

# PROCEDURA PER LA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

Allegato 3 al Modello Organizzativo Privacy MOP

**ASL 7 SULCIS IGLESIENTE** - SC AFFARI GENERALI E LEGALI

*Allegato A "Modulo di comunicazione di data breach"*

## INDICE

1.INTRODUZIONE	pag. 3
2 FINALITÀ E OGGETTO DEL REGOLAMENTO	pag.3
3.AMBITO DI APPLICAZIONE	pag. 4
4. DESCRIZIONE PROCEDURA	pag. 4
4.1 Attivazione: segnalazione	pag..4
4.2 Identificazione ruolo Privacy dell’Azienda	pag.5
4.3 Analisi di primo livello	pag.6
4.4 Analisi di secondo livello – Gestione della violazione di dati	pag.6
4.5 Valutazione rischio	pag.6
4.5.a Modalità calcolo rischio per singolo parametro	pag.7
4.5.b Istruzioni per il calcolo	pag.11
5. Notificare la violazione all’autorità di controllo	pag.12
6. Comunicare la violazione all’Interessato	pag.13
7 Documentare la segnalazione	pag.14
8. Identificare le aree di miglioramento	pag.14
9 Gestire la segnalazione in qualità di Responsabile	pag.14
Allegato A “Modulo di comunicazione di data breach”	

## **1. INTRODUZIONE**

Per “Data Breach” o “violazione dei dati personali” si intende 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” (Art. 4, par.1, punto 12 del GDPR).

Si rende quindi necessario, per la Asl Sulcis Iglesiente, predisporre misure tecniche e organizzative adeguate che garantiscano la tutela dei dati personali e prevengano il rischio di violazione dei dati personali (Data Breach) e consentano una reazione tempestiva nel caso di realizzazione dell’evento.

Allo scopo sono programmate iniziative di formazione e informazione, tra cui simulazioni dell’evento “data breach”, per tutto il personale, affinché sia messo in condizione di segnalarlo per tempo e gestirlo.

A seguito di incidente di sicurezza e sospetta/presunta violazione di dati personali le Strutture coinvolte devono, nell’ambito delle loro competenze, predisporre i mezzi e gli strumenti tecnologici ed organizzativi per:

- Individuare la violazione o sospetta violazione;
- Analizzare le cause della violazione;
- Definire le misure da adottare per rimediare alla violazione dei dati personali e attenuarne i possibili effetti negativi;
- Registrare le informazioni relative alla violazione;
- Rispondere alle potenziali violazioni dei dati, coinvolgendo anche i fornitori;
- Fornire consulenza specialistica nel settore di competenza in supporto ai soggetti identificati come Riceventi.

## **2. FINALITÀ E OGGETTO DEL REGOLAMENTO**

Scopo del presente Regolamento è descrivere il flusso di informazioni e azioni da intraprendere in caso di una violazione o sospetta violazione dei dati personali, ponendo particolare attenzione affinché siano effettuati tutti gli sforzi per evitare o limitare i danni e consentire che siano rispettati i tempi richiesti per la segnalazione all’autorità di controllo.

Le Violazioni possono accadere per varie ragioni che possono includere a titolo esemplificativo:

- divulgazione di dati confidenziali a persone non autorizzate;
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- accesso abusivo (ad esempio: data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- casi di pirateria informatica;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo “owner”;

- virus o altri attacchi al sistema informatico o alla rete aziendale;
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- smarrimento di pc portatili, devices o attrezzature informatiche aziendali;
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario.

### **3. AMBITO DI APPLICAZIONE**

La presente procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare quali:

- i lavoratori dipendenti, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare (di seguito “Destinatari interni”);
- qualsiasi soggetto (persona fisica o persona giuridica) diverso dai Destinatari interni che, in ragione del rapporto contrattuale in essere con il Titolare abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 del GDPR o di autonomo Titolare del trattamento (“Destinatari esterni”), di seguito genericamente denominati “Destinatari”.

Tutti i Destinatari devono essere debitamente informati dell’esistenza della presente procedura, mediante metodi e mezzi che ne assicurino la comprensione.

Le violazioni sono gestite dal Titolare con l’ausilio del Presidio Data Breach, costituito dalle seguenti figure:

- Referente Ufficio Privacy;
- Dirigente della Struttura coinvolta;
- Amministratore di sistema;
- DPO;

Il Referente Ufficio Privacy ha il ruolo di Responsabile del Presidio Data Breach.

