Schema "Procedura per la gestione delle violazioni dei dati personali (data breach)"

Rev. n.

Allegato D)

Redatto	Verificato	Approvato	Controllato
Paola Salvi Direttore U.O.C Privacy e Internal Audit - Responsabile Protezione Dati Personali (RPD)			

Stato documento: bozza

INDICE

1.	**Presentazione/oggetto**	Pag.
2.	**Scopo**	
3.	**Campo di applicazione**	
4.	**Responsabilità**	
5.	**Riferimenti**	
6.	**Abbreviazioni/ Definizioni**	
7.	**Modalità operative**	
8.	**Registrazione**	

Schema "Procedura per la gestione delle violazioni dei dati personali (data breach)"

Rev. n.

9.	**Archiviazione**	
10.	**Allegati**	
11.	**Lista di distribuzione**	

1. Presentazione /Oggetto

La presente procedura si applica alla violazione dei dati personali consistente in una 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.

2. Scopo

Questo documento descrive le modalità operative adottate dall'Azienda Usl toscana sud est al fine di garantire la gestione delle violazione dei dati personali nel rispetto di quanto previsto dagli art. 33 e 34 del Regolamento (UE) 2016/679 Regolamento Generale sulla Protezione dei Dati – RGPD.
iLa finalità è dimostrare, da parte del Titolare in ottemperanza al principio di responsabilizzazione ("Accountability"),che il trattamento dei dati è effettuato rispettando dei principi della protezione e che sono adottate le misure tecniche e organizzative di sicurezza in conformità al RGPD.

3. Campo di applicazione

Le disposizioni della presente procedura si applicano a tutte le strutture organizzative, in relazione ai compiti istituzionalmente previsti.

Schema "Procedura per la gestione delle violazioni dei dati personali (data breach)"

Rev. n.

4. Responsabilità

La procedura descrive le fasi di attività e i soggetti che in ognuna della diverse fasi intervengono come Responsabile di quella attività (R), come soggetto che collabora (C), come soggetto che deve essere informato al momento dell'esecuzione dell'attività (I) :

Attività/Responsabilità	Titolare	RPD	Preposto	…….	……
……	……	……	……	……	……

R: responsabile di una specifica attività; C: chi collabora ad una specifica attività; I: chi deve essere informato al momento dell'esecuzione dell'attività

5. Riferimenti

- D.Lgs. 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali", art.4, art.33, art.34, Considerando 85,86,87,88;
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016,
- Linee Guida Articolo 29 data Protection Working Party Revisione 6/2/2018
- Provvedimenti del Garante per la protezione dei dati personali

6. Abbreviazioni / Definizioni

Categorie particolari di dati personali (art.9 RGPD): i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Comitato Protezione Dati: organismo tecnico permanente aziendale di natura interdisciplinare con compiti operativi, di supporto e proposta al Titolare di soluzioni ai problemi applicativi del Regolamento (UE) 2016/679 (istituito con Deliberazione……..).

Garante: Autorità Garante per la protezione dei dati personali.

Schema "Procedura per la gestione delle violazioni dei dati personali (data breach)"

Rev. n.

Preposto: Direttore di Unità Operativa che effettua trattamenti di dati personali che effettuano trattamenti dei dati personali, nell'ambito dell'incarico ad esso assegnato e delle attività di competenza, sulla base di compiti e funzioni individuati dal Titolare (Deliberazione…….).

Pseudonimizzazione: trattamento dei dati personali in modo tale che i dati personali non possono essere più attribuiti a un interessato specifico senza l'ausilio di informazioni aggiuntive, che sono conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Responsabile del trattamento: persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta i dati per conto del titolare sulla base di un contratto.

RGPD: Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, "Regolamento Generale sulla Protezione dei dati".

Titolare: persona fisica o giuridica, l'autorità pubblica, il 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 a 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, la distruzione.

Violazione dei dati personali (*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 a dati personali trasmessi, conservati o comunque trattati e da cui possano derivare rischi per i diritti e le libertà degli interessati.

7. Modalità operative

Indice

1 Definizione di violazione dei dati personali o *data breach*
2 Valutazione preliminare del rischio
3 Esiti della valutazione del rischio
4 Notifica della violazione di dati personali
5 Obbligo di comunicazione della violazione di dati personali agli interessati

Schema "Procedura per la gestione delle violazioni dei dati personali (data breach)"

Rev. n.

