SECURITY LAB
sicurezza on line

ALLEGATO “A” GDPR

L’utilizzo di questa soluzione è necessaria in quanto la documentazione relativa al GDPR deve essere presentata al momento della richiesta e deve rispondere esattamente allo stato dell’azienda in quel preciso istante. Da questo si deduce che tutti i dati richiesti dalla normativa devono essere aggiornati ad ogni variazione.

All’interno dell’azienda devono essere presenti le seguenti cariche:

DATA CONTROLLER : L’azienda stessa

DATAPROCESSOR : Responsabile della sicurezza, di solito il titolare o un dipendente incaricato.

DATA PROCESSOR ESTERNI: Tutti coloro che per qualsiasi motivo posso accedere ai dati dell’azienda (commercialista, Consulente del lavoro, medico, ecc)

AMMINISTRATORE DI SISTEMA: La persona responsabile della rete, si occupa di controllare l’andata a buon fine dei Backup, controlla che il software utilizzato all’interno del sistema informatico venga aggiornato alle ultime release inerenti la sicurezza, sovraintende alla distruzione dei supporti magnetici in caso di cessione o rottamazione degli stessi. IL GARANTE CONSIGLIA UNA PERSONA NON DIPENDENTE PER EVITARE CONFLITTI DI INTERESSE.

INCARICATI: Tutti i soggetti che all’interno dell’azienda accedono ai dati personali. Questi signori devono frequentare un corso di formazione come previsto dalla normativa in vigore.

Se Installate delle telecamere (interne/esterne).

RESPONSABILE VIDEO SORVEGLIANZA: di Solito il DATA PROCESSOR

INCARICATO VIDEO SORVEGLIANZA: L’unica persona a cui ci si può rivolgere per avere informazioni sulle registrazioni e l’unico che può accedervi.

Quindi il GDPR si occupa delle seguenti categorie:

SICUREZZA: (vedi misure minime)

- Antivirus
- Firewall
- Crittografia
- Dispositivi USB
- Sistemi di backup

- Cancellazione Sicura
- Protezione
    1. Personale
    2. Protezione informatica
    3. Protezione ambientale
    4. Protezione apparecchiature

GDPR

- Sedi
- Uffici
- Sistemi di Elaborazione
- Data Handler (Incaricati)
- Data Processor esterni
- Banche dati

TRATTAMENTI (programmi software che accedono ai dati)

- Interni
- Presso DPE (data processor esterni)

PRIVACY ASSESSMENT

- Risk Assessment (per ogni Trattamento)
    1. Valutazione dei Rischi
        - Accessi esterni non autorizzati
        - Allagamento
        - Alterazione dolosa o colposa dati avvenuta internamente
        - Attacco ransomware
        - Azione virus informatici o di codici malefici
        - Carenza di consapevolezza, disattenzione o incuria

- Comunicazione illegale dei dati e dei documenti
- Copia abusiva
- Degrado dei supporti e delle apparecchiature
- Corto circuito elettrico
- Distruzione di apparecchiature o di supporti
- Fenomeni naturali
- Furto apparecchiature
- Incendio
- Ingressi non autorizzati a locali/aree ad accesso ristretto
- Malfunzionamento hardware e software
- Mancanza di continuità di alimentazione elettrica
- Mancata manutenzione del sistema informativo
- Perdita credenziali
- Polvere, corrosione o gelo
- Possibile rottura dell'hard disk o altri componenti hardware/software
- Accessi tramite dispositivi mobili non autorizzati
- Errato utilizzo doloso o colposo del software
- Mancata distruzione di supporti raggiunta la finalità

- Audit e future mitigazioni del rischio
- Policy di sicurezza
- Descrizione Privacy Impact Assessement

REGISTRO DEGLI INTERVENTI (a cura dell'amministratore di sistema)

Per quanto sopra descritto una "Compliance" al GDPR senza un supporto informatico dedicato diventa estremamente onerosa per il tempo da dedicarle i rischi di errore e le conseguenti mancanze di conformità.