### **4. DESCRIZIONE PROCEDURA**

#### **4.1 Attivazione: segnalazione**

La procedura viene attivata da chiunque venga a conoscenza o sospetti un incidente di sicurezza e/o violazione di dati personali a seguito di comunicazione preliminare all’Ufficio Privacy all’indirizzo e-mail: [ufficio.privacy@aslsulcis.it](mailto:ufficio.privacy@aslsulcis.it) , al DPO all’indirizzo mail [dpo@aslsulcis.it](mailto:dpo@aslsulcis.it)

La segnalazione può pervenire da:

- canali interni;

la segnalazione, fatta in qualsiasi forma (scritta, verbale, telefonica) deve essere fatta a uno dei membri del Presidio Breach nel minor tempo possibile, da chiunque all’interno dell’Azienda rilevi o sospetti una violazione di dati personali;

- canali esterni
  - segnalazione dell’interessato;

- segnalazione da parte dei fornitori;
- segnalazione da parte di ulteriori soggetti;
- segnalazione da parte degli Organi Pubblici (AgID, Polizia, altre Forze dell'Ordine, giornalisti, ecc.).

Il Responsabile del Presidio Data Breach raccoglie le segnalazioni di un possibile data breach e le comunica agli altri membri del Presidio Data Breach.

In tutti e due i casi, per canale interno e per canale esterno, la segnalazione dovrà essere inoltrata al Titolare tramite modulo (Allegato A) e comunque dovrà indicare l'orario di ricezione della segnalazione, la fonte e, se possibile la relativa documentazione.

Ad ogni segnalazione dovrà essere attribuito un numero identificativo che deve essere composto da un numero progressivo e dall'anno (es. n° ID 1/2019). Lo stesso numero dovrà essere riportato in tutta la documentazione relativa all'incidente, in modo che la stessa possa essere ricondotta in maniera univoca. Non appena il Presidio Data Breach riceve la segnalazione, la stessa dovrà essere riportata nel Registro delle violazioni. (Allegato B)

In questa prima fase devono essere attuate le prime azioni per il contenimento dell'incidente occorso. A titolo esemplificativo: in caso di accesso non autorizzato ai sistemi è consigliato cambiare la password di accesso; in caso di perdita dei dati è necessario verificare se sono stati effettuati dei back up al fine di ripristinare al più presto i dati; in caso di furto di documentazione occorre verificare che siano state messe in atto opportune misure di sicurezza come la chiusura a chiave di una stanza o la presenza di un lucchetto.

#### **4.2 Identificazione ruolo Privacy dell'Azienda**

A seguito della rilevazione del sospetto incidente e/o violazione, le Strutture coinvolte comunicano l'evento al Referente Privacy che attiva il Presidio Data Breach.

L'analisi preliminare ha come obiettivo quello di raccogliere tutte le informazioni relative all'evento segnalato:

- Data e ora;
- Fonte;
- Tipologia dell'evento e descrizione;
- Stima del numero interessati coinvolti;
- Stima della numerosità dei dati personali di cui si presume la violazione;
- Luogo in cui è avvenuta la violazione o presunta violazione;

Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

Il Presidio Data Breach individua il Ruolo Privacy dell'Azienda in relazione all'oggetto della segnalazione.

Nel caso in cui la segnalazione pervenuta riguardi trattamenti di dati personali svolti dall'Azienda in qualità di Responsabile, si procede come descritto all'art. 9 "Gestire la segnalazione in qualità di Responsabile".

Nel caso in cui la segnalazione pervenuta riguardi trattamenti di dati personali svolti dall'Azienda in qualità di Titolare si procede con i passi seguenti.

#### **4.3 Analisi di primo livello**

Il Presidio Data Breach avvia l'analisi di primo livello.

L'analisi di primo livello ha come obiettivo quello di verificare che la segnalazione non sia un falso positivo, ovvero l'evento non abbia comportato la violazione di dati personali.

Nel caso in cui l'evento segnalato risulti essere un falso positivo si chiude l'incidente e si procede come descritto al paragrafo 7 "Documentare la segnalazione".

Nel caso la violazione dei dati personali venga accertata, il Presidio Data Breach passa alla fase di analisi di secondo livello.