6 Procedura di gestione della violazione
7 Registro delle violazioni di dati personali
8 Sanzioni
9 Modello per la notifica
10 Norma finale

1 Definizione di violazione dei dati personali o *data breach*

1.1 Per "*data breach*" o «violazione dei dati personali» si intende 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, e da cui possano derivare rischi per i diritti e le libertà degli interessati.

1.2 Possono esemplificarsi, in via non esaustiva, quali *data breach* i seguenti eventi:

- l'accesso abusivo a dati personali contenuti nelle banche dati aziendali;
- la copia abusiva per immagine su supporto informatico di documenti analogici contenenti dati personali;
- la perdita o il furto di attrezzature aziendali quali personal computer, elettromedicali, dispositivi di memorizzazione, ecc… che contengano dati personali;
- attacchi condotti da persone o software che ottengano l'accesso alle banche dati aziendali;
- la cattura di dati di autenticazione e autorizzazione;
- qualsiasi evento che possa determinare o tradursi in accessi indebiti ai dati personali.

2 Valutazione preliminare del rischio

2.1 Per "rischio" di una violazione dei dati personali si intende la proprietà che una violazione di dati ha di poter avere effetti, stimati in termini di probabilità, danno conseguente e rilevabilità, sui diritti e le libertà delle persone cui i dati si riferiscono.

2.2 In presenza di una accertata violazione dei dati personali, il Titolare del trattamento procederà ad effettuare una preliminare valutazione oggettiva - con riguardo alla natura, all'ambito di applicazione, al contesto ed alle finalità del trattamento - della probabilità e gravità dei rischi per i diritti e le libertà delle persone fisiche che possono derivare dal trattamento dei dati personali oggetto di violazione.

2.3 La potenziale gravità di una violazione si valuta prendendo in considerazione anzitutto la tipologia e quantità dei dati oggetto della violazione ed i possibili effetti della violazione stessa.

2.4 Per quanto concerne la tipologia di dati, il Titolare deve accertarsi se sono stati violati dati appartenenti alle particolari categorie di cui all'art. 9 o dati relativi a condanne penali o reati di

cui all'art. 10 del Regolamento UE 2016/679, o relativi a persone fisiche vulnerabili (in particolare pazienti o minori); per quanto riguarda la quantità, se i dati personali violati sono numerosi o sono relativi ad un significativo numero di interessati.

2.5 Per quanto concerne i rischi effetto della violazione, il Titolare deve accertarsi se essa si può tradurre in:

- perdita di riservatezza di dati protetti dal segreto professionale;
- limitazione o privazione dei diritti delle persone fisiche;
- perdita dell'esercizio del controllo dell'interessato sui dati personali;
- discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- qualsiasi altro danno economico o sociale significativo alla persona fisica interessata;

2.6 In sede di valutazione oggettiva dell'effettiva sussistenza del rischio e della sua gravità, deve tenersi conto anche delle circostanze in cui la violazione è avvenuta, ad esempio se i dati siano o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso.

3 Esiti della valutazione del rischio

3.1 Ove risulti improbabile che dalla violazione possa derivare un rischio per i diritti e le libertà degli interessati, il Titolare non procederà alle notifiche all'Autorità Garante per la protezione dei dati personali e alle comunicazioni di cui ai punti 4) e 5) seguenti.

3.2 In tal caso, in adempimento al principio della responsabilizzazione, il Titolare deve poter comunque dimostrare e documentare, per una eventuale verifica, che la violazione dei dati personali non notificata o comunicata non comportava effettivi rischi per i diritti e le libertà degli interessati.

3.3 Ove il Titolare accerti che dalla violazione può derivare un rischio per i diritti e le libertà degli interessati, provvederà alle notifiche e comunicazioni di cui ai punti 4 e 5.

4 Notifica della violazione

4.1 Il Titolare deve notificare il *data breach* all'Autorità Garante per la protezione dei dati personali (di seguito: Garante), secondo le modalità di seguito precisate, ove risulti probabile che dalla violazione possano derivare rischi per i diritti e le libertà degli interessati.

