Fulcri Privacy

NEWSLETTER

gennaio 2020

Gentile Cliente,
torna il consueto appuntamento mensile con gli aggiornamenti in relazione alle novità rilevanti in tema privacy, sicurezza e GDPR.
In questa newsletter ci occuperemo di:

- **consenso** informato al **trattamento sanitario** e consenso al **trattamento dei dati**;
- **data Breach**: cos'è, come prevenirlo, come affrontarlo.

Consenso al trattamento dei dati VS consenso informato al trattamento sanitario. Quali sono le differenze?

Molto spesso il consenso al trattamento dei dati personali viene confuso con il consenso informato medico al trattamento sanitario.

L'errore è generato dal fatto che i due istituti sono entrambi identificati con il termine "consenso", ma rispondono a requisiti di Legge e normative differenti (GDPR e leggi in materia di protezione dei dati personali da una parte, norme in materia di consenso informato e di disposizioni anticipate di trattamento dall'altro)

Nella tabella qui sotto riportiamo le principali differenze:

Consenso GDPR	**Consenso informato al trattamento**
Quando parliamo di consenso al trattamento dei dati, intendiamo la manifestazione di volontà **libera, specifica, informata e inequivocabile** con cui l'interessato manifesta il proprio assenso **al trattamento dei propri dati personali** (ad esempio per ricevere comunicazioni commerciali o per consentire l'analisi delle abitudini di acquisto, oppure per il trattamento dei dati appartenenti a categorie particolari, e cioè quelli idonei a rivelare l'origine razziale o etnica, le convinzioni religiose, filosofiche, politiche, l'appartenenza sindacale, lo stato di **salute** o la vita sessuale di una persona.). L'Autorità Garante ha dedicato uno specifico provvedimento di chiarimenti legato al trattamento dei dati particolari da parte dei **professionisti sanitari:** possono trattare i dati dei pazienti, per finalità di cura e per i trattamenti di dati necessari alla prestazione sanitaria, **senza dover richiedere il loro consenso** (pur dovendo comunque fornire loro **informazioni** complete sull'uso dei dati): dunque i trattamenti essenziali connessi **alla cura della salute** e effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona soggetta all'obbligo di segretezza **non richiedono il consenso.** **Il consenso** dell'interessato è invece necessario per trattamenti connessi all'utilizzo di **app mediche** o relativi alla **fidelizzazione** della clientela in ambito farmaceutico (es. raccolta punti attraverso **fidelity card nominali**); trattamenti con **finalità promozionali o commerciali** (es. promozioni di campagne di screening); trattamenti effettuati nell'ambito del **fascicolo sanitario elettronico**.	Secondo la normativa di riferimento (Legge n. 219/2017) **nessun trattamento sanitario può essere iniziato o proseguito se privo del consenso libero e informato della persona interessata**, tranne che nei casi espressamente previsti dalla legge (es. i cosiddetti trattamenti sanitari obbligatori). Ogni persona ha il diritto di conoscere le proprie condizioni di salute e di essere informata in modo completo, aggiornato e a lei comprensibile riguardo a: - **diagnosi**, **prognosi**, **benefici** e **rischi** degli accertamenti diagnostici e dei trattamenti sanitari; - possibili **alternative** e **conseguenze dell'eventuale rifiuto** del trattamento sanitario e dell'accertamento diagnostico o della rinuncia ad essi. La persona **minorenne o incapace** deve essere informata sulle scelte relative alla propria salute in modo adeguato alle sue capacità per essere messa nelle condizioni di esprimere la sua volontà. Per i minori e gli incapaci il consenso informato è espresso (o rifiutato), rispettivamente, dagli esercenti la responsabilità genitoriale o dal tutore, tenendo conto della volontà del minore stesso, in relazione alla sua età al suo grado di maturità e dal tutore, sentito l'interdetto, ove possibile. La persona **inabilitata**, invece, può esprimere personalmente il proprio consenso e disposizioni particolari sono previste nel caso in cui sia stato nominato un amministratore di sostegno.