#### **4.4 Analisi di secondo livello – Gestione della violazione di dati**

L'analisi di secondo livello deve essere effettuata nel più breve tempo possibile dall'avvenuta conoscenza dell'evento.

Il Presidio Data Breach deve identificare:

- categoria di violazione:
  - perdita di riservatezza
  - perdita di integrità
  - perdita di disponibilità
- supporto oggetto della violazione (es. applicativo, banche dati, servizi server farm, dispositivo mobile, computer, documento cartaceo, etc.)
- dati oggetto della violazione e i relativi trattamenti censiti nel Registro dei trattamenti
- Interessati
- il contenimento del danno come di seguito descritto:
  - limitazione o annullamento degli effetti dell'incidente;
  - raccolta delle prove forensi nel caso sia ipotizzato un reato;
  - determinazione delle azioni possibili di ripristino, ed avvio delle stesse;
  - ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni;
  - valutazione dei tempi di ripristino;
  - verifica dei sistemi recuperati;
  - valutazione delle eventuali vulnerabilità collegate con l'incidente;
  - individuazione delle azioni di mitigazione delle vulnerabilità individuate.

#### **4.5 Valutazione rischio**

Per facilitare la classificazione del rischio per i diritti e le libertà fondamentali delle persone fisiche,

la violazione può essere valutata secondo i livelli di rischio riportati da ENISA (The European Union Agency for Cybersecurity) e attraverso le funzioni automatizzate del Registro delle violazioni

L'analisi dei Rischi elaborata da ENISA prende in considerazione i seguenti parametri:

1. **Contesto** del trattamento e tipologia di dati: ossia la tipologia di dati violati insieme a una serie di fattori collegati al contesto generale della loro elaborazione. Il contesto è un elemento centrale della metodologia e valuta la criticità di un determinato insieme di dati in un ambito di elaborazione specifico;
2. **Facilità di identificazione** dell'individuo sulla base dei dati violati: **ossia** la facilità con cui l'identità degli individui può essere dedotta dai dati oggetto della violazione. Tale parametro è un fattore di correzione del **"Contesto di elaborazione dati"**, infatti, la criticità complessiva di un Personal Data Breach può essere ridotta in base al valore di facilità di identificazione degli interessati. In altre parole, minore è la facilità di identificazione dell'individuo, minore è il punteggio complessivo da attribuire alla violazione del dato. Pertanto, *Facilità di identificazione* moltiplicata per il *Contesto dell'elaborazione* dati fornisce il punteggio iniziale della gravità della violazione dei dati
3. **Circostanze della violazione**: parametro che tiene conto delle specifiche circostanze della violazione, inclusa principalmente la perdita di sicurezza dei dati violati, nonché qualsiasi intento malevolo coinvolto. Questo parametro quantifica le circostanze specifiche della violazione che possono essere presenti o meno in una particolare situazione.

Quindi il livello di rischio viene calcolato attraverso la seguente formula:

**Rischio = (Contesto x Facilità di identificazione) + Circostanze**

Il risultato ottenuto permette la seguente catalogazione dei livelli di rischio:

- **Basso** (<2): gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (Es. tempo trascorso reinserendo informazioni, fastidi, irritazioni, etc.).
- **Medio** (tra 2 e 3): gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (Es. costi aggiuntivi, rifiuto di accesso ai servizi dell'Azienda, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, etc.).
- **Alto** (tra 3 e 4): gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (Es. appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.).
- **Molto alto** (>4): gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

(Vedi Tabella 1 a pag. 9)

#### 4.5.a Modalità calcolo rischio per singolo parametro

- Punteggio per il parametro "contesto"

I dati vengono classificati in almeno una delle tre categorie: Personali/Anagrafici/identificativi, Rischiosi, Particolari / Relativi a condanne penali e reati. A ciascuna categoria dovrà essere attribuita una descrizione e attribuito un punteggio.

- **Personale/ Anagrafico/Identificativo - Punteggio:1**

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.

- **Rischioso - Punteggio: 2**

Qualsiasi informazione consistente nell'utilizzo di dati personali atti a valutare determinati aspetti personali relativi a una persona fisica. Ad esempio, per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

- **Categorie Particolari di dati e/o relativi a reati o condanne penali - Punteggio 3**

In questa categoria rientrano una o più tipologie di informazioni:

- “dati genetici”: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- “dati biometrici”: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- “dati relativi alla salute”: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale o la vita sessuale o all'orientamento sessuale della persona;
- “dati relativi a condanne penali e reati”: dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza.