4.2 La notifica al Garante deve essere effettuata senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare ne sia venuto a conoscenza (a seguito di comunicazione da parte del Preposto al trattamento, art. 6, comma 1, o del Responsabile del trattamento, vedi art. 6 comma 2,).

4.3 Il Titolare deve considerarsi venuto a conoscenza di una violazione quando sia in possesso di un ragionevole grado di certezza in merito alle modalità con cui la stessa si è verificata, ottenuto anche a seguito di un'indagine approfondita.

4.4 Il Titolare deve dunque ritenersi, prima della conclusione degli accertamenti, ancora privo di un grado di conoscenza sufficiente, e tale da determinare l'obbligo di notifica, per cui il termine da cui iniziano a decorrere le 72 ore deve individuarsi nel momento in cui il Titolare sia venuto in possesso di una ragionevole certezza su quanto accaduto.

4.5 La fase di accertamento di cui ai punti precedenti non può essere abusata per prorogare illegittimamente il termine di notifica.

4.6 Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore dall'avvenuta conoscenza della violazione, come sopra determinata, è necessario esplicitare i motivi del ritardo.

4.7 La notifica deve almeno:

- 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;
- 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;
- 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.

4.8 Qualora non sia possibile fornire contestualmente tutte le suddette informazioni, queste possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

5 Comunicazione della violazione

5.1 Il Titolare è tenuto a comunicare il *data breach* agli interessati cui i dati si riferiscono, secondo le modalità di seguito precisate, ove risulti probabile che dalla violazione possano derivare elevati rischi per i diritti e le libertà degli interessati.

5.2 La comunicazione all'interessato è successiva a quella al Garante, ma deve essere effettuata senza ingiustificato ritardo, descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni e le misure seguenti:

- 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;
- 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.

5.3 La comunicazione all'interessato non è prevista se è soddisfatta una delle seguenti condizioni:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati (in tal caso si procede a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia).

5.4 Nel caso in cui il Titolare non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, può richiedere che vi provveda, o può decidere che una delle condizioni di cui di cui al comma precedente è soddisfatta.

6 Procedura di gestione della violazione

6.1 Il Preposto al trattamento che sia venuto a conoscenza di una violazione dei dati ne informa il Titolare e il Responsabile della Protezione dei dati, senza ingiustificato ritardo, e comunque entro 24 ore da quando ne è venuto a conoscenza, formalizzando la comunicazione anche a mezzo posta elettronica e allegando alla stessa la scheda evento (allegato D.1) alla presente procedura).

6.2 Ove presente, il Responsabile del trattamento che sia venuto a conoscenza di una violazione dei dati ne informa il Titolare, senza ingiustificato ritardo, e comunque entro 24 ore da quando ne è venuto a conoscenza. con comunicazione da inviarsi all'indirizzo PEC dello stesso Titolare allegando alla comunicazione la scheda evento (allegato D.2) alla presente procedura).

6.3 Il Preposto al trattamento e il Responsabile del trattamento, qualora non procedano a comunicare al Titolare, con le modalità e la tempistica di cui alla presente procedura , la violazione di dati di cui siano venuti a conoscenza, si assumono ogni responsabilità in ordine alla sanzione o al danno che al Titolare possa derivare da tale omissione o ritardo.

6.4 Il RPD non appena ricevuta notizia o formale comunicazione della violazione dei dati, al fine di ricostruire in modo circostanziato l'accaduto e di effettuare la valutazione sulle probabilità e gravità dei rischi per i diritti e le libertà degli interessati che possano derivarne, avvia un'istruttoria provvedendo a riunire e coordinare una Data Breach Unit (DBU) con la composizione minima di seguito indicata:

- RPD
- il Preposto (o i Preposti) al trattamento dati oggetto della violazione;
- il Referente Data Protection di macrostruttura,
- eventualmente, il Responsabile del trattamento;
- ove necessario, il Referente tecnico-informatico designato da Estar, a supporto dell'Azienda, sulle problematiche di sicurezza.

6.5 Il RPD, per integrare l'analisi e la valutazione, ha facoltà di coinvolgere a fini istruttori altre funzioni aziendali responsabili di attività da cui possono derivare ulteriori elementi conoscitivi, le quali devono garantire tempestivamente il supporto richiesto.

