REGIONE DEL VENETO
ULSS8 BERICA

Servizio Sanitario Nazionale - Regione Veneto
AZIENDA ULSS N. 8 BERICA
Viale F. Rodolfi n. 37 – 36100 VICENZA
COD. REGIONE 050–COD. U.L.SS.508 COD.FISC. E P.IVA 02441500242–Cod. iPA AUV
Tel. 0444 753111 - Fax 0444 753809 Mail protocollo@aulss8.veneto.it
PEC protocollo.centrale.aulss8@pecveneto.it

www.aulss8.veneto.it

Valutazione degli incidenti di sicurezza e gestione delle eventuali violazioni (Data Breach)

Linee guida metodologiche

trasmesse da AZIENDA ZERO

(nota 17.12.2018 prot. 16336) come recepite da U.L.SS. n. 8 Berica

(con apposito atto deliberativo)

INDICE

1. Premessa di carattere organizzativo e metodologico

Ogniqualvolta nel presente documento, a seguito di specifico riferimento normativo, sia indicato quale soggetto il "Titolare del trattamento" si faccia riferimento, per lo svolgimento dei diversi adempimenti, al soggetto e/o alla struttura aziendale individuata dal Titolare del trattamento *ratione materiae* ed in base all'organizzazione dettata dall'Atto Aziendale, così come riportato nella tabella di cui al paragrafo 5 "Ruoli e Responsabilità": tabella che dovrà essere quindi completata, da ciascuna Azienda, tenendo conto del proprio, peculiare assetto organizzativo, nonché delle eventuali deliberazioni aziendali già assunte in materia di "privacy europea" per far fronte agli obblighi di cui al GDPR.

Ciò detto, al fine di applicare efficacemente le presenti linee guida, ciascuna Azienda, nel caso in cui non lo avesse già fatto, individuerà preliminarmente le strutture aziendali che dovranno concorrere all'attuazione degli adempimenti oggetto del presente documento, in ragione della natura degli adempimenti medesimi *(a titolo esemplificativo e non esaustivo: verranno distinti gli obblighi di carattere giuridico da quelli di carattere tecnologico ed informatico, piuttosto che da quelli afferenti all'area statistica, di internal auditing o di controllo di gestione, o altro).*

Al fine di dare attuazione alle suesposte indicazioni di Azienda Zero, questa U.L.SS. n. 8 ha approvato l'atto deliberativo del direttore generale ad oggetto: ***"Privacy europea: approvazione del nuovo PIANO OPERATIVO DI DISTRIBUZIONE DELLE COMPETENZE all'interno dell'ULSS n. 8 Berica al fine di recepire le indicazioni fornite da Azienda Zero per l'attuazione del GDPR"***.

Secondo il *"Piano operativo"* anzidetto e per quanto concerne l'applicazione delle presenti Linee Guida, la competenza è posta in capo al **Delegato Interno al trattamento dei dati** (Direttore UOC o UOSD dell'Azienda ove è avvenuto l'incidente di sicurezza, cioè la presunta violazione della privacy), al quale compete l'istruttoria sull'incidente di sicurezza e la valutazione di prima istanza.

Al **Nucleo di valutazione ristretto** (organismo collegiale) dell'Azienda spetta la valutazione di seconda istanza, e al Direttore Generale (Titolare del trattamento) la decisione finale e la notifica al Garante della privacy.

Per i dettagli della procedura e dei compiti assegnati si fa espresso rinvio al contenuto del precitato *"Piano operativo"* approvato con atto deliberativo del direttore generale.

2. Introduzione e ambito di applicazione

La presente procedura definisce le linee di comportamento da seguire, adottate dall'Azienda ULSS n. 8 Berica (d'ora in avanti "Azienda") e indica ruoli, responsabilità, tempistiche e modalità di comunicazione di eventuali violazioni di riservatezza, d'integrità e disponibilità dei dati personali al Garante *privacy* e, ove necessario, a tutti gli Interessati i cui dati personali sono oggetto di violazione.