### **Punteggio Facilità di identificazione**

La facilità d'identificazione valuta quanto sarà facile abbinare univocamente i dati violati all'identità di una determinata persona e quindi quanto è probabile la sua identificazione.

Ai fini di questa metodologia sono stati definiti tre livelli (trascurabile, significativo e massimo) descritti in dettaglio nel seguente elenco:

- **Livello Trascurabile - Punteggio 0,25**

Quando il dato oggetto di Data Breach, di per sé, non rileva l'identità dell'individuo e non è possibile associarvi ulteriori informazioni (es. i dati sono cifrati).



- **Livello Significativo - Punteggio 0,75**

Quando il dato oggetto di Data Breach, di per sé, non rileva l'identità dell'individuo ma ne rivela ulteriori informazioni identificative (ad es. la data di nascita) ed è collegato ad altri dati (ad esempio indirizzo postale).

- **Livello Massimo - Punteggio 1**

Quando i dati oggetto del Data Breach rivelano l'identità dell'individuo.

### **Punteggio Circostanze della violazione**

Le circostanze della violazione valutano la perdita di sicurezza in relazione alla riservatezza, alla integrità, alla disponibilità e alle intenzioni malevole Più specificatamente:

- Perdita di riservatezza: si verifica quando le informazioni sono accessibili da soggetti non autorizzati o che non hanno uno scopo legittimo nell'accedervi. L'entità della perdita di riservatezza varia a seconda della portata della divulgazione, ovvero il numero potenziale e il tipo di parti che possono avere accesso illecito all'informazione.
- Perdita di integrità: si verifica quando le informazioni originali vengono alterate e la sostituzione dei dati può essere pregiudizievole per l'individuo. La situazione più grave si verifica quando esistono gravi possibilità che i dati modificati siano stati utilizzati in un modo tale da danneggiare l'individuo.
- Perdita di disponibilità: la perdita di disponibilità si verifica quando non è possibile accedere ai dati originali. Può essere temporanea (i dati sono recuperabili ma in un apprezzabile periodo di tempo) o permanente (i dati non possono essere recuperati).
- Intento malevolo: questo elemento esamina se la violazione è dovuta a un errore, umano o tecnico, o è stata causata da un'azione intenzionale. Violazioni fraudolente includono casi di furto e hacking che mirano a danneggiare le persone (ad es. esponendo i loro dati personali a terzi non autorizzati). In altri casi, l'intento malevolo potrebbe includere il trasferimento di dati personali a terzi a scopo di lucro (ad es. la vendita di elenchi di dati personali). In alcuni casi, l'intento malevolo potrebbe anche essere desunto da azioni volte a danneggiare il responsabile del trattamento dei dati (ad esempio attraverso il furto e l'esposizione dei dati personali a soggetti non autorizzati)

(N.B. Nella valutazione delle Circostanze deve essere preso il punteggio più alto associato alle tipologie di violazione esaminate).

Di seguito i diversi punteggi per ciascuna caratteristica della sicurezza dei dati e per i diversi tipi di circostanze.

Tabella 1

TIPOLOGIA VIOLAZIONE				Punteggio
Riservatezza	Integrità	Disponibilità	Intento Malevolo	
Dati esposti a rischi di riservatezza senza che vi sia una reale possibilità di utilizzo (es. i dati sono cifrati)	N.A.	N.A.	N.A.	0.25
Dati esposti a rischio di riservatezza su un certo numero di destinatari noti.	Dati modificati ma con possibilità di recuperare gli originali.	Indisponibilità temporale.	N.A.	0.50
Dati esposti a rischio di riservatezza su un numero sconosciuto di destinatari.	Dati modificati senza possibilità di recuperare gli originali.	Completa indisponibilità (i dati non possono essere recuperati dal controllore o dai singoli)	La violazione era dovuta a un'azione intenzionale, <b>1)</b> ad es. al fine di causare problemi al titolare o responsabile del trattamento (ad esempio, dimostrare la perdita di sicurezza) e/o al fine di danneggiare le persone <b>2)</b> appropriarsi di dati per fini di lucro e/o frodi economiche a danno dello Stato e della Comunità Europea	0.75

