



GDPR

NORMATIVA EUROPEA 2016/679 PROTEZIONE DATI PERSONALI

GDPR IN BREVE

Il GDPR ("Regolamento generale protezione dei dati - General Data Protection Regulation") di fatto è una importante presa di posizione ufficiale dell'Unione Europea nei confronti delle tecnologie e protezione dei dati personali.

Quello che forse non tutti sanno è che il GDPR è già in vigore, essendo stato definito il 25 maggio 2018 come data limite di applicazione della normativa. Obiettivo del regolamento è quello di garantire una adeguata protezione dei dati presenti su computer, server, gestionali, sistemi di posta, archivi cartacei e altro.

Il nuovo regolamento è applicato a tutti i titolari di attività dell'Unione Europea e, a differenza della precedente normativa, che prevedeva una serie minima di misure di sicurezza, si passa al concetto di *misure adeguate* per tutelare e garantire i diritti degli interessati presenti nei dati dei sistemi informatici.

In breve, il GDPR prevede maggiori diritti in termini di privacy personale e maggiori doveri in termini di protezione dei dati.

Sono inoltre previste segnalazioni obbligatorie di eventuali violazioni dati e severe sanzioni per mancato adeguamento. Questo implica una riprogettazione della intera struttura della gestione, conservazione e protezione dei dati.

COSA FARE

Il Regolamento Europeo obbliga ad un approccio piuttosto prudente e lungimirante, non si tratta più di una semplice compilazione di modulistica.

Deve essere dimostrata la validità delle misure e delle azioni messe in atto.

Sostanzialmente bisogna intervenire su due fronti :

Aspetto tecnico

con le misure pratiche necessarie per ridurre al minimo la possibilità violazione o perdita dati

Aspetto documentale

Dopo una fase di analisi della realtà aziendale e della tipologia dati presente, stesura di tutti i documenti necessari per dare evidenza alle misure prese per prevenire, o limitare al massimo, eventuali problematiche nella gestione dei dati in nostro possesso

COME INTERPRETARLO

L'impatto del GDPR coinvolge molti aspetti di una gestione aziendale. Costringe le aziende e gli studi a guardare alla gestione dei dati personali, in particolare quelli dei clienti, in una nuova ottica e consapevolezza. Nel caso di aziende medio grandi strutturate, adeguarsi può diventare un lavoro impegnativo, coinvolgendo molteplici settori.

Non è comunque mai troppo tardi per iniziare il processo di adeguamento.

Il 25 maggio 2018 non va inteso come punto di arrivo, ma piuttosto un nuovo punto di partenza.

Interpretandolo non come una gravosa imposizione, ma come uno strumento e occasione per una efficace riorganizzazione aziendale.

Il legislatore del GDPR ha scritto la normativa con una finalità ben precisa. Vuole che le aziende si rendano conto che trattare i dati comporta dei rischi e che i titolari siano attivi nella protezione dei dati. Per questo motivo, ad un trattamento adeguato va aggiunta la consapevolezza del rischio e dei metodi per prevenirli.

QUALI SONO I RISCHI

Una significativa rilevanza è assunta dalla possibilità di violazione o perdita dei dati.

Questo può non solo comportare sanzioni fino a 20 milioni di euro, ma anche danneggiare seriamente la reputazione della vostra azienda.

In questi casi, è infatti necessario informare gli interessati entro 72 ore, mentre nel caso si tratti di dati che possano presentare rischi per i diritti e libertà delle persone coinvolte, è inoltre necessaria una segnalazione diretta al Garante.

Ovviamente dimostrando di avere posto in essere tutte le misure ragionevolmente adeguate per la protezione dei dati su più livelli.

Esempi di violazione dei dati personali possono essere :

- Invio di una email contenente dati personali alla persona sbagliata
- Furto del computer o del notebook
- Dimenticare sulla stampante documenti contenenti dati personali
- Furto di copie dati di backup in formato facilmente leggibile





ORION INFORMATICA

Con una solida esperienza di 37 anni nel settore informatico, in particolare sull'aspetto sicurezza, la Orion Informatica è in grado di offrire proposte pratiche e concrete per qualsiasi esigenza di protezione dati e salvaguardia della privacy

Proponendo soluzioni complete e professionali, quali sistemi completi di crittografia dati e ambienti operativi, sistemi perimetrali di protezione integrata per accesso internet, unità di backup di rete con supporti cifrati

PARTE TECNICA

Crittografia integrale del sistema del sistema operativo Microsoft Windows, con tecnologia VeraCrypt e livello di sicurezza AES 256 bit

Sistema perimetrale di protezione security gateway serie USG Zyxel per accesso alla rete internet, con controllo traffico in tempo reale, controllo contenuti, analisi traffico, anti intrusione e firewall

Unità di backup di rete (NAS Network Attached Storage) Synology, da due a quattro dischi Western Digital serie Red Pro. Supporti esistenti completamente crittografati. Con possibilità di accesso esterno tramite internet, solo per soggetti abilitati con protezione password

Programmi di backup completamente automatizzati, con programmazione inizio e fine attività, spegnimento automatico dei computer.

Crittografia di sicurezza dati salvati e invio rapporto via email del risultato della copia effettuata

Utilizzo di unità esterne di backup, con capacità fino a 4 Tb, con supporto completamente crittografato

Disponibilità di spazi protetti, via internet con protocollo SFTP, per backup remoti esterni
Con controllo periodico della effettiva ripristinabilità dei backup effettuati

PARTE DOCUMENTALE

Definizione personalizzata dei ruoli

Possibilità di nomina del Titolare e dei Responsabili del Trattamento, delle persone autorizzate e dei responsabili esterni. Stesura delle rispettive lettere di nomina

Analisi dei trattamenti

Definizione del trattamento dati e delle finalità, con analisi del rischio di violazione, effetti sugli interessati e misure messe in atto per la riduzione del rischio

Registri delle attività di trattamento

Stesura dei registri per Titolari e Responsabili sulla base delle analisi effettuate, in ottemperanza degli obblighi della normativa

Lettere di incarico

Lettere di incarico e revoca per tutte le figure coinvolte nella gestione della protezione dati aziendale

Diritti degli interessati

Generazione delle informative e richieste di consenso sulla base dell'analisi dei trattamenti

Valutazione dei rischi (DPIA)

Analisi e valorizzazione dei dati trattati, con evidenziazione delle vulnerabilità e minacce derivanti
Calcolo degli impatti, analisi e ponderazione dei rischi
Identificazione delle misure per l'abbattimento del rischio