AULSS 8 BERICA

UOC AFFARI GENERALI E LEGALI

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH) DELL'AZIENDA ULSS 8 BERICA

Azienda ULSS 8 Berica

Codifica	**AG-PG-1**
Redazione/Stesura	**Dott.ssa Lisa Brazzale f.to** **Dott.ssa Linda Traverso f.to**
Verifica	**Responsabile UOSD Qualità** **Dott. Marcello Mezzasalma f.to**
Approvazione	**Direttore** **Avv. Stefano Cocco f.to**
Rev. 00	**Data 06.08.2026**
Riconferma	**Responsabile** **Data**

INDICE

PREMESSA

A partire dal 25 maggio 2018 è divenuto applicabile sul territorio nazionale il Regolamento Europeo in materia di protezione dei dati personali (679/2016 - GDPR) che disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la loro libera circolazione, introducendo un quadro normativo uniforme e vincolante per tutti gli Stati membri.

La normativa europea in esame, delineata dal citato GDPR e confermata dal D.Lgs. n. 101/2018 di modifica ed integrazione del D.Lgs. n. 196/2003, detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali.

Tra le attività attribuite al Titolare del trattamento dei dati personali rientra quella di valutare eventuali violazioni di dati personali (c.d. Data Breach) che possano comportare pericoli significativi per la protezione dei dati degli interessati e, se ne sussistono i presupposti, notificare l'evento senza ingiustificato ritardo all'autorità Garante per la protezione dei dati personali (art. 33 GDPR) e ai singoli interessati (art. 34 GDPR).

L'Azienda ULSS n. 8 Berica, al fine di garantire una più efficace gestione di potenziali incidenti di sicurezza, ha predisposto la presente Procedura ad uso interno che descrive le modalità operative adottate dall'Azienda per poter rispettare quanto previsto dagli artt. 33 e 34 del Regolamento UE 679/2016.

GRUPPO DI LAVORO

Dott.ssa Lisa Brazzale	UOC Affari Generali e Legali
Dott.ssa Linda Traverso	UOC Affari Generali e Legali

GLOSSARIO

Titolare del trattamento (Art. 4, n. 7, del Regolamento): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi di trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Interessato (Art. 4, n. 1, del Regolamento): la persona fisica identificata o identificabile a cui si riferisce il dato personale oggetto di trattamento.

Dato personale (Art. 4, n. 1, del Regolamento): qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Trattamento (Art. 4, n. 2, del Regolamento): 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.

Violazione dei dati personali/Data Breach (Art. 4. n. 12, del Regolamento): 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.

Notifica di una violazione dei dati personali all'Autorità di Controllo: comunicazione del Data Breach all'Autorità Garante per la protezione dei dati personali.

Comunicazione di una violazione dei dati personali all'interessato: comunicazione del Data Breach al soggetto i cui dati sono stati violati.

Responsabile della Protezione dei Dati (RPD/DPO): la persona fisica o giuridica nominata ai sensi dell'art. 37 del Regolamento, che svolge la propria attività ai sensi degli articoli 37, 38 e 39 del Regolamento medesimo o di altre disposizioni ivi contenute.

RIFERIMENTI NORMATIVI

La procedura è redatta tenendo in considerazione i requisiti di cui al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (di seguito *Regolamento*), e, nello specifico, gli articoli 33 e 34, nonché le linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati (GDPR).

SCOPO E CAMPO DI APPLICAZIONE

La presente procedura ha lo scopo di gestire il flusso di attività da porre in essere nel momento in cui si sviluppi una possibile violazione di dati personali ai sensi degli articoli 33 e 34 del Regolamento UE 2016/679 (GDPR).

Il Regolamento Europeo sopra menzionato prevede che, in caso di violazione dei dati personali, il Titolare del trattamento debba notificare la violazione all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro settantadue (n. 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.

CASI NEI QUALI AVVIARE LA PROCEDURA DI GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

I casi in cui è necessario applicare la presente procedura sono, a titolo esemplificativo e non esaustivo, quelli di seguito indicati:

- sottrazione di credenziali di autenticazione;
- furto o smarrimento di PC, Notebook, Tablet, Smartphone o altri dispositivi contenenti dati personali aziendali;
- erronea diffusione, pubblicazione o comunicazione di dati personali;
- divulgazione di dati confidenziali a persone non autorizzate;
- intrusione non autorizzata nei locali in cui sono conservati o archiviati dati personali;
- furto di archivi cartacei e/o digitali;
- accesso non autorizzato nel sistema informativo;
- accesso abusivo a dati personali contenuti nelle banche dati aziendali;
- azione di malware (virus, ecc.) che siano riusciti ad eludere le misure di sicurezza aziendali;
- smarrimento di dati personali (archiviati su supporti cartacei e digitali);
- distruzione di dati personali (archiviati su supporti cartacei e digitali).