Definizione del livello di gravità:

Come già specificato la gravità complessiva del rischio è calcolata con la seguente formula:

$$R \text{ (Rischio)} = (\text{Contesto di trattamento dati} * \text{Facilità identificazione}) + \text{Circostanze violazione}$$

Il punteggio finale mostra il livello di gravità del rischio per gli interessati da una determinata violazione, tenendo conto dell'impatto sugli individui stessi

Tabella 2

Livello di gravità del Data Breach			OBBLIGO
$R \leq 1$	Low (Basso)	Gli individui non saranno impattati o potrebbero solo incontrare alcuni inconvenienti, che supereranno senza alcun problema (es. tempo trascorso a reinserire informazioni).	Registrazione interna
$1 < R \leq 2$	Medium (Medio)	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (es. costi aggiuntivi, impossibilità di accedere ai servizi).	Registrazione interna
$2 < R < 3$	High (Alto)	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, black list da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, etc.).	Notifica al Garante Privacy
$3 \leq R$	Critical (Critica)	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa etc.)	Notifica al Garante Privacy Comunicazione all'Interessato*
* In conformità all'art. 34 del GDPR, la comunicazione all'Interessato NON andrà comunque effettuata se è soddisfatta una delle seguenti condizioni: 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 (es. l'inintelligibilità sotto forma di crittografia forte e senza compromissione chiave, può ridurre sostanzialmente l'impatto sugli individui, poiché riduce notevolmente la possibilità che parti non autorizzate accedano ai dati).			

*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 invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.*

#### 4.5.b Istruzioni per il calcolo

Le soglie del livello di gravità del Rischio sono definite utilizzando le matrici di calcolo dei fattori (in particolare gli addendi) che contribuiscono al calcolo di R. I razionali sono illustrati di seguito:

Contesto del trattamento(C)={1;2;3}

Facilità identificazione(ID)={0.25;0.75;1}

Circostanze del databreach(CDB)={0.25;0.50;0.75}

		C		
		1	2	3
ID	0.25	0.25	0.50	0.75
	0.75	0.75	1.5	2.25
	1	1	2	3

		C*ID							
		0.25	0.50	0.75	1	1.50	2	2.25	3
CDB	0.25	0.50	0.75	1	1.25	1.75	2.25	2.50	3.25
	0.50	0.75	1	1.25	1.50	2	2.50	2.75	3.50
	0.75	1	1.25	1.50	1.75	2.25	2.75	3	3.75

Per procedere al Calcolo, dunque, si deve attribuire un punteggio al Contesto del trattamento e alla facilità di identificazione degli interessati, e calcolare il prodotto; bisogna poi aggiungere dunque il punteggio della tabella A.1 con le tipologie di violazione (in caso di concomitanza di più fattori, scegliere il punteggio più alto) e aggiungere tale valore al risultato del prodotto calcolato in precedenza.

#### ESEMPIO PRATICO:

*Caso di smarrimento/furto smartphone aziendale (con accesso al display bloccato e protetto); lo smartphone è configurato con il Client per la posta aziendale (accesso all'APP con ulteriore password).*

*In questo esempio i parametri per il calcolo della gravità del Rischio andranno valutati nel modo seguente:*

- 1) Contesto del trattamento: sono sicuramente presenti dati personali/identificativi/anagrafici; se il dispositivo è in uso a personale che può avere dati personali del contesto "rischiosi" o "particolari", si attribuisce il punteggio più alto; nel peggiore dei casi, supponendo che siano presenti messaggi di posta con dati particolari, in questo caso il punteggio è 3.
- 2) Facilità di identificazione, nell'esempio fatto, essendo lo Smartphone protetto con sistema di crittografia (pin e altro), il Rischio è trascurabile: 0,25 di punteggio.

*A prescindere dalle circostanze del Data Breach (0,75 nel peggiore dei casi), il prodotto fra indicatore di contesto e facilità di identificazione è 0,75; sommando il valore delle circostanze 0,75 si ottiene il livello di rischio 1,50; siamo nel livello medio, gli interessati (le persone a cui si riferiscono i contatti della rubrica del telefono, e i dati personali contenenti nei messaggi di posta elettronica) non*

*dovrebbero avere conseguenze; infatti non sarà necessario notificare il data breach all'Autorità Garante.*

*Punteggio ben diverso si sarebbe ottenuto se lo smartphone non fosse stato idoneamente protetto.*

## **5. Notificare la violazione all'autorità di controllo**

Qualora, dopo l'analisi di secondo livello, risulti improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, non è necessario procedere con la notifica all'Autorità di controllo.

