Checklist di autovalutazione di conformità al GDPR

Ecco i passaggi principali da noi individuati per controllare l'effettiva conformità alla normativa GDPR della propria azienda:

- ☐ **Identificare tutti i Trattamenti di dati personali** esistenti in azienda.
- ☐ **Identificare Titolare e Responsabile del trattamento** dei dati personali (per ogni trattamento definire Titolare e Responsabile).
- ☐ **Istituire il Registro dei Trattamenti** contenente tutti i Trattamenti di dati dell'azienda (in realtà avremo un Registro del Responsabile dei trattamenti ed un Registro del Titolare, che insieme riportano tutte le informazioni necessarie sui diversi trattamenti).
- ☐ **Aggiornare Privacy Policy** con una informativa completa, corretta, semplice e di facile consultazione.
- ☐ **Adeguare la raccolta dei consensi al trattamento** per ogni singola raccolta dati personali esistente (intervenire su testo dell'informativa e meccanismi di raccolta del consenso).
- ☐ **Verificare per ogni trattamento e dato pre-esistente** se il consenso al trattamento acquisito (se è stato acquisito) all'atto della registrazione dei dati è sufficiente, oppure se è necessario **procedere nuovamente all'acquisizione del consenso** rispetto al trattamento previsto.
- ☐ **Far valere i diritti dell'Interessato** ovvero rendere disponibili adeguati servizi che garantiscano di ottenere: oblio, accesso/modifica, portabilità e limitazione del trattamento; tali funzioni dovranno essere accessibili in modo semplice, veloce ed intuitivo … almeno quanto lo è stato la fase di raccolta. Nel caso sia necessario, le risposte dovute agli Interessati dovranno essere concise, trasparenti ed utilizzare un linguaggio semplice e di facile comprensione.
- ☐ **Proteggere i Dati personali** degli Interessati osservando le buone pratiche di qualità e sicurezza dei sistemi e delle procedure di trattamento dei Dati personali indipendentemente dalla loro forma (numerico/testuale/immagine/audio/video, logica/fisica) e dal supporto di memorizzazione (cartaceo, magnetico, elettronico, cloud…).
- ☐ **Compiere il Risk Assessment per ogni trattamento identificato** al fine di rilevare il livello di rischio per lo stesso.
- ☐ **Eseguire tutte le azioni necessarie alla Mitigazione del rischio** per tutti i trattamenti che hanno rivelato un livello di Rischio elevato (High Risk).
- ☐ **Progettare ed erogare un Piano formativo** a tutti gli Stakeholder per assicurare una corretta conoscenza del Regolamento al fine di consentire a ciascuno di gestire e compiere le proprie attività lavorative in modo informato.
- ☐ **Predisporre il Piano di azione da attivare in caso di Data Breach** ovvero quando si verificasse una violazione di dati personali.

Creato da Next Software Modena

File scaricato da www.nextsoftware.it – Per informazioni tel: **059 375515** mail: **info@nextsoftware.it**