

QUESTIONARIO PRE-ASSESSMENT

Trattamento dei Dati

Valutazioni introduttive alla tematica GDPR

Il presente questionario è da considerarsi come un pre-assessment, la cui compilazione non richiede una conoscenza approfondita del GDPR (General Data Protection Regulation) nuovo regolamento europeo UE 2016/679 in materia privacy.

Obiettivo del presente documento è fornire una prima e indicativa analisi dello stato di conformità dell'organizzazione rispetto alla materia privacy e determinare il livello di controllo che la stessa ha sulle informazioni gestite e sulla legittimità delle loro elaborazioni.

Parte A – Informazioni sul cliente:

Denominazione

Settore Merceologico

Organigramma, fornire un semplice elenco delle figure con potere decisionale presenti nella struttura (es. Rossi Mario – CEO/AD)

Nome, Cognome – Ruolo

Nome, Cognome – Ruolo

Nome, Cognome – Ruolo

Nome, Cognome – Ruolo

Nome, Cognome – Ruolo

Nome, Cognome – Ruolo

Numero dipendenti

Elenco delle sedi diverse dalla sede principale, sia su territorio italiano ovvero estero. (indicare la località e lo stato se diverso dall'Italia)

| |
|--|
| |
|--|

Fatturato

Sito WEB

Parte B – Trattamento dei dati

L'azienda effettua vendita diretta a persone fisiche

SI NO

L'azienda ha creato sistemi di fidelizzazione del cliente (Tessere, APP, ecc...).

SI NO

Avviene uno scambio di dati con terzi soggetti (es. Medico Legale, Studio consulenza buste paga, ecc...)

SI NO

Se si, Elencare tali soggetti e le finalità dello scambio dei dati (es: Dott. Rossi – Medico del lavoro)

Denominazione - Finalità

| |
|--|
| |
|--|

L'azienda redigeva il DPS quando questo era obbligatorio

SI NO

Nell'azienda si è provveduto a scrivere una informativa sulla protezione dei dati

SI NO

Se si, è stata messa a disposizione dei clienti, partners e dipendenti

SI NO

E' già presente in azienda un titolare della Protezione dei Dati

SI NO

E' già presente in azienda un responsabile della Protezione dei Dati

SI NO

Avete un registro dei trattamenti, dove vengono appuntate tutte le azioni intraprese nel rispetto della privacy e del trattamento dei dati personali.

SI NO

Avete offerto ai vostri dipendenti formazione o campagne di sensibilizzazione in tema di protezione dei dati personali

SI NO

Durante la raccolta dei dati personali dei vostri clienti e dipendenti viene usato un processo di consenso esplicito e specifico

SI NO

Siete in grado di dare alle persone l'accesso a tutti i loro dati personali

SI NO

Siete in grado di aggiornare o cancellare i dati personali dei vostri clienti

SI NO

Esiste una procedura per la conservazione dei dati personali

SI NO

Siete in grado di soddisfare il diritto dei vostri clienti in merito alla portabilità dei loro dati, e cioè di trasferire a terze parti tutti i loro dati

SI NO

Esiste un sistema per gestire l'accesso sicuro agli archivi contenenti dati personali

SI NO

Nel caso di un incidente di sicurezza che coinvolga dati personali, è già presente in azienda un processo di gestione dell'incidente e della sua notifica

SI NO

Quali misure adottate per quanto riguarda i vostri fornitori e/o soggetti terzi con cui scambiate dati? Il contratto che disciplina la fornitura garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza

SI NO

Esiste una procedura per il trasferimento di dati al di fuori dell'Unione Europea

SI NO

Sono presenti in azienda un inventario dei sistemi informativi e delle applicazioni utilizzati per la gestione dei dati?

SI NO

In azienda esistono delle misure minime di sicurezza per l'accesso alla rete aziendale e ai sistemi informatici

SI NO

Esistono e vengono monitorati i sistemi di backup in azienda

SI NO

Parte C – Valutazione del livello di rischio

Esiste in Azienda o anche in uno solo degli stabilimenti aziendali un sistema di videosorveglianza.

- NC
- SI Solo Interna agli uffici
- SI Solo Esterna agli uffici
- SI In entrambi gli ambienti

La raccolta dei dati prevede una valutazione e/o scoring, compresa la profilazione

- SI NO

La raccolta dei dati prevede decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);

- SI NO

Si gestiscono dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche)

- SI NO

Si effettuano trattamenti di dati personali su larga scala (livello nazionale, ecc..);

- SI NO

Si effettua una combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);

- SI NO

Si gestiscono dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);

- SI NO

Parte D – Dati sulla compilazione del questionario.

Luogo e data

Nominativo di chi ha compilato il questionario

Funzione Aziendale