IL PERCORSO DI ADEGUAMENTO AL GDPR

Introduzione

Benvenute e benvenuti!

In questa lezione, approfondiremo le ultime novità in materia di protezione dei dati personali.

Nel dettaglio, vedremo:

- il percorso di adeguamento al GDPR
- la sicurezza dei dati personali
- il rapporto con i Responsabili del trattamento

Bene, non ci resta che cominciare!

Il percorso di adeguamento

Come per le Società private, anche per la PA l'adeguamento al GDPR – oltre a costituire un obbligo di legge – può rappresentare un'opportunità per ripensare l'organizzazione, rivederne i processi o introdurre nuovi strumenti.

Per sfruttare tali opportunità, senza naturalmente trascurare i principali adempimenti richiesti, è necessario definire un percorso di adeguamento ben strutturato assegnando in modo chiaro ruoli e responsabilità.

Il processo di adeguamento al GDPR prevede *4 fasi*:

La PRIMA fase, il CHECK UP, consiste prima di tutto *nell'analisi approfondita della normativa applicabile* così da valutare attentamente gli impatti *sulle attività del titolare del trattamento*.

Pensate ad esempio alle modifiche organizzative richieste dall'introduzione di un nuovo ruolo o di una nuova struttura.

Questa fase, inoltre, è funzionale all'identificazione delle scoperture rispetto ai requisiti individuati e soprattutto alla definizione di *azioni* concrete che dovremo intraprendere per minimizzare i rischi di non conformità.

La SECONDA fase, il DISEGNO, consiste nella progettazione di un *Sistema per la Protezione dei Dati Personali,* cioè l'insieme delle misure tecniche e organizzative, volte ad assicurare il rispetto dei requisiti normativi.

Tale Sistema prevede:

- l'identificazione e attribuzione di Ruoli e Responsabilità tra cui la nomina del Data Protection Officer, ove richiesto, e dei soggetti autorizzati al trattamento;

- la revisione dei processi e dei flussi di dati, nonché l'adeguamento della normativa interna tra cui policy, procedure e strumenti a supporto;
- l'identificazione degli asset, logici e fisici, che trattano dati personali e la definizione o adeguamento delle relative misure di sicurezza;
- la definizione delle verifiche da effettuare al fine di garantire l'esistenza, l'adeguatezza e l'effettiva applicazione della normativa interna.

In questa fase sarà fondamentale tenere traccia delle azioni intraprese così da poterne dare evidenza in futuro, in ottica di *accountability*.

La TERZA fase, l'IMPLEMENTAZIONE, consiste nella gestione degli adempimenti nel rispetto della normativa interna, tra cui ad esempio:

- manutenere il Registro delle attività di trattamento;
- valutare le nuove iniziative in ottica Privacy by Design;
- informare gli interessati e raccoglierne i Consensi;
- aggiornare le disposizioni interne in funzione delle novità introdotte.

Il requisito fondamentale per assicurare l'effettiva applicazione della normativa interna è la progettazione ed erogazione di *attività di sensibilizzazione e formazione* del personale, come per esempio la progettazione di percorsi modulari di e-Learning.

L'ULTIMA fase del percorso di adeguamento è il CONTROLLO.

Questa fase prevede la *pianificazione e la conduzione di verifiche periodiche* volte ad assicurare l'effettiva applicazione della normativa interna.

La *pianificazione ed esecuzione di verifiche* è un elemento particolarmente importante per due motivi:

- da un lato, permette di identificare eventuali non conformità, o aree di miglioramento;
- dall'altro, assicura l'evoluzione del Sistema di gestione dei dati personali nel tempo, minimizzando così il rischio che questo diventi obsoleto.

Come qualsiasi processo di controllo, anche in questo caso, sarà utile attivare un sistema di *reporting* non solo per la raccolta e formalizzazione delle evidenze, ma anche per la condivisione dei risultati con i principali *stakeholder*.

Ad ogni modo sarà fondamentale mantenere aggiornato il modello nel tempo affinché rimanga coerente con le prassi e i flussi di dati, e allo stesso tempo possa recepire eventuali aggiornamenti normativi.