Nonostante il documento relativo al consenso informato al trattamento sanitario non riguardi in maniera diretta la disciplina Privacy&Data Protection, abbiamo valutato che mettere a dispsozione

tale documento sia un grande vantaggio per i nostri clienti, soprattutto in relazione al delicato tema della somministrazione dei vaccini. Abbiamo dunque proceduto ad aggiornare il Tool a Vostra disposizione, inserendo all'interno della sezione stampa libera la possibilità di generare un documento **per la raccolta del consenso informato alla vaccinazione.** Al prossimo accesso al Tool vi verrà mostrato un pop-up che ti comunicherà questo aggiornamento, insieme a tutte le informazioni necessarie per gestire in maniera semplice ed efficace tale documento.

Data Breach

In tema di sicurezza dei dati personali, il GDPR prevede in capo a tutti i titolari di trattamento l'obbligo di notificare al Garante, e in alcuni casi comunicare anche agli interessati, la violazione dei dati personali.

Tale obbligo non trova applicazione qualora, a seguito di specifica e dettagliata analisi, il Titolare del trattamento ritenga improbabile che la violazione comporti un rischio per i diritti e le libertà delle persone fisiche.

La comunicazione deve avvenire entro 72 ore dalla scoperta della violazione. In ogni caso, il ritardo della comunicazione deve essere motivato; diversamente, il mancato o ritardato adempimento della comunicazione espone alla possibilità di sanzioni.

Cos'è il Data Breach?

Con il termine data breach si intende una violazione delle norme di sicurezza che comporti, accidentalmente o illegalmente, la distruzione, la perdita, la modifica, l'alterazione, la divulgazione non autorizzata dei dati personali trasmessi, memorizzati o altrimenti trattati, o l'accesso non autorizzato a tali dati .Si tratta di qualsiasi incidente di sicurezza, doloso o colposo, che comporti la compromissione dell'integrità, della riservatezza o della disponibilità dei dati personali.

La violazione può consistere nella perdita dei dati (incendio o altre calamità, furto o smarrimento di una chiavetta USB o altri dispositivi contenente dati riservati); impossibilità di accedere ai dati per cause accidentali o per attacchi esterni (virus, malware ecc); divulgazione non autorizzata (causato ad es. da una persona interna che avendo autorizzazione ad accedere ai dati ne produce e distribuisce una copia); alterazione dei dati personali; accesso o acquisizione dei dati da parte di terzi non autorizzati.

Come prevenirlo?

La prevenzione di data breach passa dalla valutazione dei rischi e dall'implementazione di misure di tipo tecnologico e organizzativo atte a garantire un livello di sicurezza adeguato al rischio.

Ciascun titolare pertanto dovrà porre in essere misure tecniche ed organizzative che garantiscano un livello di sicurezza adeguato rispetto ai rischi che possono derivare dai trattamenti effettuati: a livello pratico, in base quindi al singolo contesto di trattamento, il titolare dovrà individuare ed incaricare un responsabile con competenze in data protection per valutare le conseguenze sui diritti degli interessati e gestire la notifica delle violazioni; individuare un responsabile IT con competenze idonee a prevenire e gestire eventuali violazioni; definire un piano di formazione degli incaricati al trattamento dei dati personali.

A livello organizzativo, il titolare dovrà definire il livello di rischio per i diritti e la libertà degli interessati, prevedere vincoli contrattuali con professionisti o collaboratori esterni che trattano dati

personali per suo conto; definire ed adottare strumenti idonei a prevenire le violazioni; quanto alla prevenzione delle conseguenze, valutare l'adozione di sistemi atti a prevenire i rischi per i diritti degli interessati derivanti dalla violazione (ad es. adottare un sistema di crittografia dei dati).

Cosa fare dunque in caso di data breach?

Come detto, la violazione non va notificata nel caso in cui sia improbabile che essa comporti un rischio per i diritti e le libertà delle persone fisiche, quali, ad es.: danni fisici, materiali o immateriali alle persone fisiche; perdita del controllo dei dati personali; limitazione dei diritti, discriminazione; furto o usurpazione d'identità; perdite finanziarie, danno economico o sociale; decifratura non autorizzata della pseudonimizzazione; pregiudizio alla reputazione; perdita di riservatezza dei dati personali protetti da segreto professionale (come dati sanitari e giudiziari).