2.1. Riferimenti normativi

La procedura è redatta tenendo in considerazione i requisiti di cui al Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito *Regolamento*) e, nello specifico, gli articoli 33 e 34, nonché le *Guidelines on Personal Data Breach Notification under Regulation* 2016/679 (wp250rev.01) del WP29.

3. Definizioni

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.

Responsabile del trattamento (Art. 4, n. 8, del Regolamento): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Interessato: la persona fisica identificata o identificabile **(Art. 4, n. 1, del Regolamento)** 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): 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. Ai sensi del Decreto commissariale di Azienda Zero n. 157/2018, ad oggi, risulta nominato un unico RPD (persona fisica) per le Aziende SSR del Veneto.

4. Destinatari

La procedura è emanata a favore di tutti i dipendenti e collaboratori a vario titolo coinvolti nel trattamento di dati personali.

5. Ruoli, Responsabilità e Interazioni

Come già delineato all'articolo n. 1, al fine di dare attuazione alle indicazioni di Azienda Zero, questa U.L.SS. n. 8 ha approvato l'atto deliberativo del direttore generale ad oggetto: ***"Privacy europea: approvazione del nuovo PIANO OPERATIVO DI DISTRIBUZIONE DELLE COMPETENZE all'interno dell'ULSS n. 8 Berica al fine di recepire le indicazioni fornite da Azienda Zero per l'attuazione del GDPR"***, a cui si fa espresso ed integrale rinvio.

6. Attività operative

Le fasi di attività connesse alla gestione di eventuali violazioni di riservatezza dei dati (*Data Breach*) si sostanziano in:

1. Rilevazione / Valutazione;
2. Gestione;
3. Notifica al Garante per la protezione dei dati personali;
4. Comunicazione agli Interessati (ove necessario);
5. Pianificazione di Audit Interni;
6. Archivio della documentazione.

6.1 Rilevazione / Valutazione del *Data Breach*

Ai sensi dell'art. 4 n. 12) del Regolamento UE si intende per *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.
Il Gruppo di Lavoro Articolo 29 per la protezione dei dati, nella *Opinion* 03/2014, ha identificato alcuni tipi di *Data Breach*[1].

In particolare, può trattarsi di:

- "***violazione della riservatezza***": in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "***violazione dell'integrità***": in caso di alterazione non autorizzata o accidentale dei dati personali;
- "***perdita della disponibilità***": in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata).

A titolo esemplificativo, si riportano alcuni eventi di violazione dei dati personali per le quali è necessario avviare la procedura:

- perdita o furto di PC o Smartphone aziendali;
- perdita di supporti mobili quali *pen-drive* USB o *hard disk* aziendale;
- perdita di fascicoli cartacei o altra documentazione aziendale;
- invio erroneo di comunicazioni/informazioni verso l'esterno;
- attacchi informatici ai sistemi aziendali;
- accesso a dati da parte di persona non autorizzata.
- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o sia loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono stati violati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- se sono stati violati dati afferenti alla valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali,

[1] Per ulteriori approfondimenti si veda: Gruppo di Lavoro Articolo 29 per la protezione dei dati, Opinion 03/2014.

l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se la violazione afferisce a un numero rilevante di dati;
- se l'evento riguarda il trattamento di dati personali di persone fisiche vulnerabili, in particolare minori.