La sicurezza dei dati personali

Un aspetto fondamentale del processo di implementazione del Sistema a protezione dei dati personali è costituito dalla scelta delle misure di sicurezza definite "adeguate" dal GDPR. Ma quali misure di sicurezza è tenuta a adottare un'organizzazione per assicurare la protezione dei dati personali?

Il GDPR ha introdotto alcune novità importanti: spetta al Titolare il compito di individuare misure tecniche ed organizzative adeguate al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione delle misure, nonché della natura, ambito, contesto e finalità dell'attività di trattamento.

Il Regolamento indica alcune misure a titolo esemplificativo, tra i quali la cifratura e la pseudonimizzazione dei dati, lasciando però al Titolare la scelta di quali adottare in concreto in una logica risk-based.

A cosa servono tali misure e di quali rischi stiamo parlando?

Parliamo di rischi non per l'organizzazione, ma per i diritti e le libertà delle persone fisiche, che potrebbero scaturire dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o malevolo, ai dati personali trattati. Da eventuali violazioni di dati personali" (più comunemente conosciute come data breach) potrebbero derivare danni per gli interessati come ad esempio furto d'identità, perdite economico-finanziarie o danni reputazionali della persona.

Le misure servono dunque sia per prevenire data breach, ove possibile, sia, nel caso in cui lo stesso si verifichi, per reagire tempestivamente.

L'analisi dei rischi costituisce un'attività chiave durante tutto il ciclo di vita dei dati. Quando si progetta un nuovo trattamento, ci si vuole accertare che vengano attuate fin da subito tutte le garanzie necessarie, in linea con il principio di Data Protection by Design e by Default. È inoltre uno strumento indispensabile, qualora il trattamento risulti ad alto rischio, nell'ambito dello svolgimento della Valutazione di Impatto sul Trattamento.
L'analisi dei rischi deve essere svolta anche sui trattamenti già effettivi per rivalutare periodicamente l'efficacia delle misure ed individuare eventuali interventi migliorativi a fronte di cambiamenti nello scenario di rischio (es: nuovi attacchi), variazioni nell'attività di trattamento o in seguito a una violazione dei dati personali.

Per svolgere correttamente l'analisi dei rischi può essere utile fare riferimento a metodologie e criteri forniti da soggetti che possano rappresentare in maniera autorevole la prospettiva degli interessati, come gli strumenti e le linee guida messe a disposizione dalle Autorità di controllo europee e dall'ENISA, l'Agenzia europea per la sicurezza informatica.

Al termine dell'analisi dei rischi, il Titolare valuterà l'adeguatezza delle misure ipotizzate o in essere e, in caso contrario, definirà un piano di trattamento contenente ulteriori misure volte a mitigare il rischio. Difatti, le misure di sicurezza, anche se giudicate adeguate, non possono azzerare il rischio di una violazione di dati personali.

Il GDPR adotta un approccio moderno alla tematica, prevedendo sia un'adeguata sensibilizzazione e formazione del personale sui comportamenti da tenere per prevenire Data Breach (nonché sulle sue responsabilità di fronte a una violazione), sia, qualora una violazione di dati personali dovesse effettivamente verificarsi, un'adeguata strategia di gestione della stessa, comprensiva di strumenti e procedure che permettano di rilevarla tempestivamente e rispondervi in maniera appropriata, così da mitigarne l'impatto sugli interessati.

Non dobbiamo infine dimenticare l'importanza di essere in grado di dimostrare di aver ottemperato al GDPR, secondo il principio dell'"accountability", documentando l'incidente e le sue modalità di gestione: dalle circostanze in cui è stato rilevato, alle azioni di risposta messe in atto per limitarne le conseguenze fino alle misure previste per ridurre i rischi per gli interessati e far sì che l'incidente non si ripeta.

In cosa consiste esattamente un *data breach*?

Un data breach non è altro che una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Anche la temporanea mancanza di accesso a determinati dati può quindi comportare un data breach. Capite che, in un contesto ospedaliero, non poter accedere ai dati relativi alla salute può costituire un vero e proprio pericolo per i pazienti.

