METODOLOGIA VALUTAZIONE DATA BREACH

Nell'ipotesi in cui, nonostante le misure di sicurezza adottate al fine di prevenire il rischio di perdita di dati si verifichi un potenziale data breach, qui di seguito la metodologia per **la valutazione della gravità delle violazioni dei dati personali** adottata dalla Regione Sardegna. Tale metodologia è stata definita sulla base delle indicazioni fornite dall'**ENISA** (European Union Agency for Network and Information Security) all'interno del documento "*Recommendations for a methodology of the assessment of severity of personal data breaches"*.

Gli elementi chiave da tenere in considerazione in sede di valutazione della gravità risultano essere i seguenti:

- *La* natura e contesto dei dati violati **(VALUTAZIONE 1)**
- *Facilità di identificazione* dell'individuo in base ai dati violati **(VALUTAZIONE 2)**
- *Circostanze della violazione* (violazione di riservatezza, integrità e disponibilità dei dati), che hanno un'influenza aggiuntiva sulla gravità di una violazione **(VALUTAZIONE 3)**

La valutazione della gravità della violazione può essere effettuata secondo le seguenti sotto fasi:

- **Valutazione 1** analizzare la criticità dell'insieme di dati violati in un contesto di elaborazione specifico;
- **Valutazione 2:** si tratta del fattore di correzione della Valutazione 1. La criticità complessiva di un trattamento dei dati può essere ridotta in base al valore identificato.
- **Valutazione 3:** quantifica le circostanze specifiche della violazione che possono essere presenti o meno in una particolare situazione. Pertanto il fattore, laddove presente, può solo incrementare la gravità di una specifica violazione. Per questo motivo il punteggio iniziale può essere ulteriormente regolato da quest'ultima valutazione
- **Valutazione 4 - Calcolo della gravità:** calcolo della gravità della violazione sulla base dei 3 precedenti elementi.

Definizione del punteggio per la natura e contesto dei dati violati (VALUTAZIONE 1)

Il punteggio della valutazione 1 *(di seguito anche "pt.1")* è al centro della metodologia e valuta la criticità dell'insieme di dati violati in un contesto di elaborazione specifico.

Nella tabella seguente sono riassunte le attività inerenti a questa fase di valutazione**:**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
1	RPD / Gruppo di gestione data breach	Definire e Classificare i tipi di dati personali	Definisce e classifica la tipologia di dato trattato che ha subito una violazione sulla base delle seguenti quattro categorie: • dati identificativi/personali; • dati comportamentali; • dati finanziari;	Registro dei Data Breach (allegato B)

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
			• dati sensibili/particolari. Inoltre, aggiorna il Registro dei Data Breach nella sessione “Tipologia di dato trattato” (fare riferimento all’allegato B)	
2	RPD / Gruppo di gestione data breach	Attribuire il punteggio base	Attribuisce il punteggio base secondo la tabella 1 definita dalla metodologia per le categorie di natura di dato (dati identificativi/personali, dati comportamentali, dati finanziari, dati sensibili).	Tabella 1 Contesto Elaborazione Dati
3	RPD / Gruppo di gestione data breach	Aumentare o Ridurre il punteggio base secondo il contesto specifico	Aumenta o riduce il punteggio base in funzione della presenza di fattori contestuali relativi all'elaborazione dei dati (ad es. volume di dati, caratteristiche speciali dei Titolari o degli individui, inesattezza dei dati, disponibilità del dato al pubblico prima della violazione, natura del dato). Il punteggio che emerge dalla tabella 1 può variare da 1 a 4.	Tabella 1 Contesto Elaborazione Dati

Di seguito riportiamo le tabelle da utilizzare **per la determinazione del punteggio della valutazione 1:**

Tabella 1 – Natura e contesto dei dati		**Punteggio**
Dati Identificativi/ Personali	**Esempio Dati Identificativi: Data di nascita, Stato di famiglia, Studi, Lavoro, Stipendio, Inquadramento** **Esempio Dati Personali: Nome del cittadino, Numero di Telefono, Indirizzo, email, ID card, Fotografia**	
	Punteggio Base: quando la violazione riguarda "dati identificativi/personali" e il Titolare non è a conoscenza di alcun fattore aggravante.	**1**
	Il punteggio potrebbe essere **aumentato di 1**, ad esempio quando il volume di "dati identificativi/personali" e/o le caratteristiche del Titolare sono tali da consentire l'abilitazione di determinati profili o possono essere formulate assunzioni sullo stato sociale/finanziario dell'individuo.	**2**
	Il punteggio potrebbe essere **aumentato di 2**, ad esempio quando i "dati identificativi/personali" e/o le caratteristiche del Titolare possono portare a supposizioni sullo stato di salute dell'individuo, sulle preferenze sessuali, sulle convinzioni politiche o religiose.	**3**

