ASU FC
Azienda sanitaria universitaria Friuli Centrale

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

Procedura per la gestione di violazioni dei dati personali - "*DATA BREACH*"
Capo IV - Regolamento Europeo 2016/679
relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

INDICE

1. INTRODUZIONE

L'Azienda Sanitaria Universitaria Friuli Centrale (d'ora in poi ASUFC), al fine di garantire l'erogazione e la gestione delle prestazioni sanitarie, nonché la gestione dei rapporti di lavoro dipendente e non, tratta, quotidianamente, innumerevoli quantità di dati personali (ad es. dati anagrafici, indirizzi, recapiti telefonici) e di dati particolari (ad es. informazioni sullo stato di salute), degli Utenti che si rivolgono alle varie strutture e di tutti coloro che svolgono la prestazione lavorativa in favore dell'azienda stessa.

Nonostante l'adozione di misure tecniche ed organizzative adeguate a garantire il rispetto della normativa europea in materia di trattamento dei dati ed il costante aggiornamento delle misure di sicurezza in base allo sviluppo tecnologico, è possibile che si verifichino delle violazioni di dati personali, ovvero delle violazioni di sicurezza che comportano, 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.

2. SCOPO

Con la presente procedura, l'ASUFC intende descrivere i comportamenti da adottare ed i percorsi da seguire, da parte di chiunque operi all'interno dell'azienda, nell'ipotesi in cui abbia contezza del verificarsi di una violazione di dati personali.

3. DEFINIZIONI

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, numero di identificazione, dati relativi all'ubicazione, un identificativo *on line* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, generica, psichica, economica, culturale o sociale.

Dati genetici: dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

Dati biometrici: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Interessato: la persona fisica alla quale i dati si riferiscono.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità ed i mezzi del trattamento di dati personali.

Autorizzato / designato al trattamento: persona fisica che opera sotto l'autorità del titolare del trattamento, a cui sono attribuiti specifici compiti e funzioni connesse al trattamento dei dati e che ha ricevuto adeguata formazione e precise istruzioni in materia.

Responsabile della protezione dei dati (DPO – *Data Protection Officer*): persona fisica designata dal titolare ai sensi dell'art. 37 del Regolamento Europeo, con funzioni di supporto e controllo, consultive, formative ed informative relativamente all'applicazione del Regolamento.

Privacy Officer: dirigente interno all'azienda con il compito di fornire al Titolare la consulenza necessaria per operare in conformità alla normativa in materia di trattamento di dati personali, di supportare il Titolare nello sviluppo delle strategie aziendali relative al trattamento dei dati personali e di supervisionare il compimento degli adempimenti in materia da parte dell'Ufficio Privacy;

Ufficio Privacy: ufficio costituito all'interno dell'azienda, diretto e coordinato dal dirigente incaricato quale *Privacy Officer*, con il compito di porre materialmente in essere gli adempimenti previsti dalla normativa vigente in materia di trattamento di dati personali, di gestire, unitamente al Responsabile della protezione dei dati, le istanze degli interessati, nonché le ipotesi di violazione dei dati personali (*data breach*).

4. COS'E' UNA VIOLAZIONE DI DATI PERSONALI "*DATA BREACH*" – TIPOLOGIE DI VIOLAZIONI

Ai sensi dell'art. 4, punto 12, del Regolamento UE, per "violazione dei dati personali" ("*data breach")* deve intendersi 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.

Si possono, quindi, individuare tre tipi di violazioni:

a. violazione della riservatezza,
b. violazione dell'integrità,
c. violazione della disponibilità.

Si verifica una violazione della riservatezza qualora vi sia una diffusione dei dati, un accesso non autorizzato o accidentale; si ha una perdita di integrità allorquando vi sia una modifica dei dati non autorizzata o accidentale, mentre si parla di perdita di disponibilità quando si verifica l'impossibilità di accesso ai dati, la perdita, la distruzione non autorizzata o accidentale.

5. POSSIBILI CONSEGUENZE DI UNA VIOLAZIONE DEI DATI PERSONALI

Una violazione dei dati personali può avere numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali.

A titolo meramente esemplificativo, si citano i seguenti effetti negativi: la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate.

6. GESTIONE DEL *DATA BREACH* DA PARTE DEL TITOLARE DEL TRATTAMENTO

Nel caso in cui si verifichi una violazione di sicurezza, i passaggi da seguire sono i seguenti:

1. ricognizione dell'evento e comunicazione al proprio Direttore di Struttura,
2. comunicazione all'Ufficio Privacy,
3. analisi preliminare dell'evento da parte dell'Ufficio Privacy,
4. comunicazione al Responsabile della Protezione dei Dati – DPO,
5. espressione del parere da parte del DPO,
6. comunicazione al Direttore Generale,
7. determinazioni del Direttore Generale,
8. redazione del modulo di notifica del *data breach*, trasmissione al DPO ed al Direttore Generale e successivo invio all'Autorità Garante,
9. annotazione della violazione nel registro aziendale appositamente istituito.