PROCEDURA DI GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

In caso di concreta, sospetta e/o avvenuta violazione dei dati personali, è di estrema importanza assicurare che la stessa venga affrontata immediatamente e correttamente al fine di minimizzare l'impatto della violazione, valutare e limitare i potenziali effetti negativi sugli interessati, attuare eventuali misure correttive e adempiere alle prescrizioni imposte agli articoli 33 e 34 Regolamento 679/2016/UE.

Pertanto, il preposto al trattamento di dati personali che sia venuto a conoscenza di una possibile violazione, condiviso l'evento con il Responsabile del servizio di appartenenza, deve attivare, senza ingiustificato ritardo, il flusso di adempimenti di seguito descritti:

A. raccolta e comunicazione scritta all'Ufficio Aziendale referente in materia di adempimenti Privacy all'indirizzo *affari.generali@aulss8.veneto.it*, delle informazioni relative alla violazione di dati personali al fine di consentire al suddetto ufficio di effettuare un'analisi preventiva della stessa (data e ora dell'evento se conosciuti, data in cui il Titolare ne è venuto a conoscenza, descrizione dettagliata dell'evento, tipologia e quantità di dati coinvolti, categorie e numero di interessati coinvolti). Se la violazione riguarda un asset tecnologico-informatico, è opportuno che vengano coinvolti tempestivamente anche i Sistemi Informativi aziendali al fine di valutare l'entità della violazione e assumere rapidamente le opportune soluzioni per attenuare i possibili effetti negativi della stessa;
B. l'Ufficio Aziendale referente in materia di adempimenti Privacy procederà ad una valutazione preliminare riguardante la possibile violazione verificatasi, con eventuale supporto del Responsabile della Protezione dei Dati (RPD/DPO) e avvierà la necessaria istruttoria al fine di accertare se la violazione si sia effettivamente verificata, valutare la probabilità e la gravità dei rischi per i diritti e le libertà delle persone fisiche e stabilire, infine, se sia necessario o meno effettuare la notifica all'Autorità Garante per la Protezione dei Dati Personali e la comunicazione agli interessati;
C. nel caso si stabilisca che la violazione si sia effettivamente verificata e questa comporti un rischio per i diritti e la libertà delle persone fisiche in termini di disponibilità, integrità o riservatezza dei dati, è opportuno innanzitutto adottare tempestivamente le eventuali misure correttive e di protezione che possano limitare i danni che la violazione potrebbe causare;

D. l'Ufficio Aziendale referente in materia di adempimenti Privacy provvede alla trasmissione tramite email al RPD/DPO della documentazione raccolta nel corso dell'istruttoria. La comunicazione può contenere il facsimile del modello di notifica messo a disposizione dall'Autorità Garante per la Protezione dei Dati Personali nel proprio sito web, già compilato nelle parti di competenza dell'Azienda Sanitaria. In ogni caso, all'interno della comunicazione dovranno essere riportate le seguenti informazioni:
   - informazioni sulla violazione (identificazione e descrizione dell'evento, con particolare riferimento alla data in cui l'evento si è verificato, la data in cui il Titolare ne è venuto a conoscenza, la tipologia e la quantità di dati violati, le categorie e il numero di interessati coinvolti nella violazione);
   - misure tecnologiche e organizzative applicate per proteggere i dati personali (sia prima, che durante che dopo la violazione);
E. valutazione da parte del RPD/DPO della documentazione ricevuta e valutazione della necessità di effettuare la notifica all'Autorità Garante e di effettuare la comunicazione agli interessati;
F. trasmissione da parte del RPD/DPO delle risultanze delle valutazioni all'Azienda Sanitaria;
G. ove risulti improbabile che dalla violazione possa derivare un rischio per i diritti e le libertà degli interessati, il Titolare non provvederà alla notifica all'Autorità Garante per la protezione dei dati personali.
H. notifica da parte dell'Azienda Sanitaria all'Autorità Garante per la Protezione dei Dati Personali della violazione subita nell'ipotesi in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche;
I. eventuale comunicazione della violazione di dati personali agli interessati da parte del servizio che ha subito la violazione con l'eventuale supporto dell'Ufficio Aziendale referente in materia di adempimenti Privacy nel caso vi sia un rischio elevato per i loro diritti e le loro libertà;
J. in ogni caso, indipendentemente dalla notificazione della violazione all'Autorità Garante per la Protezione dei Dati Personali, ogni qualvolta si verifichi una violazione di dati personali, l'Azienda sarà tenuta a documentarlo all'interno dell'apposito Registro aziendale delle violazioni.

TEMPI DI ENTRATA IN VIGORE

La presente procedura entrerà in vigore dalla data di adozione con atto deliberativo del Direttore Generale.