da un altro documento, il **registro del trattamento**. Si tratta di un documento che, su richiesta, può essere messo a disposizione dell’autorità di controllo.

L’obbligo di presentare questo registro **non compete alle imprese e 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”.

In sostanza, cosa devono fare le imprese per adeguarsi al nuovo GDPR?

Il GDPR del 2018 prevede la figura del **Data Privacy Officer (DPO)**, ovvero del responsabile per la protezione dei dati personali. Parliamo di un vero manager dei database aziendali, e non di un semplice garante del legittimo trattamento dei dati.

È obbligatorio nominare un Data Privacy Officer in questi casi:

- Chi tratta i dati è un soggetto pubblico
- Si trattano rilevanti qualità di dati personali
- Si trattano sistematicamente dati sensibili o giudiziari.

È prevista la possibilità di nominare come DPO un **consulente esterno all'azienda**.

Egli avrà il compito di interfacciarsi con il titolare o il responsabile del trattamento per informarlo sugli obblighi derivanti dal regolamento europeo, dovrà vigilare e verificare l'attuazione e l'applicazione della nuova normativa da parte dei titolare o del responsabile del trattamento;

inoltre, dovrà controllare che la documentazione relativa ai trattamenti effettuati sia opportunamente creata e conservata; infine, fungerà da punto di contatto per il Garante e ne raccoglierà le richieste.

Ecco
le principali
attività da
svolgere
prima del 25
maggio 2018:

Attribuire correttamente **i ruoli e il modello organizzativo** di gestione dei dati, designando un DPO quando necessario;

Effettuare la **mappatura delle banche dati**: dovrò analizzare quali dati sono presenti  e quali banche dati sono conservate in pc locali;

- Sostituire le soluzioni di archiviazione locale con **sistemi che centralizzino la gestione delle autorizzazioni e l'accesso ai dati**, affidandomi a soluzioni di storage e backup più affidabili, come i sistemi cloud;

- Realizzare la **mappatura dei trattamenti**: definire quali dati ho raccolto, la loro finalità e la provenienza, garantendo il principio della minimizzazione dei dati. Questo passaggio deve essere documentato lasciando un testo scritto coi dati mappati;

- Attribuire correttamente **i ruoli e il modello organizzativo** di gestione dei dati, designando un DPO quando necessario;

- Effettuare la **mappatura delle banche dati**: dovrò analizzare quali dati sono presenti  e quali banche dati sono conservate in pc locali;

- Sostituire le soluzioni di archiviazione locale con **sistemi che centralizzino la gestione delle autorizzazioni e l'accesso ai dati**, affidandomi a soluzioni di storage e backup più affidabili, come i sistemi cloud;

- Realizzare la **mappatura dei trattamenti**: definire quali dati ho raccolto, la loro finalità e la provenienza, garantendo il principio della minimizzazione dei dati. Questo passaggio deve essere documentato lasciando un testo scritto coi dati mappati;

- Attuare un **piano d'azione (Privacy Program)**, ovvero un processo strutturato di gestione dei dati.

Tutte queste attività dovranno essere compiute quanto prima, poiché si renderà necessario un periodo di prova in cui testare le nuove normative, anche per valutare quali siano le più efficaci sul piano della comunicazione.

# Le Sanzioni

Le **sanzioni** previste in caso di mancata osservanza delle regole sono tutt'altro che leggere;

esse possono arrivare, infatti, fino al 4% del fatturato globale annuo dell'azienda stessa o a 20 milioni di euro.

Per venire incontro alle aziende coinvolte e per una maggiore consapevolezza anche da parte dei cittadini stessi, spieghiamo quali sono le principali novità introdotte dal GDPR:

**Sportello unico** (*One Stop Shop*):

per facilitare il compito delle imprese operanti in più Paesi dell'Unione e uniformare l'approccio alla gestione dei dati, si farà riferimento a una sola Autorità Sovrintendente (Garante della privacy), quella dello Stato dove l'azienda ha la propria sede principale. Inoltre, le diverse Autorità degli Stati membri dovranno collaborare e operare congiuntamente e uniformemente nel loro compito di supervisione delle attività di gestione dati.