Diversamente la violazione va notificata al Garante **entro 72 ore dalla scoperta** all'indirizzo PEC protocollo@pec.gpdp.it , oppure tramite posta elettronica ordinaria all'indirizzo protocollo@gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. Le notifiche effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Il Garante ha messo a disposizione un **modello** da utilizzare (reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501). La comunicazione inviata **non deve contenere i dati personali oggetto di violazione** (es. non deve contenere i nomi dei soggetti interessati dalla violazione).

Il modello messo a disposizione è intuitivo e di rapida comprensione: diviso in sezioni precompilate, una volta scaricato sarà possibile modificarlo spuntando tra le opzioni fornite quella adeguata al caso specifico, inserendo i dati ove richiesti e compilando i riquadri relativi alle domande a risposta aperta. Nel modello stesso sono contenuti istruzioni e chiarimenti per una corretta e precisa compilazione. È obbligatoria la compilazione delle sezioni relative ai dati del soggetto che esegue la notifica (sez. A), ai dati del titolare del trattamento (sez. B), ai dati di contatto del soggetto incaricato a fornire ulteriori spiegazioni e chiarimenti eventualmente richiesti dal Garante (sez. B1), alle informazioni di sintesi sulla violazione (sez. C). Sarà possibile successivamente integrare le informazioni inviando un'ulteriore notifica al Garante, scegliendo nell'intestazione relativa al tipo di notifica la voce notifica "integrativa".

Se la violazione comporta un rischio elevato per i diritti delle persone, infine, il titolare deve comunicarla anche a tutti gli interessati. Nel provvedimento adottato nei confronti di uno tra i principali fornitori nazionali di posta elettronica il Garante ha avuto modo di precisare che le comunicazioni agli utenti dei data breach non devono essere generiche e devono **fornire precise indicazioni su come proteggersi da usi illeciti dei propri dati**, primo fra tutti il furto di identità (nel caso di specie la violazione era consistita in un accesso fraudolento tramite un hot spot della rete Wifi, che aveva provocato la violazione di circa un milione e mezzo di credenziali di utenti che avevano avuto accesso tramite webmail).

Il data breach e il suo "decorso" devono essere puntualmente documentati in maniera tale da consentire all'autorità garante di valutare l'efficacia delle misure rimediali poste in essere dal titolare, a pena di pesanti sanzioni fino a 10.000.000 euro o per le imprese fino al 2% del fatturato mondiale annuo dell'esercizio precedente.

Fulcri Privacy

A proposito di data breach…

Nel corso della quarantunesima conferenza internazionale delle Autorità per la protezione dei dati, le oltre 120 Autorità intervenute all'evento annuale hanno lavorato per definire un programma di lavoro comune, adottando sei risoluzioni, tra cui la "**Risoluzione sul ruolo dell'errore umano nei data breaches**" in cui è stata messa in evidenza la necessità di un'adeguata formazione del personale, di ulteriori misure per la riduzione del rischio e della costituzione di un archivio globale dove tener traccia delle violazioni.

Ha avuto inizio il 23 Settembre 2019 il "**Privacy Sweep 2019**", un'indagine a carattere internazionale dedicata alla gestione dei data breach da parte di soggetti pubblici e privati. Le Autorità di protezione dati di ogni Stato hanno svolto l'indagine prendendo in esame i processi e le procedure adottati per la gestione delle violazioni dei dati personali dai titolari dei trattamenti che operano sui rispettivi territori nazionali. L'iniziativa è coordinata dalla Global Privacy Enforcement Network (GPEN), la rete internazionale nata per rafforzare la cooperazione tra le Autorità della privacy di diversi Paesi, di cui il Garante italiano fa parte. Allo Sweep 2019 hanno partecipato, oltre a quella italiana, altre 17 Autorità garanti della privacy di vari Paesi del mondo.

Lo "Sweep" ("indagine a tappeto") sulla gestione dei data breach fa seguito ad analoghe indagini effettuate negli scorsi anni che hanno preso in esame il principio di responsabilizzazione (accountability), le informative privacy su siti web e le app per la telefonia mobile, i servizi online destinati a minori, l'Internet delle cose.

A breve saranno comunicati gli esiti delle indagini effettuate.

Per ulteriori informazioni commerciale@fulcri.it