Qualsiasi persona autorizzata al trattamento in Azienda, ogni qualvolta rilevi un avvenuto o potenziale *Data Breach*, ha la responsabilità di portare l'avvenimento immediatamente all'attenzione del Titolare del trattamento.
La comunicazione al Titolare del trattamento della violazione dei dati personali dovrà pervenire via posta elettronica all'indirizzo istituzionale di questa Azienda ULSS n. 8 (MAIL: protocollo@aulss8.veneto.it / PEC: protocollo.centrale.aulss8@pecveneto.it).
Parimenti, qualora la rilevazione avvenga a cura di un soggetto terzo esterno all'organizzazione (es. Responsabile del trattamento), questi informa il Titolare del trattamento senza ingiustificato ritardo, ai sensi dell'art. 33 comma 2 Regolamento (UE), con le medesime modalità di cui sopra.
Il Titolare del trattamento, avuta notizia dell'avvenuto o potenziale *Data Breach*, avvia l'istruttoria per l'identificazione dell'evento, informando del caso il personale delegato di competenza in relazione alla questione e coinvolgendo eventualmente anche il Referente aziendale ICT.
In questa fase, il Titolare del trattamento ha la possibilità di consultare il RPD per funzioni di indirizzo, utilizzando apposita modulistica *(allegato 1)* e, comunque, nel rispetto delle condizioni disciplinate dal Regolamento di funzionamento del RPD.
Il Titolare del trattamento procede alla compilazione del *Registro Interno delle Violazioni (allegato 2)* indipendentemente dalle notifiche che saranno effettuate all'Autorità di controllo. Tale registro ha la funzione di documentare le valutazioni effettuate circa l'identificazione del *Data Breach*.

6.2 Gestione del *Data Breach*

Il Titolare del trattamento, laddove necessario o opportuno, procede nella gestione del *Data Breach* raccogliendo le informazioni necessarie alla descrizione dell'evento, delle misure tecniche e organizzative analogiche e/o digitali adottate e di quelle di possibile adozione per porre rimedio alla violazione e/o per attenuarne i possibili effetti negativi; ciò al fine di poter procedere nella compilazione della modulistica per la notifica al Garante.

Infine, valuta la possibilità che la violazione presenti un rischio per i diritti e le libertà degli interessati, avvalendosi del supporto del RPD nei casi di particolare complessità, per ricevere indicazioni di indirizzo.
Qualora il Titolare del trattamento dovesse ritenere non opportuno notificare la violazione di riservatezza dei dati, è necessario che le motivazioni sottostanti a tale decisione siano documentate all'interno del sopracitato *Registro Interno delle Violazioni.* A tale proposito, occorrerà descrivere i motivi per cui il Titolare del trattamento ha ritenuto che la violazione non costituisse fattore di rischio per i diritti e le libertà degli individui.

Ai fini della gestione del *Data Breach* occorre considerare se:

- i dati siano stati in precedenza resi anonimi oppure pseudonimizzati;
- i dati siano stati oggetto di cifratura e se fosse garantita, al momento della violazione, la riservatezza della chiave di decifratura;
- i dati violati non siano riconducibili all'identità di persone fisiche;
- i dati siano già stati oggetto di pubblicazione;
- l'evento non costituisca un *Data Breach.*

6.3 Notifica al Garante per la protezione dei dati personali

Ai sensi dell'art. 33 del Regolamento, la notifica del *Data Breach* all'Autorità di controllo è sempre obbligatoria, salvo i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Alla comunicazione effettuata dal Titolare del trattamento dovrà essere allegata anche dettagliata relazione, comprensiva di tutti gli elementi informativi e delle valutazioni in merito effettuate.
Qualora il Titolare del trattamento ed il RPD (eventualmente consultato) abbiano opinioni discordanti circa l'insussistenza del rischio per i diritti e le libertà degli interessati, la decisione sull'opportunità di notificare la violazione dei dati personali al Garante per la protezione dei dati personali ricadrà unicamente sul Titolare del Trattamento e dovrà essere debitamente motivata.
Laddove, invece, venga rilevato ed accertato un effettivo rischio per i diritti e le libertà degli interessati, il Titolare del trattamento dovrà effettuare la notifica all'Autorità Garante. In particolare, il Titolare del trattamento, utilizzando il *format* e le procedure previste dall'Autorità Garante, dovrà notificare la violazione all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui sia venuto a conoscenza dell'accertata violazione con il verificarsi di un effettivo, comprovato "rischio" nei termini sopra descritti.
Contestualmente è inoltrata dal Titolare del trattamento comunicazione scritta al RPD di avvenuta notifica al Garante, per mettere il medesimo a conoscenza dell'istruttoria in atto.
Se non fosse possibile fornire tutte le informazioni contestualmente, queste ultime potranno essere inviate in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non sono disponibili.
In questo caso sarà cura del Titolare del trattamento raccogliere le informazioni mancanti e procedere, senza ritardo, alle integrazioni eventualmente necessarie avvalendosi della collaborazione delle funzioni interessate che, a tal fine, dovranno prestare pronta, piena e fattiva disponibilità.
La mancata collaborazione delle risorse coinvolte assume rilevanza a fini disciplinari.
Ai sensi dell'art. 33 del Regolamento, la notifica all'Autorità di controllo deve contenere almeno i seguenti contenuti:

a) descrizione della 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) comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) descrizione delle 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.

