ASL Salerno
Azienda Sanitaria Locale Salerno

# PROTOCOLLO AZIENDALE PRIVACY

# IN MATERIA DI DATA BREACH

# INDICE

**ALLEGATI**

All. 1 – Modulo di segnalazione di un potenziale *data breach*

All. 2 – Registro *data breach*

## TITOLO I

## DATA BREACH

### ART. 1 – DEFINIZIONI

La presente *policy* definisce i principi, le azioni e le procedure volte alla corretta gestione della risposta ad una violazione di dati (*data breach*) e all'adempimento degli obblighi di notificazione all'Autorità di Controllo e di comunicazione ai singoli interessati, come richiesto dal *General Data Protection Regulation* (GDPR).

La procedura deve essere portata a conoscenza di tutti i dipendenti, anche temporanei, dell'Azienda Sanitaria Locale Salerno (ASL Salerno), collaboratori, fornitori e terzi che lavorano e/o agiscono per conto dalla suddetta Azienda, i quali sono tenuti a seguirla in caso di violazione dei dati personali.

Si precisa che l'evento di *data breach* consiste in una violazione di sicurezza che comporta accidentalmente o in modo volontario e illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati dal Titolare.

La violazione dei dati personali può distinguersi in tre categorie:

- "*confidentiality breach*": in caso di divulgazione o accesso non autorizzato o accidentale a dati personali;
- "*availability breach*": in caso di alterazione non autorizzata o accidentale dei dati personali;
- "*integrity breach*": in caso di modifica non autorizzata o accidentale di dati personali.

La presente *policy* si applica nel caso in cui vi sia violazione del dato personale di qualsivoglia natura attinente ad interessati residenti negli Stati Membri dell'Unione Europea (UE) e negli Stati membri dello Spazio Economico Europeo (SEE).

Si riportano di seguito le definizioni tratte dall'articolo 4 del GDPR:

"**Dato Personale**": 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;

"**Dato relativo alla Salute**": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rilevano informazioni relative al suo stato di salute;

"**Titolare del trattamento**": 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 del trattamento di dati personali.

"**Responsabile del trattamento**": una persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Controllore.

"**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.

"**Violazione dei Dati Personali**"**:** 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.

"**Autorità di Controllo**": l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE.

## ART. 2 – FONTI

1. GDPR (Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE);
2. Nuovo Codice Privacy (D. Lgs. 196 del 2003 come novellato dal D. Lgs. 101 del 2018);
3. Linee guida pubblicate dal WP-29 in data 3 ottobre 2017 e riviste in data 6 febbraio 2018;
4. Linee guida pubblicate dal EDPB in data 14 dicembre 2021, n. 01/2021;
5. FAQ pubblicate dal Garante per la Protezione dei Dati Personali (GPDP).

## TITOLO II

## OBBLIGHI CONNESSI AD UNA VIOLAZIONE DEI DATI

### ART. 3 – NOTIFICA E COMUNICAZIONE

In caso di *data breach*, il Titolare del trattamento deve effettuare la notificazione della violazione dati personali al Garante per la protezione dei dati personali, ai sensi dell'art. 33 GDPR. Inoltre, sempre il Regolamento europeo distingue la notifica da rivolgere all'Autorità Privacy in tutti i casi in cui vi sia stata effettivamente una violazione dei dati personali dalla comunicazione agli interessati *ex* art. 34 GDPR.

Il suddetto adempimento è volto a comunicare agli interessati il sinistro privacy occorso, qualora il rischio per i diritti e le libertà delle persone fisiche, derivante da tale violazione, venga valutato come alto; in caso di rischio basso, nonché nei casi prestabiliti dal paragrafo 3 dell'art. 34 GDPR, al contrario, non si procederà con la comunicazione agli interessati.

