

Piano di Formazione Nazionale

29 MAGGIO 2019

11.00 – 13.00

“Privacy: il registro delle attività di trattamento”

Il giorno 29 maggio 2019 si è tenuto il 5° webinar organizzato da ProMIS nell’ambito del Piano di Formazione Nazionale per il 2019, il quale ha visto la partecipazione di una quarantina di persone connesse.

La lezione è stata tenuta dall’ **Ing. Alberto Lombardi**, responsabile protezione dati e responsabile Ingegneria clinica per l’ASL di Benevento, che ha presentato **“Il sistema di gestione della Protezione Dati: dal Registro delle attività di trattamento alla gestione dei Data Breach”**. Il GDPR sulla privacy, all’art 32, prevede un nuovo approccio di gestione del rischio stabilendo che *“Il titolare deve adottare opportune misure e per dimostrare la conformità per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio”*. Tale nuovo approccio prevede:

- ✓ la conoscenza dei processi aziendali, dei flussi informativi e relativi trattamenti;
- ✓ l’individuazione, valutazione e gestione dei rischi;
- ✓ l’adozione delle adeguate misure di sicurezza organizzative e tecniche.

Il sistema di gestione e organizzazione del lavoro vede la necessità di una definizione di una strategia aziendale condivisa di trattamento dei dati personali; sviluppo di un sistema di gestione della protezione dei dati strutturato ed efficace; individuazione di un programma di attuazione condiviso in materia di protezione dei dati personali, suddividendo il processo in tre step principali:

1. Assessment e mappatura dei trattamenti, dell’organizzazione e delle procedure esistenti;
2. Design e definizione di un nuovo modello tecnico-organizzativo, con ridefinizione dei processi e delle metodologie di trattamento;
3. Management e controllo del sistema.

All’art.30 del GDPR si prevede altresì, tra gli adempimenti principali del titolare e del responsabile del trattamento, la tenuta del **Registro delle Attività di Trattamento**, che costituisce uno dei principali elementi di accountability del titolare, in quanto strumento idoneo a fornire un quadro aggiornato dei trattamenti in essere all’interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e dunque preliminare rispetto a tali attività. Deve essere in forma scritta (anche elettronica) ed esibito su richiesta al Garante. Il Garante ne raccomanda la redazione a tutti i titolari e responsabili del trattamento, in quanto strumento che, fornendo piena contezza del tipo di trattamenti svolti, contribuisce ad attuare, con modalità semplici e accessibili a tutti, il principio di accountability e ad agevolare l’attività di controllo del Garante stesso. L’analisi ed individuazione dei trattamenti deve essere effettuata nella azienda attraverso un’attenta mappatura dei processi e quindi analisi dei flussi informativi ad esso sottesi. Il Registro dei trattamenti deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all’effettività dei trattamenti posti in essere. Qualsiasi cambiamento,

in particolare in ordine alle modalità, finalità, categorie di dati, categorie di interessati, deve essere immediatamente inserito nel Registro, dando conto delle modifiche sopravvenute.

Il nuovo regolamento ha un approccio basato sulla **valutazione del rischio (risk based)**, piuttosto che sulla protezione dell'utente. Con tale valutazione si determina la misura di responsabilità del titolare o del responsabile del trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti. Quindi, il rischio inerente al trattamento è da intendersi come l'impatto negativo sulle libertà e i diritti degli interessati. Alcuni esempi di rischi definiti nel GDPR: Trattamento (raccolta) di dati non necessario in base alla finalità; Informativa e termini non chiari o trasparenti; Dati personali non aggiornati o obsoleti; Inefficace o intempestiva cancellazione dei dati personali; condivisione di dati con terze parti; accesso illegittimo, modifica indesiderata e scomparsa dei dati.

Molto importante è il processo della **valutazione d'impatto** sulla protezione dei dati, inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. La valutazione d'impatto sulla protezione dei dati è necessaria soltanto quando il trattamento *"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*. I titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento può presentare tale rischio. Sebbene una valutazione d'impatto sulla protezione dei dati possa essere richiesta anche in altre circostanze, l'articolo 35, paragrafo 3, fornisce alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati": a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 1013; c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Alcuni criteri di individuazione del rischio: valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione; monitoraggio sistemico; processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente; dati sensibili o dati aventi carattere altamente personale; trattamento di dati su larga scala; creazione di corrispondenze o combinazione di insiemi di dati; dati relativi a interessati vulnerabili; uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; e quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto". Un trattamento che soddisfi due criteri può formare oggetto di una valutazione d'impatto. Maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti. Un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.

Violazione dei dati personali (c.d. Data Breach) è la 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 (art. 4, punto 12 - GDPR).

Alcune possibili cause di violazione: divulgazione di dati confidenziali a persone non autorizzate; perdita o furto di dati o di strumenti nei quali i dati sono memorizzati; perdita o furto di documenti cartacei; infedeltà aziendale (ad es. persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia

distribuita in ambiente pubblico); accesso abusivo (ad es. accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite); casi di pirateria informatica, etc.

Gli obblighi del titolare in questo senso sono:

- a. Descrivere **la natura della violazione dei dati personali** compresi, ove possibile, le categorie e il numero approssimativo degli interessati, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b. Comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c. Descrivere le probabili **conseguenze** della violazione dei dati personali;
- d. Descrivere le **misure adottate** o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

La gestione di una violazione dei dati personali è stata standardizzata in un processo suddiviso in quattro fasi:

1. Identificazione e indagine preliminare;
2. Risk assessment e individuazione delle misure;
3. Notifica all'Autorità Garante: se è stata verificata la necessità di effettuare la notifica della violazione dei dati, il Titolare del trattamento provvederà alla notifica all'Autorità Garante senza ingiustificato ritardo e, ove possibile entro 72 ore dal momento in cui ne è venuta a conoscenza.
4. Comunicazione agli interessati: se è stata valutata la necessità di effettuare la comunicazione della violazione dei dati a coloro dei cui dati si tratta, in quanto è stato riscontrato un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà alla comunicazione all'Interessato senza ingiustificato ritardo.