Gestione e Notifica del Data Breach

Autore	Dott.ssa Lisa Furlanis –referente aziendale privacy
Approvazione dei contenuti:	Direzione strategica
Validazione	Responsabile internal auditing

Emissione	uoc affari generali
Distribuzione	Tutte le uu.oo./pubblicazione sito internet
Archiviazione	Uoc affari generali/sito internet
Revisione	uoc affari generali

INDICE

1. INTRODUZIONE ED AMBITO DI APPLICAZIONE

La presente procedura definisce le linee guida di comportamento da seguire, adottate dall'azienda ulss n. 4 "Veneto Orientale" ed indica i 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.

1.1. RIFERIMENTI NORMATIVI

La presente procedura viene 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 artt. 33 e 34.

2. 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 ed i mezzi di trattamento di dati personali; quando le finalità e i mezzi di trattamento determinati dal diritto dell'Unione o dagli Stati Membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o dagli 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 ed applicate a dati personali o insieme 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 l'interconnessione, la limitazione, la cancellazione o la distruzione.

Violazione dei dati personali /Data breach (art. 4 n. 2 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 a dati personali trasmessi, conservati o comunque trattati.

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

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

3. DESTINATARI

La procedura è emanata a cura dell'azienda ulss n. 4 "Veneto Orientale" a favore di tutti i dipendenti e i collaborati a vario titolo coinvolti nel trattamento dei dati personali.

4. RUOLI E RESPONSABILITA'

La tabella propone una sintesi delle attività riconducibili a ciascuna risorsa, sia interna che esterna all'azienda, coinvolta nel processo del Data Breach.

Legenda: (R=responsabile diretto/I= informato/C=collaborazione/FI=funzione di indirizzo)

		Titolare del trattamento	Responsabile del Trattamento (se coinvolto)	Responsabile della Protezione dei dati
FASE ATTIVITA'	Rilevazione	I (uoc affari generali e unità supporto privacy	R	FI
	Valutazione	R	C	FI
	Gestione	R (uoc affari generali/uoc sistemi informativi/unità supporto pirvacy)	C	FI
	Notifica al Garante	R (uoc affari generali)	I	I
	Comunicazione agli interessati	R (uoc affari generali)	I	I
	Audit interni	R (uoc affari generali avvalendosi del controllo interno)		I
	Archivio della documentazione	R (uoc affari generali)		

5. ATTIVITA' OPERATIVE

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

- Rilevazione/Valutazione;
- Gestione;
- Notifica al Garante per la protezione dei dati personali;
- Comunicazione agli interessati (ove necessario);
- Pianificazione di Audit Interni;
- Archivio della documentazione.

5.1. RILEVAZIONE /VALUTAZIONE DEL DATA BREACH

Ai sensi dell'art. 4, n. 12 del Regolamento 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.

Qualsiasi persona autorizzata al trattamento in azienda, ogniqualvolta 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 di dati personali dovrà pervenire all'indirizzo di posta elettronica privacy@aulss4.veneto.it.

Parimenti, qualora la rilevazione avvenga a cura di un soggetto terzo esterno all'organizzazione, questi informa il Titolare del trattamento senza ingiustificato ritardo, ai sensi dell'art. 33 comma del 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 gestione e coinvolgendo eventualmente anche il referente aziendale privacy.

In questa fase, il Titolare ha la possibilità di consultare il RPD per le funzioni di indirizzo, utilizzando apposita modulistica (allegato 1).

Il Titolare del trattamento procede alla compilazione del Registro Interno delle Violazioni (allegato 2) indipendente 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.

5.2. 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 e porre rimedio alla violazione e/o per attenuare 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 in indirizzo.

Qualora il Titolare del trattamento dovesse ritenere non opportuno notificare la violazione di riservatezza dei dati, è necessario che le motivazioni sottostanti tale decisione siano documentate all'interno del sopra citato Registro Interno della 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 sono riconducibili all'identità delle persone fisiche;
- i dati siano già stati oggetto di pubblicazione;
- l'evento non costituisca un Data Breach.

5.3. 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 una dettagliata relazione, comprensiva di tutti gli elementi informativi e delle valutazioni in merito effettuate.

Qualora il Titolare del trattamento e il RPD (eventualmente consultato) abbiano opinioni discordanti circa l'insussistenza del rischio per 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 e dovrà essere debitamente motivata.

Laddove, invece, sia rilevato un 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.

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 ai 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.

5.4. 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 a tutti gli 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) il nome e i 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 ed 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 ad 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.

5.5. PIANIFICAZIONE 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 del Data Breach.

6. ARCHIVIAZIONE

Il Titolare del trattamento, conclusa la procedura, archivia tutta 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

All. 1: Modulo di richiesta consulenza al RPD
All. 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.

REGIONE DEL VENETO

ULSS4 VENETO ORIENTALE

All. 1

RICHIESTA DI CONSULENZA AL RPD PER DATA BREACH

Il/La sottoscritto/a .....in qualità .....di.....dell' Azienda Sanitaria ..... contatto telefonico.....e il.....

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 rivelazione della presunta violazione .....

Natura e tipologia della presunta violazione:

.....
.....
.....

Soggetti coinvolti:

.....
.....
.....

Informazioni raccolte:

.....
.....
.....

Azioni sviluppate:

.....
.....
.....

Azioni che il titolare intenderebbe adottare

.....
.....
.....

Quesito

.....
.....
.....

REGIONE DEL VENETO

ULSS4 VENETO ORIENTALE

All. 2

REGISTRO INTERNO DELLE VIOLAZIONI

ID	Soggetto Registratore	Data Segnalazione	Data inizio Disservizio	Data fine Disservizio	Durata hh:mm	Descrizione dell'evento	Impatti Verificatesi	Misure di Migrazione del Rischio
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								