Si riporta di seguito il testo del paragrafo 3 dell'art. 34 GDPR:

"*Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:*

a) *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;*
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 di cui al paragrafo 1;*
c) *detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.*

### ART. 4 – NOTIFICA AL GARANTE DEL *DATA BREACH*

Il GDPR specifica vari aspetti relativi alle violazioni di dati personali, la notifica di queste al Garante per la Protezione dei Dati Personali, i soggetti destinatari dell'obbligo di comunicazione, le tempistiche, le modalità, nonché le sanzioni previste in caso di inosservanza della normativa. La notificazione deve essere effettuata dal Titolare del trattamento in modo chiaro e specifico, nel più breve tempo possibile (entro le 72 ore dalla conoscenza dell'incidente, altrimenti si dovrà giustificare l'eventuale ritardo) e come sancito dall'art 33, par. 3 GDPR, che qui si riporta integralmente, deve:

a) *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;*
b) *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;*
c) *descrivere le probabili conseguenze della violazione dei dati personali;*
d) *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.*

Qualora non sia possibile fornire tutte le suddette informazioni contestualmente alla notifica, quest'ultima dovrà essere integrata, mediante l'apposito *format* predisposto dal Garante anche in fasi successive, con i dati e le notizie mancanti, senza ulteriore ingiustificato ritardo.

Infatti, all'inizio del *format* presente sulla pagina del Garante Privacy si dovrà indicare se si tratta di una notificazione **preliminare** (sia essa conclusiva o meno), oppure **integrativa** (conclusiva o volta a dare ulteriori informazioni senza chiudere il *data breach*).

Infine, il Titolare del trattamento dovrà informare e coordinarsi con il DPO in merito ad ogni notifica effettuata al Garante.

## ART. 4*bis* – NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI AL TITOLARE DEL TRATTAMENTO DA PARTE DELL'AZIENDA SANITARIA LOCALE SALERNO, NELLA QUALITÀ DI RESPONSABILE DEL TRATTAMENTO

Se la violazione o la sospetta violazione riguarda i dati personali che vengono trattati dalla ASL Salerno, in qualità di Responsabile del Trattamento, per conto di terzi, Titolari del trattamento, il Gruppo di Risposta (di cui all'art. 8 del presente regolamento) comunica senza ritardo a quest'ultimo soggetto:

- una descrizione della natura della violazione;
- le categorie dei dati personali violati;
- il numero, anche approssimativo, degli interessati;
- il nome e le informazioni di contatto dei componenti del Gruppo di Risposta;
- le conseguenze della violazione dei dati personali;
- le misure adottate per gestire la violazione dei dati personali;
- qualsiasi informazione utile relativa alla violazione dei dati.

La ASL Salerno, anche in questo caso, deve registrare nel proprio Registro delle Violazioni dei dati, allegato alla presente *policy*, i sinistri occorsi in qualità di Responsabile del trattamento.

## ART. 5 – COMUNICAZIONE AGLI INTERESSATI

Come prescritto dall'art. 34 del GDPR, quando la violazione dei dati è suscettibile di presentare un **rischio elevato** per i diritti e le libertà delle persone fisiche, la ASL Salerno, in qualità di Titolare del trattamento, comunicherà **senza ingiustificato ritardo** la violazione all'interessato, anche al fine di consentirgli l'adozione di idonee precauzioni volte a ridurre al minimo il potenziale danno derivante dalla violazione dei suoi dati.

La comunicazione all'Interessato dovrà descrivere, con linguaggio **semplice e chiaro**, in maniera evidente e trasparente l'accaduto, e dovrà contenere almeno gli elementi indicati dall'art. 33, par. 3, lett. b), c) e d) GDPR, che di seguito si riportano integralmente:

b) "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;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) 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.

Nel caso in cui il Titolare non abbia comunicato all'interessato la violazione dei dati, l'Autorità di controllo può **ingiungere**, dopo aver valutato la probabilità che tale violazione presenti un rischio elevato, che il Titolare vi provveda o può decidere che una delle condizioni descritte all'ultimo capoverso dell'art. 3 "*Notifica e comunicazioni*" della presente *policy* sia soddisfatta e, pertanto, la comunicazione anche se presenta un rischio elevato non verrà comunicata agli interessati.

## TITOLO III

## PROCEDURA DI RISPOSTA ALLA VIOLAZIONE

### ART. 6 – GRUPPO DI RISPOSTA ALLA VIOLAZIONE DEI DATI

Il Gruppo di Risposta alle Violazioni dei Dati personali (di seguito "Gruppo") è costituito da più persone interne alla ASL Salerno, esperte e competenti nei diversi settori di cui è composto l'Ente.