Solitamente si collega il data breach all'ambiente digitale: l'immaginario collettivo rimanda certamente ad episodi di attacchi informatici o ad hacker che entrano nei sistemi dell'azienda attraverso mail di phishing per bloccare i sistemi e chiedere un riscatto. Tuttavia, la violazione di dati personali non si limita solo a tali situazioni, ben potendo esistere anche nel mondo "off-line": lo smarrimento di fascicoli, di documenti, di cartelle cliniche o referti cartacei sono solo alcuni esempi di come un data breach possa avvenire anche al di fuori di internet e dell'ambiente digitale.

Cosa fare in caso avvenga un data breach?

Oltre ovviamente alle operazioni necessarie a limitare i danni e ripristinare l'operatività, il GDPR prevede che il Titolare notifichi l'incidente all'autorità di controllo entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Analogamente dovrà provvedere anche ad effettuare una comunicazione agli interessati allorché la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Il rapporto con i Responsabili del trattamento

Uno degli aspetti chiave utili ad assicurare che il trattamento di dati personali mantenga standard adeguati e sia conforme al GDPR è il rapporto tra il Titolare e i suoi Responsabili.
Il Titolare decide perché e come trattare i dati personali. Il Responsabile è colui che li tratta dal punto di vista operativo secondo quanto indicato dal Titolare e per conto di questo.

Molto spesso gli aspetti chiave della sicurezza non sono gestiti direttamente dai Titolari, ma sono in mano ai Responsabili, ai quali viene affidata l'esecuzione di ampie e rilevanti porzioni del servizio erogato ai clienti.

Quindi è necessario che il Titolare scelga con attenzione i propri responsabili del trattamento tra quelli che presentino garanzie sufficienti sulla messa in atto di misure tecniche e organizzative adeguate.

L'articolo 28 del GDPR impone di sottoscrivere con il Responsabile un accordo che lo vincoli alle istruzioni impartite dal Titolare, definendo in maniera chiara, tra i molti aspetti, la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento, le modalità per l'eventuale ingaggio di sub-responsabili ed il rilascio di specifiche garanzie rilasciate dal fornitore.

L’adozione di accordi contrattuali è fondamentale, ma non è sufficiente. Al Titolare, infatti è attribuita la responsabilità generale del trattamento ed è tenuto, pertanto, ad effettuare controlli sull’attività dei Responsabili.

Dunque, ogni qual volta il Titolare si confronti con un potenziale nuovo fornitore è opportuno che vengano rispettati i seguenti passaggi.

Innanzitutto, sarebbe opportuno che il Titolare del trattamento svolgesse delle verifiche preventive sul fornitore, selezionando così solamente soggetti che, ad un prima verifica, siano in grado di garantire un adeguato livello di conformità al GDPR. Ciò potrebbe avvenire, ad esempio, sottoponendo ai medesimi un questionario utile a vagliare il livello di conformità alla normativa, nonché le capacità o le caratteristiche che il Titolare consideri indispensabili. Nel caso concreto, potrebbe trattarsi anche della richiesta di particolari tipi di certificazione, come la ISO 27001 relativa alla sicurezza informatica.

Inoltre, è obbligatorio sottoscrivere con il fornitore uno specifico accordo sul trattamento dei dati, oppure l’inserimento di una specifica clausola contrattuale, che contengano tutti i requisiti ai sensi dell’art. 28 del GDPR.

Questo tipo di patto deve definire, in maniera chiara:

- la durata, la natura e la finalità del trattamento,
- il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del titolare del Trattamento
- le modalità per l’eventuale ingaggio di sub-responsabili
- il rilascio di specifiche garanzie rilasciate dal fornitore.

Il terzo ed ultimo passaggio consiste nella pianificazione e implementazione di attività di audit sui fornitori, con redazione di relativo verbale contenente, eventualmente, un piano degli interventi correttivi. Difatti, l’omissione di verifiche sull’operato del Fornitore potrebbe comportare la responsabilità del Titolare per *culpa in vigilando*.

Effettuando le suddette attività, il Titolare sarà in grado di dimostrare la propria conformità al GDPR relativamente al rapporto con i propri fornitori.

Conclusioni

Bene, siamo giunti alla fine di questa videolezione.

Ti ricordo che abbiamo approfondito:

- il percorso di adeguamento al GDPR
- la sicurezza dei dati personali
- il rapporto con i responsabili del trattamento

Grazie per l’attenzione!