PROCEDURA OPERATIVA

PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

INDICE di REVISIONE	00	
DATA di AGGIORNAMENTO	19/05/2023	
DESCRIZIONE/MODIFICHE	Emissione	
FASE	**NOMINATIVO**	**Firma**
REDAZIONE Data _____	S. Ruffoni – Ufficio Privacy	
PRE-VERIFICA Data _____	C. Paganoni – Incarico di Funzione Qualità e Risk Management - SC Gestione Operativa: Next generation EU – Qualità e Risk Management	
	A. Scarafoni – SC Gestione Operativa: Next generation EU – Qualità e Risk Management	
VERIFICA Data _____	S. Benedetti - Responsabile SS Trasparenza e Internal Auditing	
	R. Coppola – DPO Aziendale	
	A. Panese – Direttore SC Sistemi Informativi Aziendali	
	V. Berta – Responsabile per la tenuta del protocollo informatico della gestione dei flussi documentali e degli archivi	
	A. Rossodivita - Direttore SC Gestione Operativa: Next Generation EU - Qualità e Risk Management	
APPROVAZIONE Data _____	A. De Vitis - Direttore Amministrativo	

VISTO Data _____	T. Saporito – Direttore Generale	
	G. Ardemagni – Direttore Sanitaria	
	P. Formigoni – Direttore Socio Sanitario	

INDICE

1. SCOPO

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

Per data breach, in italiano "violazione dei dati personali", si intende una violazione di sicurezza che comporta accidentalmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

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 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.

La procedura sarà gestita tramite il flusso "data breach" presente nel software MUA – Motore Unico Amministrativo, in uso presso l'ASST Valtellina e Alto Lario, tramite la compilazione di un questionario on-line e coinvolgerà le diverse Unità Organizzative che segnaleranno l'avvenuta violazione, la funzione interna competente in materia di protezione dei dati ed il Data Protection Officer (DPO).

Scopo della Procedura è, altresì, definire i ruoli, le responsabilità e le attività da effettuare qualora si verifichi un incidente di sicurezza che comporti la violazione dei dati personali.

In particolare, la presente Procedura mira a disciplinare compiutamente le fasi di segnalazione, valutazione ed eventuale notifica/comunicazione di un data breach.

2. CAMPO DI APPLICAZIONE

Casi nei quali avviare la procedura di gestione della violazione dei dati personali (data breach)

I casi in cui sarà necessario applicare la presente procedura sono, a titolo esemplificativo e non esaustivo:

- sottrazione di credenziali di autenticazione;
- furto/smarrimento di PC, Notebook, Tablet, Smartphone contenenti dati personali;
- erronea diffusione, pubblicazione o comunicazione di dati personali;
- intrusione non autorizzata in locali in cui sono conservati/archiviati dati personali;
- furto di archivi cartacei e/o digitali;
- accesso non autorizzato nel sistema informativo;
- azione di malware (virus, etc.) 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);
- ecc.

3. RESPONSABILITÀ

Le SC e i soggetti coinvolti nella gestione del processo sono le seguenti:

- L'**Ufficio Privacy** ha il compito di:
  - raccogliere le segnalazioni di ogni evento anomalo (quali perdita di strumenti, accessi illegittimi, ecc.);
  - valutare se l'evento segnalato coinvolga dati personali, con il supporto del DPO e dei Responsabili interni interessati dall'evento;
  - decidere, con il supporto del DPO, sulla necessità di comunicare il data breach al Garante della Privacy e/o agli Interessati;
  - decidere, con il supporto del DPO, il contenuto della comunicazione al Garante della Privacy e/o agli Interessati;
  - redigere, con il supporto del DPO, ed inviare la comunicazione al Garante della Privacy e/o agli Interessati;
  - aggiornare, con il supporto del DPO, il Registro delle segnalazioni ricevute, dando evidenza – tramite specifica annotazione – di ogni data breach e delle azioni assunte con

riferimento allo stesso.

- Il **DPO (Data Protection Officer)** è responsabile delle seguenti attività:
  - vigilare sulla corretta gestione della segnalazione;
  - supportare il Titolare, tramite l'Ufficio Privacy, nella valutazione di ogni segnalazione e, ove necessario, nelle scelte di comunicazione all'Autorità e/o agli Interessati;
  - supportare il Titolare, tramite l'Ufficio Privacy, nell'individuazione delle misure correttive da adottare a seguito di violazione.
- Il **Responsabile interno del trattamento** è tenuto alle seguenti attività:
  - segnalare all'Ufficio Privacy immediatamente qualsiasi evento anomalo o perdita/divulgazione, anche accidentale di dati personali (anche solo sospetto), di cui abbia avuto conoscenza nello svolgimento della propria attività lavorativa in modo diretto o indiretto;
  - supportare l'Ufficio Privacy nell'individuazione delle misure correttive da adottare al fine di eliminare o minimizzare gli effetti della violazione sui diritti e le libertà degli Interessati.
- Ogni **Incaricato al trattamento** è tenuto alle seguenti attività:
  - segnalare al Responsabile interno del trattamento immediatamente qualsiasi evento anomalo o perdita/divulgazione, anche accidentale di dati personali (anche solo sospetto), di cui abbia avuto conoscenza nello svolgimento della propria attività lavorativa in modo diretto o indiretto.
- **SC Sistemi Informativi Aziendali:**
  - se la violazione riguarda un asset tecnologico-informatico collabora con l'Ufficio Privacy per la gestione del Data Breach.

