GDPR
Consultant Team

Cos'è il GDPR

Il regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation- Regolamento UE 2016/679) Regolamento europeo sulla Privacy (Regolamento Generale sulla Protezione dei Dati – **RGPD**) è un Regolamento con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali di cittadini dell'Unione Europea e dei residenti nell'Unione Europea, sia all'interno che all'esterno dei confini dell'Unione europea (UE). Il testo, pubblicato su Gazzetta Ufficiale Europea il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno, inizierà ad avere efficacia il 25 maggio 2018.

Trattandosi di un regolamento, non necessita di recepimento da parte degli Stati dell'Unione e verrà attuato allo stesso modo in tutti gli Stati dell'Unione senza margini di libertà nell'adattamento. Il suo scopo è, infatti, **la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea**. In tal senso, quindi, non vi sarà una normativa italiana in materia, quanto piuttosto dei chiarimenti in relazione ad alcuni aspetti, ad esempio sui poteri dell'Autorità Garante nazionale.

Il regolamento pone con particolare enfasi l'accento sulla responsabilizzazione (**accountability**) del **titolare** e dei **responsabili del trattamento**, che si deve concretizzare **nell'attuazione di comportamenti proattivi a dimostrazione della concreta** (e non meramente formale) **dell'adozione del regolamento**. In particolare, si evidenzia la necessità di attuare misure di tutela e garanzia dei dati trattati, con un approccio del tutto nuovo che demanda ai titolari il compito di decidere autonomamente le modalità e i limiti del trattamento dei dati alla luce dei criteri specifici indicati nel Regolamento:

Sanzioni Art. 83

Condizioni generali per infliggere sanzioni **amministrative** pecuniarie

Viene previsto un aumento dei rischi e delle responsabilità, sia di carattere civile (cambia, notevolmente la responsabilità per i danni arrecati per effetto del trattamento di dati personali) sia di carattere amministrativo-pecuniario. Si rischiano sanzioni fino a **20.000.000** di euro o addirittura fino al **4% del fatturato mondiale annuo**.

Nell'analisi dell'apparato sanzionatorio del GDPR ci si concentra di solito sulle rilevanti cifre previste dall'articolo 83, che arrivano a colpire Titolari e Responsabili con sanzioni amministrative fino a 20 milioni di euro o fino al 4 % del fatturato mondiale totale annuo.

In realtà, come già previsto dalla legislazione vigente, le autorità di controllo hanno una serie di poteri correttivi previsti dall'articolo 58. Tali poteri prevedono fra gli altri la possibilità di limitare o vietare un trattamento. Le conseguenze economiche di una disposizione di questo tipo potrebbero essere anche più gravi di quelle derivanti da una sanzione amministrativa.

L'impossibilità di effettuare un trattamento potrebbe comportare, ad esempio, la sospensione dell'erogazione di un servizio verso i clienti, con le conseguenti possibili cause legali da parte di questi ultimi.

Se quindi le sanzioni amministrative possono avere conseguenze economiche e reputazionali, le azioni previste dall'articolo 58 possono comportare anche rischi sulla stessa sopravvivenza di un'azienda.

Prepararsi al GDPR

GDPR: le contromisure tecniche

La valutazione di impatto del trattamento (P.I.A., Privacy impact assessment) ha il compito di assicurare trasparenza e protezione delle operazioni di trattamento dei dati personali, imponendo al titolare l'onere di una valutazione preventiva delle conseguenze del trattamento dei dati sulle libertà e i diritti degli interessati.

Attività da svolgere:

- Predisporre un elenco dei vari sistemi informatici utilizzati (p.es. pacchetto office, eventuali applicativi specifici come programma di fatturazione, CRM, ecc.) e rendere disponibili le licenze;
- Elencare i vari utenti che utilizzano i programmi informatici e quali modalità di accesso hanno;
- Elencare quali sistemi ANTIVIRUS o FIREWALL utilizzati e che tipo di protezione è stata attivata;
- Fare un elenco delle varie e-mail aziendali, chi ne possiede l'accesso e come sono stabilite le credenziali di autenticazione (PASSWORD)
- Definire il sistema di salvataggio dei dati informatici, frequenza e modalità di salvataggio;
- Se si utilizzano sistemi in Cloud avere chiaro come vengono archiviati i dati e su quali server, se sono residenti in territori Italiani, Europei o fuori dai confini Europei;
- Definire le attività di distruzione supporti dismessi ossia corretta distruzione dei dati presenti su Hard Disk o supporti fisici

Sistemi minimi per la sicurezza informatica

Dal punto di vista informatico i sistemi minimi da attivare per dimostrare di aver compiuto tutte le attività necessarie ad evitare perdite di dati e proteggere i dati personali dei clienti da accessi non autorizzati (data breach) sono le seguenti:	**Ambito**	**Note**
Strumenti		
Accesso autorizzato ai dati e sistemi	Credenziali di accesso ai PC e Device Mobili	password complesse e con scadenza
Antivirus	Antivirus a copertura di Server, PC e device mobili	Software aggiornati
Firewall	Apparecchio necessario per impedire accessi non autorizzati alla rete aziendale e dotato di software per il monitoraggio delle minacce esterne ed interne	Software e firmware aggiornati
Accessi wifi	Accessi distinti per Ospiti e personale interno	Software e firmware aggiornati
Sistemi di backup	Back up locali e esterni (in cloud) Backup su unità locali dedicate (NAS, RDX)	Software e firmware aggiornati
Recupero dati di backup	Verifica periodica del recupero dei dati di Backup	

NOTA BENE

Questo documento è stato elaborato a mero scopo informativo e non deve essere inteso come parere legale o come esempio per stabilire come applicare il GDPR alla propria organizzazione. Ti invitiamo perciò a consultare un legale qualificato per analizzare il GDPR e capire come applicarlo nello specifico alla tua azienda in modo da assicurare il giusto livello di compliance.