Adeguamento trattamento dati secondo **GDPR** (General Data Protection Regulation)

Regolamento Ue 2016/679 (I primi 12 adeguamenti)

Entrato in vigore Il 25 maggio 2016 e applicato ufficialmente a partire dal 25 maggio 2018

1. Attivazione del **certificato SSL DV** (Domain Validated).
2. Forzare tutte le richieste SSL con **redirect** da http a https.
3. **Informativa** ai sensi dell'art. 13 del Regolamento UE n. 679/2016 (GDPR)
4. **Avviso cookie** con banner senza blocco. Ovvero attivare la barra delle notifiche che avvisa i navigatori dell'utilizzo di cookie di profilazione.
5. **Nomina Incaricato** del trattamento dei dati personali.
6. **Privacy by design**: onere, per chi detiene un database di informazioni personali, di organizzarlo e strutturarlo avendo ben in mente gli obblighi imposti dalla nuova normativa: eventuali problemi legati alla riservatezza dei dati, vanno prevenuti (e non corretti!) utilizzando tecniche adeguate come la **pseudonimizzazione** dei dati. In altre parole, qualora un soggetto intenda trattare dati altrui, deve prevedere un sistema che, sin dall'inizio dell'attività, riduca al minimo i rischi di una possibile violazioni dei dati raccolti.
7. **Architettura a 3 livelli**: le applicazioni a livello del server sono "**delocalizzate**" e ogni server è specializzato in un compito.
8. **Backup** dei dati in rete.
9. **Interfaccia sitoweb** secondo le nuove normative.
10. Invio **email tracciate**.
11. **Registro delle email** tracciate.
12. **Registro dei trattamenti**.

Aggiornamento **DB anagrafe** alla normativa GDPR (da valutare separatamente).

Chi non adempie alla Normativa del GDPR (General Data Protection Regulation) può subire sanzioni che arrivano fino al 4% del fatturato totale annuo.

Il GDPR si fonda sui principi di **Accountability, Privacy by design e Privacy by default.**

Accountability

Il titolare del trattamento è **responsabile** della scelta e della messa in atto di misure tecniche e organizzative adeguate a garantire che ogni trattamento è effettuato in conformità al Regolamento, e deve essere in grado di dimostrarlo.

Privacy by design & Privacy by default

La **protezione incorporata nella progettazione** (Privacy by design) rappresenta un insieme di principi, prassi e tecnologie con le quali sin dalla fase di pianificazione si progetta un sistema con intrinseche caratteristiche di protezione, configurate al massimo livello di protezione. Per impostazione predefinita (Privacy by default) le amministrazioni devono trattare **solo i dati personali nella misura necessaria e sufficiente per le finalità previste** e per il **periodo strettamente necessario a tali fini**.

Data breach prevention & detection

Necessità di adottare misure di sicurezza adeguate per la **prevenzione**, necessità di riconoscere gli incidenti di sicurezza e notificarli al Garante Privacy.