La responsabilità di revisione è a carico del DPO Aziendale e l'ufficio Privacy e la diffusione della presente Procedura Operativa è in capo all'ufficio Privacy e alla Direzione Amministrativa.

4. RIFERIMENTI BIBLIOGRAFICI

I presupposti, i termini e i contenuti della notifica all'Autorità di controllo competente e della comunicazione agli Interessati trovano definizione negli artt.33 e 34 del GDPR.

In particolare, l'art.33 GDPR ("Notifica di una violazione dei dati personali all'autorità di controllo") al suo co.1 prescrive che: «In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 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. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo».

Inoltre, l'art.34 GDPR ("Comunicazione di una violazione dei dati personali all'interessato") al co.1 dispone che: «Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo».

Ulteriori riferimenti normativi ed interpretativi sono contenuti:

- nelle Linee Guida dell'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA) e ulteriori parametri tratti dall'art. 3, par. 2 reg. (UE) n. 611/2013;
- nelle Linee Guida del Gruppo di Lavoro WP29 sulla notifica delle violazioni dei dati personali – WP250 rev.01;
- nelle comunicazioni della Commissione al Parlamento europeo e al Consiglio (tra cui COM (2018), 24.1.2018, Maggiore protezione, nuove opportunità).

5. TERMINI E DEFINIZIONI

TERMINE/ABBREVIAZIONE	DEFINIZIONE
Incaricato al trattamento	Soggetto interno al quale viene attribuito il compito di trattare dati secondo le istruzioni impartite dal Titolare.
Data breach	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.
Data Protection Officer **(DPO)**	Soggetto incaricato dall'ASST a fornire supporto nell'ambito del trattamento dei dati personali e, tra l'altro, figura di contatto con l'Autorità e con gli Interessati.
Dato Personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato"). Si considera identificabile la persona fisica che può essere individuata, direttamente o indirettamente, con particolare riferimento ad 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.
Garante per la protezione dei dati personali	L'Autorità incaricata di sorvegliare sull'osservanza della normativa *privacy*, nazionale ed europea, vigente.
Interessato	Persona fisica a cui si riferiscono i dati personali.
Misure di sicurezza	Insieme di tutti gli accorgimenti tecnici ed organizzativi utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, nonché l'accesso ai dati alle sole persone autorizzate.
Responsabile interno del trattamento	Soggetto interno referente in tema privacy per gli incaricati al trattamento e responsabile nelle diverse Unità della corretta applicazione della normativa privacy e delle indicazioni fornite dal Titolare.
Responsabile esterno del trattamento	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento.
Titolare del trattamento	Persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i

	mezzi del trattamento di dati personali.
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.
Ufficio Privacy	Unità responsabile della gestione degli adempimenti in materia di protezione dei dati personali all'interno dell'Azienda.
SC Sistemi Informativi Aziendali	Unità responsabile dell'implementazione di procedure e processi ICT.

6. DOCUMENTI ALLEGATI

- Allegato 1 "Istruzioni flusso data breach".

7. DESCRIZIONE DELL'ATTIVITÀ

7.1 Procedura di gestione della violazione dei dati personali (data breach)

Nel caso in cui un soggetto venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati.

La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:

A. rilevazione della violazione o di una presunta violazione dei dati personali da parte del soggetto incaricato al trattamento o dal responsabile interno del trattamento e comunicazione immediata all'ufficio privacy alla e-mail ufficio.privacy@asst-val.it.
B. In caso di urgenza, le segnalazioni trasmesse via mail devono essere comunicate tempestivamente anche telefonicamente ai numeri 0342 521055/521033/521943 (SC Affari Generali e Legali), dal lunedì al venerdì - 8.00 /16.30.
C. L'Ufficio Privacy dell'ASST procederà ad una prima analisi della violazione di concerto con il DPO.
D. Compilazione della prima parte del flusso di data breach fino a chiusura della sezione (step A-B-C dell'Allegato 1 Descrizione flusso Data Breach).
E. Compilazione da parte del DPO della seconda parte del Flusso, e valutazione della necessità di effettuare la comunicazione all'Autorità Garante.
F. Notifica all'Autorità Garante della violazione subita, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche.
G. Eventuale comunicazione della violazione di dati personali all'interessato nel caso vi sia un rischio elevato. (Il documento per la segnalazione agli interessati potrà essere generato tramite il flusso dei "data breach").
H. Nel caso in cui si sia valutato di non effettuare comunicazione all'Autorità Garante sarà necessario registrare la violazione all'interno del sistema MUA, tramite lo svolgimento del Flusso di segnalazione di data breach, al fine di mantenere aggiornato il "Registro degli incidenti". Tale registro sarà reperibile all'interno del sistema nella pagina "Elementi di analisi", alla voce "Regolamento 679/2016/UE - Data breach".