6.4 Comunicazione agli Interessati

Nel caso in cui la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvede alla comunicazione di detta violazione agli interessati coinvolti, senza ingiustificato ritardo, dandone comunicazione per conoscenza al RPD.
La comunicazione agli interessati deve descrivere, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e deve contenere almeno le seguenti informazioni:

a) la descrizione delle probabili conseguenze della violazione dei dati personali;
b) la descrizione delle 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;
c) nome e dati di contatto del RPD.

Ai sensi dell'art. 34, comma 3, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto 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;
b) 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;
c) detta comunicazione richiederebbe sforzi sproporzionati; in tal caso, è necessario procedere a una comunicazione pubblica, ovvero a una misura simile alternativa, tramite la quale gli Interessati sono informati con analoga efficacia.

Nel caso in cui sia il Garante per la protezione dei dati personali a ordinare con provvedimento la comunicazione del *Data Breach* agli interessati, il Titolare del trattamento pone in essere tutte le attività necessarie per ottemperare al provvedimento.

6.5 Pianificazione degli *audit*

Il Titolare del trattamento prevede, all'interno del proprio piano di *audit*, con cadenza almeno biennale, una verifica sulla tenuta del Registro interno delle violazioni e delle segnalazioni di violazione dei *Data Breach*.

6.6 Archiviazione

Il Titolare del trattamento, conclusa la procedura, archivia tutte la documentazione relativa al procedimento, incluse le notifiche trasmesse al Garante per la protezione dei dati personali e agli interessati, nonché il Registro interno delle violazioni debitamente aggiornato. Il RPD potrà accedere al Registro interno delle violazioni in qualsiasi momento.

7 Modulistica allegata alla procedura

Allegato 1_Modulo di richiesta consulenza al RPD
Allegato 2_Registro interno delle violazioni

8 Modifiche al presente documento

Eventuali modifiche al presente documento avranno efficacia dal momento della loro pubblicazione e si applicheranno alle nuove fattispecie di *Data Breach* che si manifesteranno, eventualmente, dopo tale efficacia, salva diversa disposizione.

***

Data Breach – Allegato 1

Data, _____ Prot.n. _____

Al Responsabile della Protezione dei Dati
Avv. Piergiovanni Cervato
E-mail: rpd_ssrveneto@cervato.it

Oggetto: Richiesta consulenza al RPD per *Data Breach*

Il sottoscritto ..... in qualità di .....
dell'Azienda Sanitaria .....
contatto telefonico ..... e-mail .....
fornisce le seguenti indicazioni relative alla presunta violazione dei dati personali, oggetto di consulenza:

QUESITO *(descrizione di alcuni elementi utili alla definizione della risposta):*

Data rilevazione della presunta violazione.....

Natura e tipologia della presunta violazione:
.....
.....
.....

Soggetti coinvolti:
.....
.....

Informazioni raccolte:
.....
.....

Azioni sviluppate:
.....
.....
.....

Azioni che il Titolare intenderebbe adottare:
.....
.....
.....

Quesito:
.....
.....
.....

Firma .....

Allegato 2 - Registro Interno delle Violazioni
"Procedura di Gestione e Notifica Data Breach"

Registro Interno delle Violazioni

---------- FORMAT che è possibile utilizzare ----------

ID	Soggetto registrante	Data segnalazione	Data Inizio Disservizio	Data Fine Disservizio	Durata hh:mm	Descrizione dell'evento	Impatti Verificatisi	Misure di mitigazione del rischio
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								