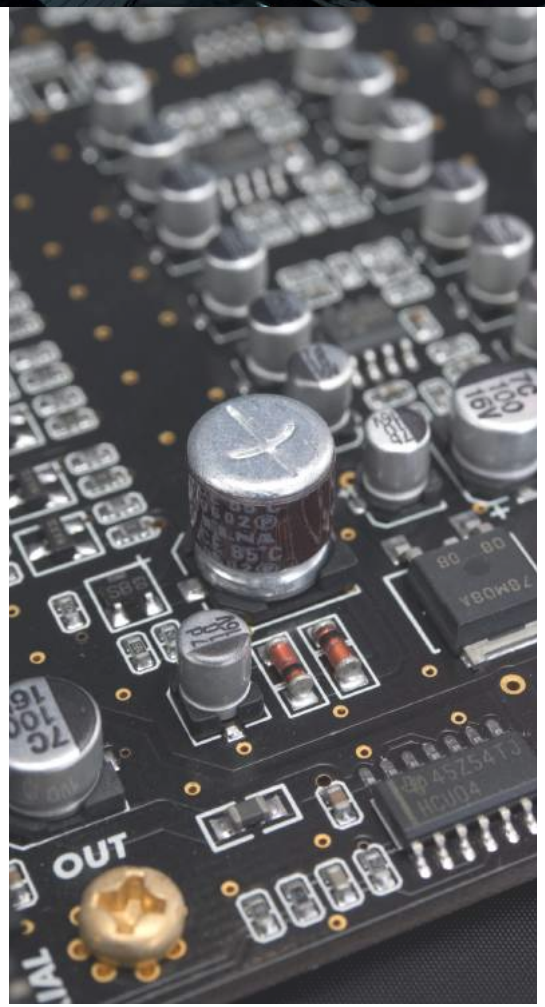
GDPR: COSA FARE PER METTERSI IN REGOLA

NUOVO REGOLAMENTO SULLA PRIVACY

Il 25 maggio 2018 è il termine ultimo per mettersi in regola con il GDPR, General Data Protection Regulation, ovvero il Regolamento generale sulla protezione dei dati nell'unione Europea. Tutte le aziende e le pubbliche amministrazioni devono adeguarsi a pena di potenziali multe salatissime: fino a 20 milioni di euro.



DI COSA SI TRATTA

Il GDPR chiede alle aziende di controllare dove sono i dati personali e garantire che siano protetti. Non devono essere protetti solo i dati ma anche i dispositivi e la rete, così come tutti i dipendenti dovranno essere istruiti per un utilizzo sicuro del sistema.

COSA PRESCRIVE

Il titolare del trattamento deve obbligatoriamente redigere il Registro dei Trattamenti e tenerlo aggiornato con le informazioni riguardo:
Operatori interni e/o esterni con accesso ai dati
Finalità dei trattamenti dei dati
Categorie e tipologie di dati
Modalità e tempi di cancellazione dei dati
Misure tecniche ed organizzative di protezione adottate
Il Data Breach - È previsto l'obbligo di dare comunicazione all'autorità di controllo competente (e in alcuni casi ai diretti interessati), di eventuali attacchi informatici con violazioni dei dati personali entro il tempo massimo di 72h.

AUDIT

Il primo passo è fare una valutazione corretta e precisa della situazione odierna all'interno dell'azienda.

CONTROLLO ACCESSI

Un altro passo fondamentale è sapere chi ha accesso ai dati dell'azienda

ACCOUNTABILITY

Occorre poter dimostrare l'adeguatezza dei propri processi di compliance. Sarà quindi necessario produrre una documentazione descrittiva e accurata di tutti i processi di trattamento con dettaglio di tipo di dati e finalità. Bisognerà dimostrare quali strumenti vengono usati per anonimizzare, pseudonimizzare e crittografare tutti i dati

SICUREZZA INFORMATICA

Implementare una sicurezza stratificata molto seria dal punto di vista informatico è il passo finale. Servirà per rispondere ad eventuali violazioni. Per questo motivo la prevenzione è alla base di tutto. Una regolare scansione e update dei software del sistema è d'obbligo. Non basteranno update regolari dei sistemi di sicurezza e dei software, fondamentali per il mantenimento in sicurezza dell'infrastruttura, ma saranno indispensabili tradizionali difese come l'antivirus e l'UTM del Firewall . Inoltre l'utilizzo di software di vulnerability scan, investendo quindi in nuovi dispositivi più sicuri e apportando i giusti sistemi di sicurezza, eviterà possibili potenziali violazioni. Formare i dipendenti sui rischi degli attacchi informatici è altrettanto importante: la maggior parte degli attacchi informatici sono dovuti a errori da parte dei dipendenti.

Le nostre soluzioni forniscono un aiuto valido per mantenersi in regola con il GDPR: Panda e Data Protect

CHECKLIST AUTOVALUTAZIONE

La check list dinamica consiste in domande semplici e di facile comprensione, su come sono gestiti aspetti della Farmacia che hanno impatto sulla Data Protection; il percorso di autovalutazione viene creato dinamicamente in base al tipo di risposte e vengono segnalati i punti di attenzione dove sono suggerite degli interventi. CGM Data-Protect ti guiderà in questo

STAMPA DOCUMENTI E DELEGHE

Una volta concluso il questionario, il sistema propone i moduli di delega o autorizzazione al trattamento pronti per la stampa. Prima di accedere alle stampe vere e proprie, la funzione analizza tutte le risposte inserite e mostra un elenco di errori e/o incongruenze per permettere le eventuali correzioni da apportare (Gap-Analisys). Con CGM Data-Protect tutto questo sarà immediato.

DATA BREACH

In caso di attacchi informatici, perdita dati, ricette etc è previsto l'obbligo di dare comunicazione all'autorità di controllo entro 72 ore: con Panda Data Control sarà facile capire come e perchè è successo.

PROTEZIONE DATI

Panda Adaptive Defense consente di adeguarsi alla normativa GDPR in modo semplice e completo: Prevenzione degli Incidenti, Protezione dei Dati Personali trattati su tutti i dispositivi, Riduzione del Rischio, Meccanismi di Controllo e notifica dei Dati per il DPO, Obbligo di Notifica GDPR.