Processo di Governance della Privacy

Introduzione

La tematica della Compliance alle normative in tema di Privacy e del trattamento dei dati individuali ha un peso sempre crescente nella definizione delle strategie aziendali le quali, nel corso del tempo, hanno approcciato a tali tematiche implementando processi e sistemi al fine di adempiere alle prescrizioni declinate dalle normative di riferimento.

In tale contesto, nell'ottica di un'implementazione ed evoluzione continua del processo di Data Protection necessario per le imprese e di compliance rispetto al nuovo regolamento, sarà necessario avviare un processo di analisi e definizione di un modello che le permetta di valutare l'attuale status di conformità dell'organizzazione, di eseguire un assessment e di misurare lo stato di esposizione al rischio.

Al fine da identificare, definire, implementare e gestire nel tempo le evoluzioni organizzative, processive e tecnologiche necessarie alle aziende, in linea con le strategie e le necessità del business, in riferimento alla nuova normativa europea in ambito Privacy, si rende necessario dotarsi di servizi per la realizzazione di una piattaforma di supporto alla Governance della privacy in linea con la normativa "GDPR" in grado di assicurare un adeguato presidio alla gestione del:

- Registro Dei Trattamenti
- Registro Dei Data Breach

La realizzazione di una piattaforma di supporto alla Governance della privacy in grado di assicurare la gestione delle funzionalità dei Trattamenti" e dei consensi correlati; "Registro Dei Data Breach" in linea con la normativa "GDPR",

consentendo agli attori coinvolti di svolgere le azioni previste sui dati di competenza.

In particolare, la componente “Registro dei Trattamenti” dovrà consentire la gestione di tutti i trattamenti, il legame con l’organizzazione aziendale, con le banche dati e gli strumenti applicativi nonché tutte le informazioni di dominio che contribuiscono alla caratterizzazione dei singoli trattamenti (finalità, base giuridica, tipologia del consenso/contratto, tipologia dati trattati, categorie di interessati e legame con le misure di sicurezza identificate a valle dell’analisi dei rischi e/o della Data Protection Impact Assessment – DPIA).

La componente “Registro Dei Data Breach” dovrà consentire la gestione di tutte le violazioni di dati personali verificatesi all’interno del contesto aziendale riportando: la tipologia (tipo e natura) del dato violato – dettagli relativi alla violazione (disponibilità dati violati, misure di sicurezza) – dettagli sull’incident (data ora, posizionamento dei dati, eventuale causa della violazione, numerosità persone impattate dalla violazione, Remediation Plan) – il livello di gravità della violazione dei dati personali.

Inoltre, dovranno essere gestite su base storica le informazioni che riguardano le comunicazioni con gli interessati dalla violazione e con le autorità di controllo includendo la gestione dei documenti inviati e ricevuti.

Impatti del GDPR

La conformita` al GDPR richiede un impegno considerevole, mettere in campo una serie di azioni e tecnologie specifiche finalizzate a tutelare i dati trattati dall’azienda al fine di:

- proteggere i dati durante la memorizzazione e il transito attraverso la rete;

- garantire la consapevolezza dei rischi tramite un’analisi dei log costante e monitoraggio di chi sta facendo cosa sui vari filesystem di rete;
- consentire azioni preventive, correttive in realtime contro le vulnerabilita`o incident rilevati che possano rappresentare un pericolo per i dati;
- fornire strumenti di valutazione per l’efficacia delle policy di sicurezza;
- implementare meccanismi di recupero dei dati che consentano di ripristinare l’accesso ai dati ed ai sistemi quando un incidente ne pregiudica la disponibilità;
- aumentare la consapevolezza degli utenti relativamente alle minacce in termini di sicurezza informatica che si trovano ad affrontare quotidianamente tramite una formazione/informazione, anche solo basilare ma costante;

Il GDPR declina una serie di obblighi e benefici per quanto riguarda le misure tecniche e organizzative tecniche poste in essere per garantire la sicurezza dei dati trattati ad esempio:

- Tali obblighi devono essere implementati dal Titolare e dal Responsabile del trattamento dei dati personali (art.24 GDPR);
- I principi di privacy by design e privacy by default sono inclusi in appropriate misure tecniche e organizzative (art.25 GDPR);
- Danno efficacia al diritto alla portabilità dei dati personali (articolo 20 GDPR) e al diritto all’oblio (art.17 GDPR);
- Dimostrano che il Titolare e il Responsabile del trattamento hanno garantito un livello adeguato di protezione dei dati personali;

Misure Tecniche

Le misure tecniche includono i controlli relativi alla pseudo anonimizzazione, (procedimento che comporta la possibile attribuzione di determinate qualità a un interessato specifico solo attraverso l'utilizzo di informazioni aggiuntive, tipicamente l'impiego di chiavi crittografiche, sistemi di autenticazione, politiche per le password, ecc. e deve essere completato per quanto riguarda le Applicazioni IT utilizzate per l'elaborazione dei dati personali. Nella compilazione delle misure tecniche la funzione IT dovra`fare riferimento alle applicazioni IT utilizzate per i trattamenti di dati personali.

Misure Organizzative

Le misure organizzative includono i controlli relativi alle istruzioni operative fornite ai responsabili del trattamento dei dati e agli incaricati, controlli critici che ogni azienda dovrebbe implementare per mettere in sicurezza la propria infrastruttura.

Di seguito uno schema funzionale della Piattaforma di Governance.



Figura 1 – Architettura Funzionale Registro Trattamenti.

Considerazioni

Partendo dal presupposto che il grado di sicurezza di un'azienda sia strettamente legato ai processi organizzativi, dove procedure e sensibilizzazione verso i dipendenti sono gli elementi "core", le soluzioni tecnologiche finalizzate alla risoluzione di specifiche problematiche dovranno essere individuate analizzando l'ambito secondo reali esigenze e soprattutto garantire un'integrazione completa della

preesistente infrastruttura tecnologica al fine da massimizzarne benefici e costi.

La sicurezza è guidata dai processi di business, i quali sono concepiti come attività nelle quali operano: persone, sistemi, infrastrutture, in genere autonomi e interdipendenti, interni ed anche esterni.

La garanzia della corretta operatività e interazione tra i processi e quindi del flusso delle informazioni è data dalla gestione della sicurezza, la quale provvede non solo alla prevenzione di: errori umani e/o procedure, infiltrazioni e attacchi, ma, soprattutto, è arbitro della corretta interazione tra i processi e scambio delle informazioni.

Una soluzione per il monitoraggio della Privacy implica un approccio condiviso, è l'impiego di strumenti omogenei che siano in grado di garantire un framework completo che inizi soprattutto dall'analisi del processo di business fino ad arrivare al processo tecnologico come ad esempio nell'ambito della protezione dei dati attraverso il processo di cifratura delle informazioni classificate "sensibili" con impiego di soluzioni preconfezionate o sviluppate ad hoc che tengano in considerazione tutto il ciclo di vita del dato (residente o in transito).

Articolo a cura di **Cristian Rei**

https://www.ictsecuritymagazine.com/articoli/processo-di-governance-della-privacy/