ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI
DELLA PROVINCIA DI FIRENZE

DATA BREACH E PROCEDURA PER LA GESTIONE DEGLI EVENTI
(Deliberazione Consiglio Direttivo n. 38 del 24/03/2021)

La presente procedura è adottata per la gestione degli eventi ricondotti alla violazione di dati personali ai sensi degli artt. 33 e ss del Reg. Ue 679/2016 da parte dell'Ordine dei Medici Chirurghi e degli Odontoiatri della provincia Firenze

I Premessa
Con il termine data breach, ai sensi degli artt. 33 e 34 del Reg. UE 679/2016, s'intende la violazione dei dati personali dell'interessato persona fisica, che può consistere, a titolo esemplificativo e non esaustivo (Considerando 85 del Regolamento), in:
- perdita del controllo dei dati personali che riguardano gli interessati o limitazione dei loro diritti;
- discriminazione, furto o usurpazione d'identità;
- perdite finanziarie, decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale;
- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.

II Le tipologie di violazione dei dati personali
In linea con la definizione di violazione di dati personali, ex art. 4 p.12 Reg. UE, si distinguono 3 (tre) tipi di violazione, che possono tuttavia combinarsi tra loro e che possono compromettere la riservatezza, l'integrità o la disponibilità dei dati:
1) violazione di riservatezza, quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
2) Violazione di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3) Violazione di disponibilità, quando si verifica perdita, inaccessibilità, o distruzione, accidentali o non autorizzate, di dati personali.

III Cosa prescrive a riguardo il Regolamento UE
Art. 33: Notifica al Garante
Il Regolamento UE prescrive che il titolare, non appena viene a conoscenza di un'avvenuta violazione dei dati personali del trattamento, dovrebbe notificare la violazione al Garante della Privacy, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza del Data breach.
Se non effettuata entro 72 ore, deve essere fornita una giustificazione per il ritardo.

Che cosa deve contenere la notifica
A norma dell'art. 33 la notifica deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione 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.
Resta fermo che qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Al fine di semplificare la procedura, l'autorità Garante ha predisposto un Pdf editabile da compilare, firmare digitalmente ed inviare per ottemperare all'obbligo di notifica.

La notifica è sempre un obbligo in caso di data breach
Il Regolamento consente di non effettuare la notifica se risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Tale evenienza si verifica, per esempio, allorché siano state efficacemente attuate misure tecnologiche di cifratura o pseudonimizzazione che rendano improbabile ricostruire l'origine del dato, oppure quando il dato è inidoneo a rivelare alcunché di pregiudizievole o comunque riservato circa l'interessato.

Art. 34: Comunicazione all'interessato
In aggiunta all'obbligo di notifica all'autorità di controllo, è previsto l'obbligo di comunicare, in un linguaggio semplice e chiaro, la violazione dei dati personali allo stesso interessato allorché tale violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Cosa deve contenere la comunicazione
A norma dell'art. 34 la comunicazione, la cui forma è libera, deve obbligatoriamente:
- rappresentare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- 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.

IV Obblighi generali in capo al titolare del trattamento dei dati
Oltre alle specifiche richiamate dal Regolamento in ordine alle tecnologie che devono essere adottate per trattare i dati personali in sicurezza, l'art. 32 all'ultimo comma dispone che il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali (ovvero gli incaricati) non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
E' dunque quantomai opportuno che il titolare predisponga lettere di incarico precise ai responsabili ed agli incaricati, e fornisca loro adeguata formazione circa gli obblighi derivanti da Data breach.
Parimenti (art. 32.5) è fatto obbligo per il titolare di documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto delle disposizioni di legge (cd. "registro" delle violazioni).

Si ricorda che l'obbligo di notifica spetta al titolare, che pertanto è chiamato a verificare preventivamente l'idoneità del responsabile del trattamento, specie se trattasi di un fornitore di servizi esterno all'azienda, a gestire tempestivamente ed adeguatamente un data breach, anche prevedendo, a norma dell'art. 28 del Regolamento, idonei accordi che regolino il rapporto di fornitura in modo da garantire il rispetto del Regolamento.
L'uso dei servizi Cloud di archiviazione dati, infine, richiede una particolare attenzione da parte del titolare del trattamento, giacché il Cloud generalmente spoglia il titolare del trattamento della possibilità di ingerirsi nella gestione del sistema informatico. In tal caso il titolare del trattamento, oltre a verificare preventivamente che il servizio in Cloud abbia specifiche conformi al Regolamento Ue, in primis circa l'ubicazione dei server e le condizioni generali di contratto, dovrà anche monitorare sistematicamente il registro dei log e degli eventi, per verificare eventuali violazioni dei dati personali, specie in punto accessi non autorizzati di terzi.

V Criteri per determinare l'opportunità della notifica
La qualificazione della violazione del Data breach è rimessa sostanzialmente al titolare, sulla base della valutazione tanto della qualità del dato, quanto dei sistemi tecnologici a presidio dello stesso. Ed invero, a fronte della perdita di dati estremamente sensibili, un efficace sistema di anonimizzazione potrebbe rendere superfluo procedere alla notifica. Nel dubbio, tuttavia, è opportuno adottare la soluzione maggiormente in linea con le esigenze di tutela richiamate dal Regolamento.
In via preliminare si rimanda alle linee guida WP 29 aggiornate al 6 febbraio 2018, che forniscono una casistica di situazioni tipo che un titolare del trattamento può essere chiamato ad affrontare in presenza di un Data Breach. Ove il caso concreto sfugga alla casistica elencata, criteri per potere compiere tale scelta sono rimessi alla sensibilità del titolare in concerto con DPO incaricato, a seguito della visione della reportistica della violazione.

VI Procedura per la gestione degli eventi
1. Scoperta
L'incaricato al trattamento ravvisa un incidente nella gestione dei dati che astrattamente può determinare un data breach ai sensi del regolamento oppure un responsabile "esterno" segnala un evento che astrattamente po' determinare un data breach oppure un interessato segnala un evento che astrattamente po' determinare un data breach.

2. Avviso
Viene senza indugio informato il responsabile o referente dall'area che, a loro volta, avvisano il Titolare (o in sua assenza una persona appositamente designata). Il Responsabile e/o il Titolare di concerto con l'amministratore di sistema, nel caso il data breach si riferisca al trattamento dati effettuato con strumenti informatici, procedono alla valutazione d'impatto dell'incidente in relazione ai diritti degli interessati.
Il DPO deve essere informato e messo nelle condizioni di partecipare.

3. Convocazione del "comitato di crisi"
Il Titolare e il Responsabile dell'area (ove presente) convocano anche telefonicamente o con modalità tipo skype, etc. il "comitato di crisi" di cui fanno parte:
i) il DPO;
ii) l'amministratore di sistema o il responsabile IT;
iii) eventuali altri soggetti coinvolti (responsabile esterno etc.);
Il "comitato" verifica l'eventuale sussistenza del rischio per gli interessati.

4. L’esito della verifica

a) se il data breach non risulta presentare alcun rischio per gli interessati, non si provvede ad alcuna notifica né all’autorità di controllo né agli interessati. Si procede comunque ad annotare nell’apposito registro l’incidente.

b) Se il data breach risulta presentare rischi per gli interessati si cerca di stimare la gravità del rischio per procedere alla notifica al Garante mediante il modulo apposito.