La documentazione prodotta in fase di analisi e corredata dalle relative motivazioni andrà inserita nel Registro dei Data Breach dal Presidio Data Breach.

Nei casi in cui sussista un maggiore livello di rischio il Presidio Data Breach deve valutare le azioni da intraprendere ed effettuare la notifica all'Autorità di controllo **entro e non oltre 72 ore** dal momento in cui il Titolare è venuto a conoscenza della violazione, tramite il modello presente sul sito del Garante link: [https://servizi.gpdp.it/databreach/resource/1629905132000/DB\\_Istruzioni](https://servizi.gpdp.it/databreach/resource/1629905132000/DB_Istruzioni)

La mancata comunicazione può essere sanzionata. Nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

La notifica Garante deve essere effettuata nel caso in cui i rischi per le persone fisiche non siano trascurabili e solo nei seguenti casi:

- l'Azienda è Titolare del/i trattamento/i dei dati coinvolti nella violazione;
- l'Azienda è Responsabile del trattamento con delega alla notifica.

**Qualora la notifica al Garante non sia effettuata entro 72 ore, va corredata dei motivi del ritardo.**

La notifica al Garante deve descrivere, ove possibile:

- la natura della violazione dei dati personali compresi;
- le categorie e il numero approssimativo di interessati in questione;
- le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- il nome e i dati di contatto del DPO;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate, o di cui si propone l'adozione da parte dell'Azienda, per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora non sia possibile fornire fin da subito le informazioni queste possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Nell'ipotesi in cui la violazione dei dati personali integri gli estremi di un incidente significativo, il Titolare del trattamento dovrà premurarsi di segnalarlo a CSIRT Italia per il tramite del Referente CSIRT ovvero del Punto di Contatto.

## 6. Comunicare la violazione all'Interessato

Il Presidio Data Breach deve informare gli interessati dell'evento anomalo, in tutti i casi in cui, a norma degli artt. 33-34 GDPR, la violazione presenta gravi rischi per i diritti e le libertà delle persone fisiche.

La comunicazione deve essere rivolta all'interessato senza ingiustificato ritardo dall'avvenuta conoscenza e valutazione della violazione, attraverso il canale di comunicazione ritenuto più idoneo:

- comunicazione diretta agli interessati, attraverso un canale dedicato che renda certa l'evidenza al destinatario (es. invio di un'apposita e-mail);

Solo laddove non sia possibile raggiungere gli interessati attraverso una modalità di comunicazione dedicata:

- comunicato stampa;
- comunicazione tramite sito WEB/social media;
- altre forme.

La comunicazione deve essere intellegibile, concisa, trasparente e facilmente accessibile. Deve essere utilizzato un linguaggio semplice e chiaro adottando, se possibile, la stessa lingua parlata dall'interessato.

La comunicazione di Data Breach all'interessato deve contenere le seguenti informazioni:

- data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
- la natura della violazione dei dati personali;
- il nome e i dati di contatto del DPO;
- le probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte dell'Azienda per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

- sono state messe 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; salvo i casi in cui la violazione della sicurezza ha comportato la distruzione o la perdita dei dati personali degli interessati;
- sono state successivamente adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà delle persone fisiche; in tal caso è necessario documentare le misure nel Registro e nella comunicazione all'autorità di controllo;
- 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.

L'Azienda deve effettuare la comunicazione nelle casistiche descritte in precedenza e solo per i trattamenti in qualità di Titolare del Trattamento.

Ulteriori istruzioni (es. eventuale delega alla comunicazione) possono essere definite negli atti di nomina a Responsabile del trattamento, ex art. 28 GDPR.

## **7. Documentare la segnalazione**

L'Art. 33 del GDPR prescrive al Titolare e al Responsabile del trattamento di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

Nel Registro dei Data Breach, il Presidio Data Breach documenta ogni singolo evento, sia esso falso, irrilevante o rilevante; in quest'ultimi due casi, devono essere indicate nel Registro:

- le conseguenze del Data Breach;
- i provvedimenti adottati per porvi rimedio o attenuarne le conseguenze;
- l'eventuale notifica all'autorità di controllo;
- l'eventuale comunicazione all'Interessato.