- **Principio di “responsabilizzazione”**:

i titolari del trattamento dati hanno la responsabilità (*accountability*) della gestione di tali dati, per cui non solo devono rispondere di eventuali danni alla libertà e alla privacy dei propri clienti, derivanti da gestioni poco sicure dei loro dati, ma devono soprattutto predisporre un’**analisi dei rischi** preventiva, in modo da evitare che tali danni si verifichino.

- ***Data breach***:

*il titolare del trattamento dati ha l'obbligo di comunicare al Garante per la privacy, entro 72 ore, eventuali* ***violazioni dei dati personali*** *riscontrate. Se la violazione rappresenta una minaccia per i diritti e le libertà delle persone coinvolte, inoltre, avrà l'ulteriore obbligo di comunicare il data breach anche agli interessati e fornire indicazioni su come intende limitare i danni.*

## DPO (Data Protection Officer):

il GDPR ha introdotto anche una nuova figura all'interno delle aziende che trattano dati personali, quella del Responsabile della protezione dei dati (Data Protection Officer), che avrà il compito di assicurare la corretta gestione dei dati da parte dell'azienda/ente.

Tale profilo deve essere selezionato sulla base di specifiche competenze "della normativa e delle prassi in materia di dati personali nonché delle norme e delle procedure amministrative che caratterizzano il settore" e di "qualità professionali adeguate alla complessità del compito da svolgere" (dovrà essere esperto, ad esempio, di processi informatici e di tecniche per la sicurezza dei dati e la gestione dei cyber-attacchi).

Il DPO deve essere **indipendente** dal titolare del trattamento e avere autonomia decisionale, deve riferire direttamente al vertice dell'azienda e deve avere a sua disposizione adeguate risorse umane e finanziarie per lo svolgimento del delicato compito che gli compete.

- **Portabilità dei dati**:

diritto di trasferimento (“portabilità”) dei propri dati personali da un titolare del trattamento a un altro, all’interno del territorio dell’Unione e fatta eccezione per i dati contenuti negli archivi di interesse pubblico.

- ***Consenso****:*

*il nuovo Regolamento europeo prevede norme più chiare in merito al consenso al trattamento dei propri dati personali, che deve essere esplicitato, così come devono essere chiare, legittime e pertinenti le finalità per cui tali dati saranno utilizzati; esso, inoltre, può essere ritirato o limitato in qualsiasi momento da parte dell’interessato.*

- **Sicurezza dei dati**:

il titolare del trattamento e il responsabile della protezione dei dati devono garantire la sicurezza di questi ultimi, mettendo a punto misure tecniche e organizzative adeguate al rischio calcolato.

- **Accesso ai dati**:

il titolare del trattamento dati avrà anche l'obbligo di predisporre un **registro delle attività di trattamento**, dove specificare le finalità della raccolta dati, le categorie di dati personali e di soggetti interessati, le misure di sicurezza adottate, ai fini della **trasparenza** e del rispetto del diritto di accesso ai dati da parte degli utenti.

**Diritto alla cancellazione, limitazione e rettifica**: l’interessato ha diritto a chiedere al titolare del trattamento dei suoi dati la cancellazione di questi ultimi o, anche, la limitazione del loro trattamento o la rettifica.

ansap
associazione nazionale sindacale attivita' produttive

TEAMLAB
PRIVACY COMPLIANCE

# *AFFIDATI AL NOSTRO GRUPPO*

Viste le svariate novità introdotte, è facile capire che l'**adeguamento** di aziende e Pubbliche Amministrazioni al **GDPR** non sarà certo semplice, in quanto richiederà un sostanziale impegno e investimento organizzativo, tecnologico e finanziario. Ma, allo stesso tempo, esso risulta necessario, oltre che giusto e vantaggioso per i cittadini dell'Unione.