7.2 Modalità di avvio della procedura di gestione della violazione

L'avvio della procedura di gestione data breach dovrà essere sviluppata seguendo le seguenti fasi:

1. Comunicazione/segnalazione dell'evento che può comportare una violazione di dati all'Ufficio privacy dell'ASST (vedi paragrafo precedente) mezzo e-mail, cellulare, recapito ufficio, o personalmente.
2. L'Ufficio Privacy deve raccogliere, prima dell'avvio del flusso tramite il sistema MUA, tutte le informazioni necessarie.
3. Se la violazione riguarda un asset tecnologico-informatico, è opportuno che venga coinvolta la SC Sistemi Informativi Aziendali, o il referente per il sistema informativo, o la società esterna incaricata dell'assistenza informatica, al fine di valutare la portata della violazione e descrivere dettagliatamente l'accaduto. È inoltre opportuno che chi avvierà la procedura di gestione della violazione coinvolga il referente (interno o esterno) del servizio che ha subito la violazione.
4. L'Ufficio Privacy procede con l'accesso nominativo al sistema MUA attraverso l'indirizzo web https://asst-val.muacloud.it/ e avvia il flusso "Privacy – Data breach" secondo le istruzioni descritte nell'allegato 1 "Descrizione del flusso data breach".
5. L'Ufficio Privacy deve rispondere alle domande del questionario presenti in MUA relative a:
   - identificazione e descrizione dell'evento;
   - misure tecnologiche e organizzative applicate a protezione dei dati (prima, durante e dopo la violazione);
   - informazioni relative ai soggetti individuati per la gestione della procedura; se necessario dovrà farsi affiancare nella sua compilazione da coloro che sono in possesso delle informazioni.
6. Conclusa la compilazione del questionario l'Ufficio Privacy chiude il flusso, completandolo e passando l'incarico al DPO.
7. Il flusso incarica il DPO, dello svolgimento della seconda parte del flusso.
8. Il DPO riceve una e-mail dal sistema MUA che lo informa che è stato incaricato di svolgere la seconda parte del flusso.
9. Il DPO accede al sistema MUA attraverso l'indirizzo web https://asst-val.muacloud.it/ dove trova evidenziato in rosso il pulsante "Attività da svolgere" e attiva il flusso attivo chiamato "Privacy – data breach".
10. Il DPO visualizza all'interno del sistema MUA le informazioni inserite durante la prima parte del flusso.
11. In base alle informazioni inserite il DPO valuta la necessità di fare comunicazione all'Autorità Garante e agli interessati e procede con la compilazione del questionario.

7.3 Disciplina delle fattispecie

Il DPO fino alla chiusura del flusso in MUA:

7.3.1 Caso A: incidente da inserire nel registro incidenti

1. Inserimento della violazione nel registro incidenti.
2. Comunicazione da parte del DPO di chiusura dell'incidente.

7.3.2 Caso B: incidente da inserire nel registro incidenti e da notificare all'Autorità Garante (nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche)

1. Inserimento della violazione nel registro incidenti.
2. Generazione del fac-simile di comunicazione di data breach.
3. Trasmissione della comunicazione di chiusura della procedura da parte del DPO alla e-mail ufficio.privacy@asst-val.it.
4. Acquisizione, mediante download, del fac-simile di segnalazione di data breach all'Autorità Garante nel seguente modo:

- accedere alla sezione “Elementi d’analisi” alla voce “Regolamento 679/2016/UE - data breach”;
- posizionarsi sulla violazione/incidente inserito;
- espandere la sezione “File allegati”;
- cliccare sul documento da scaricare denominato “Modello di comunicazione al Garante - data breach”;
- la documentazione viene inviata anche mezzo e-mail agli indirizzi indicati durante lo svolgimento del flusso;

5. utilizzo del fac-simile di comunicazione di data breach quale bozza di riferimento per la notifica della violazione dei dati personali all’Autorità Garante;
6. invio della notifica della violazione dei dati personali secondo le modalità operative previste dall’Autorità Garante e rese accessibili sul sito ufficiale dell’Autorità al link https://servizi.gpdp.it/databreach/s/;
7. trasmissione al DPO – per conoscenza – del modulo di notifica della violazione dei dati personali;
8. acquisizione in MUA del modulo di notifica della violazione dei dati personali nel seguente modo:
   - accedere alla sezione “Elementi d’analisi” alla voce “Regolamento 679/2016/UE - Data breach”;
   - posizionarsi sulla violazione/incidente inserito;
   - espandere la sezione “File allegati”;
   - cliccare su “Nuovo” e successivamente su “Seleziona il file da allegare”
   - caricare il modulo di notifica della violazione dei dati personali e cliccare su “salva allegati”.

7.3.3 Caso C: incidente da inserire nel registro incidenti, da notificare all’Autorità Garante e da comunicare agli interessati (nel caso in cui la violazione comporti un rischio elevato per i diritti e la libertà delle persone fisiche)

1. Inserimento della violazione nel registro degli incidenti e notifica all’Autorità Garante come da punti da 11.2.1 a 11.2.8;
2. Comunicazione della violazione di dati personali all’interessato.