6.1. Ricognizione dell'evento e comunicazione al proprio Direttore di Struttura

Chiunque operi all'interno di ASUFC (personale dipendente e non), qualora venga a conoscenza di una potenziale violazione di dati, anche tramite segnalazioni esterne dei cittadini, deve avvisare tempestivamente il proprio Direttore di Struttura, fornendo al medesimo, in modo dettagliato, tutte le informazioni di cui dispone.

6.2 Comunicazione all'Ufficio Privacy

Il Direttore di Struttura, effettuata una prima valutazione sul merito della questione, la segnala rapidamente all'Ufficio Privacy, mediante l'invio di una mail all'indirizzo di posta elettronica privacy@asufc.sanita.fvg.it. Può essere utilizzato l'apposito modulo per la segnalazione presente sul sito aziendale, in allegato alla presente procedura.

La mail deve avere il seguente contenuto:

- indicazione della tipologia di violazione;
- collocazione temporale e descrizione dettagliata dell'evento;
- indicazione della categoria di dati personali oggetto della violazione, precisando se i dati in questione determinano l'immediata identificabilità dell'interessato e se trattasi di dati in grado di

rivelare patologie e / o aspetti della personalità che possono comportare discriminazioni o danneggiare gravemente la dignità o la reputazione dell'interessato;

- indicazione, ove possibile, del volume / numero di dati personali oggetto di violazione;
- indicazione, ove possibile, del numero e della tipologia di soggetti che hanno ricevuto e visionato i dati oggetto di violazione;
- indicazione delle possibili conseguenze dannose (possibili danni fisici, materiali o immateriali) per l'interessato;
- precisazione delle eventuali misure tecniche ed organizzative adottate nell'immediato, al fine di porre rimedio alla violazione e ridurre gli effetti negativi sugli interessati;
- indicazione di ogni altro aspetto o circostanza che si ritenga utile indicare.

6.3 Analisi preliminare dell'evento da parte dell'Ufficio Privacy

L'ufficio privacy, che riceve la mail, analizza quanto comunicato per accertare che l'incidente di sicurezza si sia effettivamente verificato. Per l'accertamento, l'ufficio potrà avvalersi dei soggetti che ritiene maggiormente competenti alla trattazione del caso specifico.

6.4 Comunicazione al Responsabile della Protezione dei Dati (DPO)

Terminata questa prima analisi, i relativi esiti vengono comunicati al DPO, affinché fornisca il suo parere.

6.5 Espressione del parere da parte del DPO

Il DPO è tenuto a svolgere una valutazione dei seguenti elementi:

- se c'è stata una violazione dei dati personali ai sensi del GDPR, se ci sono prove evidenti o se è probabile / possibile che si tratti di una violazione,
- quali sono le categorie di persone interessate dalla (possibile) violazione e quali categorie di dati personali sono state coinvolte,
- se la violazione comporta un rischio "probabile" o "improbabile" di mettere in pericolo i diritti e le libertà delle persone fisiche,
- se sussiste un rischio elevato per i diritti e le libertà delle persone fisiche (con conseguente necessità anche della comunicazione agli interessati).

6.6 Comunicazione al Direttore Generale

A questo punto, l'Ufficio privacy informa il Direttore Generale di quanto accaduto, esponendo gli esiti della propria analisi ed il parere espresso dal DPO.

6.7 Determinazioni del Direttore Generale

Il Direttore Generale viene, quindi, messo a conoscenza dell'avvenuta violazione di sicurezza e assume le proprie determinazioni, in qualità di legale rappresentante del Titolare del trattamento, disponendo la necessità o meno della notifica all'Autorità Garante, sulla base di un giudizio di probabilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica all'Autorità Garante deve essere effettuata nel termine di 72 ore dal momento in cui il Titolare è venuto a conoscenza del *data breach*. Oltre il termine di 72 ore, la notifica deve essere corredata dalle ragioni del ritardo.

6.8 Redazione del modulo di notifica del *data breach,* trasmissione al DPO ed al Direttore Generale e successivo invio all'Autorità Garante.

Qualora il Direttore Generale ritenga necessaria la notifica all'Autorità Garante, la relativa comunicazione viene predisposta dall'Ufficio Privacy, utilizzando l'apposito modulo messo a disposizione della stessa Autorità e, successivamente, viene sottoposta al DPO per una sua valutazione e, infine, al Direttore Generale per la sua approvazione.

L'Ufficio privacy cura anche la parte relativa all'invio del modulo, in conformità alla procedura indicata dall'Autorità Garante.

