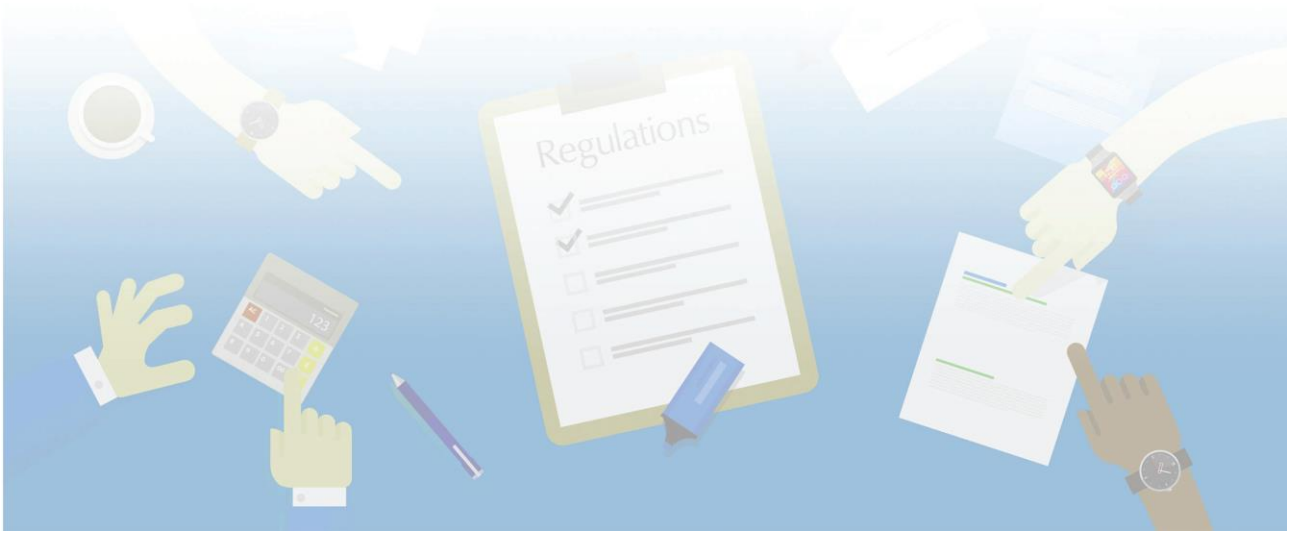
G.D.P.R.

Codice Europeo Privacy

Il **25 Maggio 2018** è il termine ultimo
per l'adeguamento al **G.D.P.R.**

Quest'ultimo regolamento sulla privacy porta diverse e importanti novità
in ambito di sicurezza dei dati, distaccandosi dalla regolamentazione attuale.
Vediamo come



1. Introduzione del diritto all'oblio con il quale gli interessati potranno ottenere la cancellazione dei propri dati personali anche online da parte del titolare del trattamento.

Questo significa che chiunque tratti i dati per utilizzarli pubblicamente in rete deve predisporre una modalità di cancellazione dei dati e dei link agli stessi per concedere il diritto all'oblio agli interessati.

2. Introduzione dell'obbligo della redazione del Privacy Impact Assessment (documento di valutazione d'impatto nel trattamento dei dati). In tale documento occorre considerare quali dati verranno trattati, quali sono i rischi concreti derivanti dall'utilizzo di tali dati e quali cautele possono essere messe in atto per prevenire e risolvere tali criticità. Il documento comprende una lista di potenziali rischi o criticità e un programma per la loro gestione e risoluzione.

Questo significa la reintroduzione di un documento analitico che riassuma chiaramente tutti gli adempimenti del GDPR.

3. E' cambiata, in senso più ampio, la definizione di dato personale in "*Qualsiasi informazione che identifichi o che permetta di identificare una persona fisica a cui ci si riferirà in seguito come "soggetto dei dati"; una persona identificabile è una persona che può essere identificata, direttamente o indirettamente, in particolare mediante un numero identificativo o da uno o più fattori specifici relativi alla sua identità fisica, psicologica, mentale, economica, culturale o sociale*".

Questo significa che il dato personale sarà un dato comprendente molte più caratteristiche identificative e dovrà essere trattato seguendo le regole del GDPR.