Salerno

Tale Gruppo si compone delle seguenti figure:

- Direttore Generale o suo Delegato;
- Referente Privacy ASL Salerno;
- Direttore della Struttura (designato al trattamento dei dati) in cui si è verificato il *Data Breach*
- Direttore UOC SIA.

Il Gruppo, in linea con il principio di *privacy by design*, è istituito ed è operante a prescindere dal fatto che una violazione sia o meno avvenuta.

Il Gruppo fornisce una risposta immediata ed efficace a qualsiasi sospetta/ presunta o effettiva violazione dei dati personali che riguardi l'Azienda. A tal fine, i componenti del Gruppo sono individuati tra i soggetti che garantiscono la preparazione necessaria per adempiere all'incarico conferito. Al Gruppo sono assegnate risorse adeguate allo svolgimento del proprio incarico.

Il Gruppo può trattare più di una violazione dei dati personali presunta o effettiva alla volta.

Il Titolare del trattamento può scegliere di inserire personale aggiuntivo o coinvolgere parti esterne (es. fornitore di sicurezza informatica, periti di informatica forense, ecc.) allo scopo di gestire una specifica violazione dei dati personali.

Il Gruppo è incaricato di rispondere ad ogni violazione dei dati personali, presunta o effettiva, 24 ore su 24, 7 giorni su 7, per tutto l'anno.

### ART. 7 – COMPITI DEL GRUPPO DI RISPOSTA ALLE VIOLAZIONI DEI DATI

Il Gruppo si riunisce, anche da remoto, a seguito di segnalazioni di violazione dei dati personali, presunta o effettiva, comunicata da qualsivoglia soggetto; infatti, potrebbe accadere che la presunta o effettiva violazione venga comunicata da un interessato, da un Responsabile del trattamento, nonché da un dipendente della ASL Salerno.

Inoltre, il Gruppo è coordinato dal Titolare del trattamento e, ove il rischio per i diritti e le libertà delle persone fisiche risulti elevato, chiede un parere al *Data Protection Officer* (DPO).

Il Gruppo:

- valuta il livello di rischio derivante dalla violazione dei dati personali;
- identifica i requisiti per la risoluzione della violazione e ne monitora la concreta applicazione.

Il Titolare del trattamento, nello svolgimento della sua funzione di coordinamento:

- se necessaria, assicura che sia avviata e documentata un'indagine;
- riferisce i risultati al DPO;
- provvede al coordinamento con le autorità competenti se necessario (AgID e CSIRT, ecc.);
- coordina le comunicazioni interne ed esterne;
- garantisce che gli interessati siano adeguatamente informati, se necessario.

**Art. 7*bis* – VALUTAZIONE PRELIMINARE DEL RISCHIO**

Una violazione dei dati può, se non affrontata in modo tempestivo, provocare danni fisici, materiali o immateriali, oltre che reputazionali alle persone fisiche, anche molto gravi.

In presenza di un'avvenuta e accertata violazione dei dati, la ASL Salerno, in qualità di Titolare del Trattamento, procederà subito a effettuare una preliminare valutazione oggettiva sulle **probabilità** e **gravità dei rischi** per i diritti e le libertà delle persone fisiche che possono derivare dai trattamenti illeciti, prendendo in esame la natura, l'ambito di applicazione, il contesto e le finalità del trattamento.

In particolare, il Gruppo di Risposta dovrà considerare i seguenti impatti, come descritti anche dal Garante per la Protezione dei Dati Personali:

- limitazione o privazione dei diritti degli interessati;
- perdita di controllo dei dati personali dell'interessato;
- discriminazioni;
- furto d'identità;
- perdite finanziarie;
- frodi;
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale;
- conoscenza da parte di terzi non autorizzati;
- qualsiasi altro danno economico o sociale significativo;
- danni fisici e psicologici.

Inoltre, il Gruppo esaminerà:

- se sono trattati dati personali "particolari" *ex* art. 9 GDPR che, per loro natura, sono maggiormente sensibili;
- in caso di violazione di aspetti personali che possono fornire dettagli sulle caratteristiche, abitudini, stili di vita, relazioni personali, stato di salute, situazione economica, affidabilità, comportamento, ubicazione o spostamenti dell'interessato al fine di cercare o utilizzare profili personali;
- se sono trattati dati di persone fisiche vulnerabili, in particolare i minori;
- se il trattamento riguarda una notevole quantità di dati o un vasto numero di interessati.

