# IL GDPR SVELATO

*Come sopravvivere al nuovo regolamento GDPR*

## QUANDO PARLIAMO DI GDPR...

...facciamo riferimento a una normativa europea per la conservazione dei dati nell'epoca digitale. Il regolamento europeo GDPR sarà attivo dal 25 maggio 2018 e questo comporta per le aziende tutta una serie di passaggi da effettuare per risultare conformi entro quella data. Sarà dunque necessario seguire una serie di regole dalle quali non ci si può esimere. Anche nel rarissimo caso in cui non si dovesse essere soggetti a GDPR o ad altre normative, è buona norma prendersi cura almeno dei dati finanziari, delle informazioni sui clienti, delle informazioni sul personale e sui fornitori, dei dati sui prodotti e delle informazioni commerciali.

La protezione dei dati personali è una questione importante. Nell'ultimo mese sono stati annunciati nuovi attacchi cyber, per cui le infrastrutture moderne potrebbero essere impattate – la sicurezza dei dati risultare a rischio – quindi è fondamentale trovare una soluzione per evitare la perdita dei dati.

PARLIAMO ANCHE DI:

- **DATA PROTECTION**
- **COMPLIANCE**

# Criteri

Ecco alcuni dei criteri da seguire per aderire, in qualità di azienda, al regolamento GDPR:

1. Rispetto del data breach: in caso di attacco informatico con compromissione di dati o fughe di dati, vi è l'obbligo da parte delle aziende di notificarlo entro 72 ore all'Autorità competente (garante) e agli utenti interessati.

2. Accountability: le aziende interessate devono essere in grado di dimostrare con prove documentali la loro piena conformità al regolamento.

3. Obbligo di trattare i dati in termini di sicurezza sia interna sia esterna rispetto alla mia organizzazione. La progettazione 'by design' ripercorre il cliclo di vita del dato, mentre la progettazione 'by default' prevede la massima tutela di default nelle configurazioni. Le progettazioni devono essere in linea con quelle che sono le linee guida del GDPR.

**Entro il 25 maggio 2018**

# Call for action

Call for action: adottare soluzioni idonee per rispondere ai requisiti del GDPR. Fra i requisiti:

1. Secure processing: è l'obbligo di progettare i dati in sicurezza all'interno e all'esterno di un'organizzazione per dimostrare di essere in piena compliance (tramite registro dei trattamenti).

2. Non è obbligatoria per tutti la nomina del Data Protection Officer, lo è per le amministrazioni pubbliche, per le aziende con più di 250 dipendenti e per tutti i soggetti che trattano dati su larga scala (es. grande distribuzione, chi lavora sul web, dati estrapolati dal web).

Una delle cause di violazione di sicurezza potrebbe essere la stampa di documenti. Avete idea di cosa venga stampato nel vostro perimetro aziendale?
'Un ambiente di stampa non controllato rappresenta un grave pericolo'. Fonte: ENISA: European Network and Information Security Agency.

.