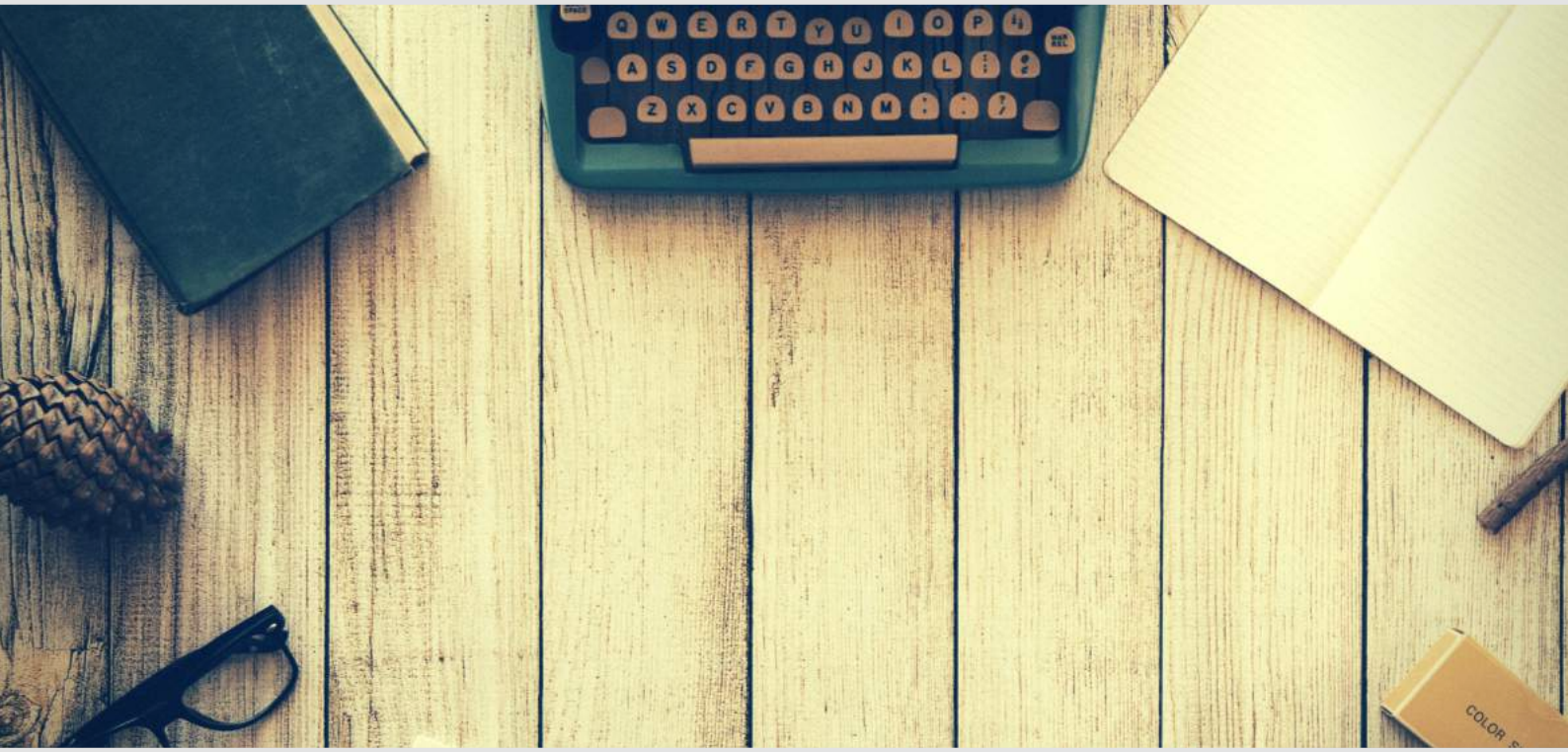
GDPR: INFO

Ecco una checklist per risultare conformi al GDPR



OSSERVAZIONI

Per risultare conformi al GDPR (General Data Protection Regulation) è necessario fare un audit innanzitutto allo scopo di stabilire il contesto fattuale della vostra società: quali dati avete, dove sono conservati, chi sono i terzi che accedono ai dati, quali problemi di conservazione possono esserci, livello di sicurezza, ecc. Questa checklist si concentra sull'aspetto legale, non pratico, della normativa GDPR.

Questa checklist presuppone che una società elabori sia i dati personali dei dipendenti sia quelli dei clienti, includendo le categorie speciali di dati. Essa non tratta problemi specifici di settore né ambisce a spiegare l'ambito di legge di chi controlla o è controllato dalla normativa. Si possono trovare maggiori informazioni qui, con l'invito di verificare la lista dei requisiti per la compliance al GDPR.

GDPR: TOOLKIT

Corporate Governance

Art. 30: I responsabili devono tenere un registro con indicato:
- il nome e i dati personali del responsabile e del DPO (qualora presente);
- lo scopo dell'elaborazione dati;
- una descrizione delle categorie dei soggetti e dei dati personali;
- le categorie di coloro a cui vengono rivelati i dati, inclusi quelli residenti all'estero;
- i trasferimenti di dati personali all'estero, inclusi i documenti di sicurezza per il trasferimento;
- dove possibile, i limiti di tempo entro cui si devono cancellare le diverse categorie di dati;
- dove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Data Protection Officer (DPO)

Art. 37: stabilisci se l'azienda ha bisogno di un DPO. Per esempio quando:
- l'elaborazione è gestita da un ente pubblico, eccetto tribunali;
- le attività consistono nel monitorare le operazioni che richiedono monitoraggio regolare e sistematico di soggetti di dati su larga scala;
- le attività principali consistono nell'elaborare categorie speciali di dati personali e di dati relativi a eventuali carichi pendenti.
Se alla società non viene richiesto di acquisire un DPO, si può incaricare un DPO volontario.
I dati per contattare il DPO devono essere resi noti e inviati all'autorità competente.

Data Retention

Art. 5: I dati possono solo essere conservati per un periodo di tempo necessario allo scopo per cui gli stessi sono stati raccolti. La società deve determinare per quanto tempo tenerli prima di cancellarli o renderli anonimi.

Privacy Impact Assessment (PIA)

Art. 35: la società deve fare un PIA quando implementa nuove tecnologie che possono portare a un rischio dal punto di vista dei diritti e delle libertà degli individui.
Questo è un esercizio per determinare che impatto ha la tecnologia e l'elaborazione sugli individui e per aderire a tutti gli aspetti del GDPR.

Employee training

Art. 5: I dipendenti che gestiscono dati personali di altri dipendenti o di clienti devono ricevere un training che fornisca loro gli strumenti per la gestione nei termini del GDPR. La società deve tenere uno storico di tutti i training ed effettuare anche dei corsi di aggiornamento periodici.

Policies and procedures

Art. 5: per assicurarsi che la società abbia implementato i 6 principi di data protection, si deve implementare una policy di data protection apposita.
Non esiste un format stabilito e l'elenco esatto di policy competenti dipende dal tipo di dati elaborato.