Inoltre, in sede di valutazione oggettiva della effettiva sussistenza del rischio e della sua gravità, ai fini dell'assolvimento dell'**obbligo di notifica** delle violazioni dei dati, si terrà debitamente conto anche delle circostanze di tale violazione, quali ad esempio:

- se i dati personali fossero o no protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso;
- se esistono legittimi interessi delle autorità incaricate all'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze della violazione dei dati.

## ART. 8 – ESITI DELLA VALUTAZIONE DEL RISCHIO

In relazione ai diversi esiti che possono derivare dalla valutazione preliminare del rischio, si potranno verificare le seguenti conseguenze:

- ove risulti probabile che dalla violazione dei dati possano derivare rischi per le libertà e i diritti dell'interessato bisogna immediatamente notificare il *data breach* all'Autorità Garante;
- ove risulti probabile che dalla violazione dei dati possano derivare **elevati** rischi per le libertà e i diritti dell'interessato, si dovrà:
    A. notificare il *data breach* all'Autorità Garante *ex* art. 33 GDPR e
    B. comunicare il *data breach* all'interessato cui si riferiscono i dati violati, ai sensi dell'art. 34 GDPR.
- ove risulti improbabile che dalla violazione dei dati possano derivare rischi per le libertà e i diritti dell'interessato, il Titolare del trattamento **NON** procederà con la notifica all'Autorità né ad alcuna comunicazione all'interessato. In tal caso risulta fondamentale e necessario richiedere un parere al DPO.

Conformemente al principio di "*accountability*", dunque la ASL Salerno è esentata dall'effettuare la notifica solo se è in grado di dimostrare al Garante che la violazione dei dati non presenta rischi per i diritti e le libertà fondamentali degli interessati.

## ART. 9 – PROCESSO DI RISPOSTA ALLA VIOLAZIONE

Chiunque (dipendente, collaboratore o terzo che lavori ovvero agisca per conto della ASL Salerno) sia notiziato di una presunta ovvero effettiva violazione di dati personali deve immediatamente e senza ritardo comunicarla, attraverso i dati di contatto messi a disposizione di tutti i suddetti soggetti, al Gruppo di Risposta.
Ogni soggetto richiamato è tenuto alla comunicazione di cui sopra mediante la compilazione del "modulo di segnalazione di un potenziale *data breach*" allegato al presente documento.
Il Titolare del trattamento convoca il Gruppo di Risposta per valutare se tale notizia debba essere considerata una violazione dei dati personali o meno.
Il Gruppo è responsabile della determinazione del grado di complessità e del rischio relativo alla violazione, pertanto, laddove il caso risulti complesso, chiede parere al DPO.
Il Titolare del trattamento, per il tramite del Gruppo di Risposta, deve documentare tutte le violazioni che si siano verificate, indipendentemente dall'obbligo di notifica, al fine di poter dimostrare la conformità al GDPR.
Ai sensi dell'articolo 33, paragrafo 5 GDPR, il Titolare del trattamento deve registrare i dettagli relativi alla violazione, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti addottati per porvi rimedio.

Pertanto, si dovranno indicare in apposito Registro, allegato alla presente *policy*, tutte le notifiche effettuate al Garante Privacy e le comunicazioni inoltrate all'interessato.
Inoltre, ogni riunione del Gruppo va documentata e tale documentazione va conservata in modo accurato e preciso poiché questi documenti potrebbero essere esaminati dalle *Authority* ed annotata nel suddetto registro.

## TITOLO IV

## DISPOSIZIONI FINALI

### ART. 10 – VALIDITÀ E GESTIONE DEL DOCUMENTO

Il responsabile del presente documento è il Titolare del trattamento, il quale deve controllare e, se necessario, aggiornare il documento con frequenza almeno annuale.

Salerno, __/__/____

Titolare del trattamento

**Azienda Sanitaria Locale Salerno**

nella persona del

**Direttore Generale**

_____

[firma]