6.6 La DBU analizza congiuntamente tute le informazioni raccolte ed effettua la valutazione e la classificazione del rischio come di seguito indicato.

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

- gravità: rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati);
- probabilità: grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati).

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, è possibile considerare i seguenti fattori:

- tipo di violazione (violazione della riservatezza, dell'integrità, della disponibilità)
- natura, sensibilità e volume dei dati personali;
- facilità nella identificazione degli interessati;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati;

- numero degli interessati.

Gravità	**Impatto della violazione sui diritti e le libertà delle persone coinvolte**: ❷ Basso: nessun impatto ❷ Medio: impatto poco significativo, reversibile ❷ Alto: impatto significativo, irreversibile
Probabilità	**Possibilità che si verifichino uno o più eventi temuti** ❷ Basso: l'evento temuto non si manifesta ❷ Medio: l'evento temuto potrebbe manifestarsi ❷ Alto: l'evento temuto si è manifestato

	Gravità			
Probabilità		**A**	**M**	**B**
	A			
	M			
	B			

	Descrizione	**Notifica all'Autorità**	**Comunicazione agli interessati**
Rischio	Basso: nessun pregiudizio sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	NO	NO
	Medio: possibile pregiudizio sui diritti e sulle libertà degli	SI	NO

	interessati e sulla sicurezza dei dati personali coinvolti		
	Alto: pregiudizio certo sui diritti e sulle libertà degli interessati né sulla sicurezza dei dati personali coinvolti	SI	SI

Il RPD cura e documenta l'attività istruttoria, acquisendo tutti gli elementi necessari per l'effettuazione della valutazione.

6.7 All'esito di tale attività, che deve compiersi tempestivamente, il RPD redige un verbale corredato dalla documentazione di supporto e da una proposta operativa da sottoporre al Titolare a mezzo mail. Ove a seguito dell'analisi, venga accertato il breach, è dall'invio della mail che decorre la tempistica prevista dalla normativa per la notificazione al Garante.

6.8 Il RPD redige gli eventuali atti di notifica al Garante e la eventuale comunicazione all'interessato o agli interessati e li sottopone al Direttore Generale, o suo delegato, per la sottoscrizione.

7 Registro sulle violazioni di dati personali

7.1 Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nonché l'eventuale effettuazione della notifica al Garante e della comunicazione agli interessati.

7.2 Ai fini di cui al punto precedente è predisposto e implementato un Registro delle violazioni dei dati personali (allegato D.3) alla presente procedura).

7.3 E cura del RPD tenere, in ordine cronologico, il Registro delle violazioni dei dati personali e la correlata documentazione.

8 Sanzioni

8.1 In caso di mancato rispetto delle disposizioni in materia di violazione dei dati personali si applicano le sanzioni amministrative pecuniarie di cui all'art. 83 paragrafo 4 lettera a) del RGPD, fino ad un importo massimo di 10 milioni di euro.

9 Modello per la notifica

9.1 La notificazione della violazione dei dati è effettuata utilizzando il modello allegato D.4) alla presente procedura da inviarsi in modalità telematica all'indirizzo protocollo@pec.gpdp.it

10 Norma finale

10.1 Per tutto quanto non espressamente previsto nella presente procedura, si rinvia alla vigente normativa.

10.2 La presente procedura è pubblicata nella sezione "Privacy in Azienda" del sito web istituzionale dell'Azienda.

10.3 La presente procedura sarà soggetta a modifiche e integrazioni che si renderanno necessarie in adeguamento a disposizioni normative intervenute successivamente all'approvazione della procedura stessa o a pronunciamenti, linee guida e provvedimenti del Garante.

8. Registrazione

Il registro delle violazioni dei dati personali è tenuto dal Responsabile della protezione dei dati personali e a disposizione del Garante in sede di verifica.

9. Archiviazione

L'originale della presente procedura è archiviato presso il Responsabile della Protezione dei Dati Personali.

10. Allegati

1. Scheda segnalazione evento per Preposto al trattamento
2. Scheda segnalazione evento per Responsabile del trattamento
3. Registro violazioni
4. Modello notifica

Schema "Procedura per la gestione delle violazioni dei dati personali (data breach)"

Rev. n.

11. Lista di Distribuzione

- Direzione Aziendale
- Tutte le Unità Operative aziendali