Nel Registro vanno inserite tutte le segnalazioni di violazione pervenute all'Azienda sia come titolare del trattamento sia come Responsabile del trattamento.

Per quanto riguarda la documentazione delle violazioni, il Titolare del trattamento tiene conto del parere del DPO in merito alla struttura, all'impostazione e all'amministrazione della documentazione stessa.

## **8. Identificare le aree di miglioramento**

Le azioni di miglioramento previste in fase di applicazione della presente procedura sono le seguenti:

- analisi dell'evento con figure tecniche-professionali competenti per individuare le vulnerabilità;
- adozione di nuovi sistemi tecnici di prevenzione/protezione e/o di sistemi di controllo/monitoraggio/allarme;
- individuazione di controlli e misure di sicurezza che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- valutazione su possibilità di copertura assicurativa;
- azioni informative rivolte ai dipendenti;
- revisione delle relazioni con i Fornitori;
- pianificazione dei test periodici per verificare la validità della presente procedura;
- revisione della procedura, se necessario, e di eventuali altri documenti collegati.

## **9. Gestire la segnalazione in qualità di Responsabile**

Nei casi in cui l'Azienda agisca come Responsabile del trattamento di dati personali, il Presidio Data Breach deve comunicare l'incidente di sicurezza riguardante i dati personali al Titolare con le

modalità convenute negli atti di nomina/istruzioni ricevute e con la massima tempestività, fornendo tutte le informazioni necessarie e mettendosi a disposizione di quest'ultimo per approfondimenti e contenimento dei danni.

L'Azienda non ha il dovere di notificare all'autorità Garante quando agisce come Responsabile del trattamento per conto di altro Titolare (senza delega alla notifica al Garante). Spetta infatti al Titolare la valutazione dell'effettiva sussistenza della violazione di dati personali.

Anche la comunicazione verso l'Interessato, nei casi in cui l'Azienda agisca in qualità di Responsabile spetta al Titolare.

Quindi, va comunque documentato l'incidente di sicurezza riguardante i dati personali, come descritto al paragrafo 4.8 "Documentare la segnalazione".

## **10. Sanzioni**

Il rispetto del presente regolamento è obbligatorio per tutti i Destinatari e la mancata conformità a quanto previsto dallo stesso potrà comportare provvedimenti disciplinari a carico dei dipendenti inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia

**MODULO DI COMUNICAZIONE DI DATA BREACH**

Qualora sia rilevata una sospetta, presunta o effettiva violazione dei dati personali, è necessario darne immediata comunicazione al Titolare del trattamento mediante compilazione del modulo che segue da inviare a mezzo e-mail ai seguenti indirizzi: [dpo@aslsulcis.it](mailto:dpo@aslsulcis.it) e [ufficio.privacy@aslsulcis.it](mailto:ufficio.privacy@aslsulcis.it)

## Comunicazione di Data Breach

Data di compilazione:
-----------------------

☐ DESTINATARIO INTERNO \*

Dati della persona che fa la segnalazione:

Cognome e nome	
Incarico/Mansione	
Dati di contatto (indirizzo e-mail, numero di telefono)	

☐ DESTINATARIO ESTERNO \*

Dati del soggetto che fa la segnalazione:

Ditta\Ragione sociale	
Dati di contatto del DPO (ove nominato)	
Cognome e nome del soggetto segnalatore	
Dati di contatto (indirizzo e-mail, numero di telefono)	

\*indicare, alternativamente, se il soggetto che fa la segnalazione è un Destinatario interno o un Destinatario esterno.



## DESCRIZIONE DELL'EVENTO:

Data di scoperta della violazione (data, ora)	
Data e luogo della violazione (data, ora, luogo)	
Descrizione di cosa è successo	
Descrizione di come è successo	
Categorie e numero approssimativo di interessati coinvolti nella violazione	
Altri dettagli rilevanti (eventuali azioni poste in essere al momento della scoperta della violazione ecc..)	

A cura del Titolare del trattamento (o del referente da esso incaricato)	Data e ora di ricevimento del modulo di segnalazione	
Modalità di ricezione:	N° Progressivo di segnalazione (da Registro Violazione Dati):	
Sistemi coinvolti:		
Vulnerabilità rilevate:		