4. Data breach. In caso di violazione di dati che mettono in pericolo i diritti e le libertà delle persone, il Titolare del trattamento deve segnalare all'autorità nazionale quali sono gli individui in pericolo e comunicare alle persone interessate la violazione nel più breve tempo possibile (limite di 72h). Non si applica tale obbligo se il Titolare ha adottato misure di sicurezza tali da rendere illeggibili i dati violati (crittografia) o se è troppo grande il numero di interessati dalla violazione (in questo caso deve fare una comunicazione pubblica).

Questo significa essere pronti ad assumersi la responsabilità di vigilare e comunicare.

5. Privacy by design e by default. Garantire la protezione dei dati nei prodotti e nei servizi già dalle prime fasi del loro sviluppo, avendo già dei modelli di riferimento e variandoli di volta in volta a seconda del tipo di trattamento.

Questo significa che il tracciamento del dato, le misure minime di sicurezza e le analisi dei rischi non dovranno essere fatte per l'azienda in generale ma per ogni trattamento di ogni banca dati.

6.

Introduzione del diritto alla portabilità dei propri dati personali per trasferirli da un titolare del trattamento ad un altro.

Ad esempio le compagnie telefoniche dovranno provvedere alle automatizzazioni necessarie per trasferire i dati da un provider all'altro senza dover nuovamente fornire tutti i nostri dati.

7.

Le decisioni che producono effetti giuridici (come, la concessione di un prestito), non potranno essere basate esclusivamente sul trattamento automatizzato dei dati (ad esempio, la profilazione).

Questo significa che per certi tipi di dati non potranno più essere considerati validi ad esempio i form di auto compilazione per la raccolta degli stessi ma sarà necessario il rapporto fisico tra cliente e fornitore di servizio.

8.

Introduzione della crittografia o dei sistemi ad impronta digitale.

Questo per evitare che i dati possano entrare in possesso di persone non autorizzate.

9.

Introduzione del DPO che deve essere una figura con competenze informatiche, che conosca il regolamento europeo e che non sia in conflitto d'interesse all'interno dell'azienda (ad esempio non può fare il DPO chi è già responsabile dell'ICT).

Può essere un libero professionista o un dipendente interno o esterno all'azienda. Il suo compito è quello di osservare, valutare e gestire il trattamento dei dati personali allo scopo di far rispettare le normative europee e nazionali in materia di privacy.

10.

Pseudonomizzazione, il principio per cui le informazioni di profilazione debbano essere conservate in una forma che impedisca l'identificazione dell'utente.

Questo significa l'utilizzo di codici identificativi che non abbiano apparentemente nessun legame con l'interessato.

L'azienda inoltre deve avere:

Conoscenza precisa dei dati che ospitano e processano

- **Che tipo di dato è:** personale, sensibile, relativo al cliente o al dipendente
- **La sua posizione:** su quale device
- **Il suo utilizzo:** per quale scopo, per quanto tempo, da chi, in quali applicazioni
- **La sua sicurezza:** adottare le giuste precauzioni per proteggere i dati da un uso non autorizzato
- **Il modo in cui è raccolto:** consentito dalla legge o con il consenso del soggetto fornendo informazioni sul suo utilizzo e sui diritti del soggetto in relazione ai suoi dati

La capacità di gestire i dati personali in modo conforme alla normativa

- **Fornire su richiesta** dell'interessato i dati memorizzati, comprese le informazioni sul loro utilizzo in modo conciso
- **Cancellare su richiesta** dell'interessato i suoi dati in conformità al diritto all'oblio
- **Memorizzazione o conversione** di dati in un formato che consenta la portabilità ad altre piattaforme

Le pratiche pianificate IT che garantiscono la conformità con il GDPR

- Controlli interni efficaci e mitigazione dei rischi
- Pianificazione di nuovi processi, applicazioni e tecnologie che incorporano i requisiti del GDPR
- Istruzioni chiare su come reagire a una violazione della sicurezza dei dati personali

Il nuovo Regolamento sta per entrare in vigore ed è chiaro che servono strumenti in grado di poter intervenire dinamicamente sul trattamento dei dati in tempo reale.

Parlane con il tuo consulente informatico, la soluzione esiste ed è alla portata di tutti.

assist informatica

Via Delle Querce 15/17, 06083 Bastia Umbra (PG) – T. 075 8001062 – F. 075 8006640

www.assistinformatica.com – info@assistinformatica.com