6.9 Annotazione dell'evento nell'apposito registro

Tutte le violazioni, tanto quelle soggette a notifica all'Autorità Garante, quanto quelle per le quali la notifica non è necessaria, sono annotate, a cura dell'Ufficio Privacy, nell'apposito registro, al fine di documentare l'accaduto ed il rispetto della normativa.

7. GESTIONE DEL *DATA BREACH* DA PARTE DEL RESPONSABILE DEL TRATTAMENTO

In tutti i casi in cui il Titolare ricorre ad un Responsabile del trattamento dei dati, l'articolo 33, paragrafo 2, del Regolamento UE prevede l'obbligo di quest'ultimo di informare, senza ingiustificato ritardo, il Titolare dopo essere venuto a conoscenza della violazione.

Il Responsabile del trattamento non è tenuto a valutare la probabilità di rischio derivante dalla violazione prima di notificarla al Titolare, deve limitarsi soltanto a stabilire se si è verificata o meno una violazione e provvedere alle dovute comunicazioni al Titolare. Ogni ulteriore e più approfondita valutazione compete al Titolare.

Nei contratti di nomina a responsabile del trattamento, ASUFC, all'art. 5, prevede che "*il Responsabile si impegna ad informare il Titolare, senza ingiustificato ritardo dal momento in cui ne è venuto a conoscenza (inviando una comunicazione PEC all'indirizzo asufc@certsanita.fvg.it), di ogni violazione della sicurezza che comporti 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, fornendo le informazioni necessarie alla gestione delle misure 33 e 34 del Reg. UE 2016/679 e collaborando con il Titolare per fornire tempestivamente ogni informazione da questi comunque richies*ta".

Viene, quindi, formalizzato l'impegno di comunicazione, senza ingiustificato ritardo, e di collaborazione con il Titolare nella gestione del *data breach* e le modalità della comunicazione stessa (invio di una pec all'indirizzo asufc@certsanita.fvg.it).

8. SANZIONI IN CASO DI MANCATA NOTIFICA DELLA VIOLAZIONE ALL'AUTORITA' GARANTE

Il mancato rispetto dell'obbligo di notifica ex art. 33, Regolamento UE, comporta l'applicabilità da parte dell'Autorità Garante di sanzioni fino a 10.000.000 di euro (art. 83, paragrafo 4, lett. A, Regolamento UE).

L'Autorità Garante potrebbe, inoltre, applicare le misure correttive previste dall'art. 58 del Regolamento Europeo e, quindi, rivolgere al Titolare avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti provvisori o definiti al trattamento e di divieti, ordini di rettifica e cancellazione dei dati, revoche di certificazioni.

9. COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'INTERESSATO

L'art. 34 del Regolamento Europeo prevede che, quando la violazione di dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve comunicare la violazione all'interessato senza ingiustificato ritardo.

All'interessato, con un linguaggio semplice e chiaro, deve essere comunicata la natura della violazione dei dati personali, il nome e i dati di contatto del DPO, le probabili conseguenze dell'evento e le misure adottate o in fase di adozione dal Titolare per porre rimedio alla violazione e, se possibile, per attenuare i possibili effetti negativi.

La comunicazione all'interessato non è richiesta qualora sia soddisfatta una delle seguenti condizioni:

a. il Titolare del trattamento ha applicato misure tecniche e organizzative adeguate a proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi;
b. il Titolare del trattamento, immediatamente dopo l'evento, ha adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c. la comunicazione agli interessati richiederebbe uno sforzo sproporzionato (in questi casi è necessario prendere in considerazione una comunicazione pubblica o una misura analoga).

Anche il mancato rispetto dell'obbligo di comunicazione agli interessati comporta l'applicazione, da parte dell'Autorità Garante, di sanzioni fino a 10.000.000 di euro.

10. ELEMENTI PER LA VALUTAZIONE DELL'ESISTENZA DI UN RISCHIO O DI UN RISCHIO ELEVATO

Nel momento in cui si viene a conoscenza di una violazione, è fondamentale valutare il rischio che potrebbe derivarne. Ciò per due motivi: conoscere l'entità dell'impatto sulle persone fisiche permette di adottare misure efficaci per contenere e risolvere la violazione e permette di stabilire se è necessaria la notifica all'autorità di controllo ed, eventualmente, anche la comunicazione alle persone fisiche interessate.

Al fine di valutare l'esistenza di un rischio o di un rischio elevato, secondo le Linee Guida elaborate dal Gruppo di Lavoro Art. 29, è necessario tenere in considerazione i seguenti criteri:

- tipo di violazione
- natura, carattere sensibile e volume dei dati personali
- facilità di identificazione delle persone fisiche
- gravità delle conseguenze sulle persone fisiche
- caratteristiche particolari dell'interessato (minori, soggetti vulnerabili)
- caratteristiche particolari del Titolare
- numero di persone fisiche interessate.