Tabella 1 – Natura e contesto dei dati		Punteggio
	Il punteggio potrebbe essere **aumentato di 3**, ad esempio quando a causa di determinate caratteristiche dell'individuo (ad es. gruppi vulnerabili, minori), l'informazione può essere critica per la sicurezza personale o per le condizioni fisiche / psicologiche.	**4**
Dati Comportamentali	**Esempio: Abitudini, preferenze personali e interessi, vita sociale e contatti**	
	Punteggio Base: quando la violazione comporta "dati comportamentali" e il controllore non è a conoscenza di fattori aggravanti o di diminuzione.	**2**
	Il punteggio potrebbe essere **diminuito di 1**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	**1**
	Il punteggio può essere **aumentato di 1**, ad esempio quando il volume di "dati comportamentali" e / o le caratteristiche del controllore sono tali da consentire la creazione di un profilo dell'individuo, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	**3**
	Il punteggio può essere **aumentato di 2**, ad esempio se è possibile creare un profilo basato sui dati di una persona (es. cittadini).	**4**
Dati Finanziari	**Esempio: IBAN, Numero di conto, Saldo conto, Transaction History, Informazione di base sulla carta di credito (senza CVC), Complete informazioni sulla carta di credito (con CVC), Dati sui mutui/prestiti**	
	Punteggio Base: quando la violazione riguarda "dati finanziari" e il responsabile del trattamento non è a conoscenza di fattori aggravanti o di diminuzione.	**3**
	Il punteggio potrebbe essere **diminuito di 2**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni finanziarie dell'individuo (ad esempio, il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	**1**
	Il punteggio potrebbe essere **diminuito di 1**, ad esempio quando il set di dati specifici include alcune informazioni finanziarie ma non fornisce ancora informazioni significative sullo stato / sulla situazione finanziaria dell'individuo (ad esempio: i numeri di conti bancari semplici senza ulteriori dettagli).	**2**

Tabella 1 – Natura e contesto dei dati		Punteggio
	Il punteggio potrebbe essere **aumentato di 1**, ad esempio quando a causa della natura e / o del volume dell'insieme di dati specifici, vengono divulgate informazioni complete finanziarie (ad esempio: informazioni complete sulla carta di credito con il codice cvc)	**4**
Dati Sensibili/Particolari	**Esempio: Dati Sanitari, Razza / origine etnica, Orientamento politico e religioso, Orientamenti sessuali, Procedimento penale / condanna, Dati biometrici, Dati genetici**	
	Punteggio Base: quando la violazione riguarda "dati sensibili" e il controllore non è a conoscenza di alcun fattore di diminuzione.	**4**
	Il punteggio potrebbe essere **diminuito di 3**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni sui dati sensibili o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	**1**
	Il punteggio potrebbe essere **diminuito di 2**, ad esempio quando la natura dei dati può portare a ipotesi generali.	**2**
	Il punteggio potrebbe essere **diminuito di 1**, ad esempio quando la natura dei dati può portare a supposizioni su informazioni sensibili.	**3**

Si specifica che l'elenco dei tipi di dati descritti nelle quattro categorie non è esaustivo; tuttavia, la maggior parte dei dati coinvolti in casi reali può essere abbinata ad almeno una delle categorie.

La definizione dell'indicatore per la natura e contesto dei dati violati è il punteggio più alto raggiunto. Se i dati corrispondono a più di una categoria, è necessario seguire i passaggi sopra indicati per ogni categoria applicabile e in questi casi il valore da prendere in considerazione è il punteggio della categoria a cui è stato attribuito il valore più alto. Esempio:

- se la violazione riguarda "dati identificativi/personali" e il Titolare non è a conoscenza di alcun fattore aggravante, il punteggio da attribuire è 1;
- se la violazione riguarda anche dati comportamentali" e il Titolare non è a conoscenza di fattori aggravanti o di diminuzione, il punteggio è 2;

Pertanto, ai fini del calcolo del punteggio per la natura e contesto dei dati violati (VALUTAZIONE 1), occorre prendere in considerazione il valore 2.

<u>Definizione del punteggio per la facilità di identificazione (Valutazione 2)</u>

Il punteggio della 2^ valutazione *(di seguito anche "pt.2")* è il fattore di correzione della Valutazione 1 che tiene in considerazione la facilità di identificazione dell'individuo in base ai dati violati.

Nella tabella seguente sono riassunte le attività inerenti alla **valutazione 2:**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
4	RPD	Valutare la facilità di identificazione dell'individuo e determinare il pt.2	Valuta la **facilità di identificazione** dell'individuo ed attribuisce un punteggio secondo la tabella 2 definita dalla metodologia secondo i seguenti quattro livelli: • trascurabile (0,25); • limitato (0,5); • significativo (0,75); • massimo (1). Il fattore di correzione pt.2 può essere 0,25 / 0,5/ 0,75 o 1. Il punteggio più basso viene attribuito quando la possibilità di identificare l'individuo è trascurabile, il che significa che è estremamente difficile abbinare i dati a una determinata persona, ma comunque potrebbe essere possibile con determinate condizioni. Al contrario, il punteggio più alto viene attribuito quando l'identificazione è possibile direttamente dai dati violati, senza alcuna ricerca specifica per determinare l'identità dell'individuo.	Tabella 2 Facilità di identificazione
5	RPD	Correggere il valore identificato in fase 1 moltiplicando con il fattore di valutazione 2	Una volta individuato il fattore di correzione, esso viene moltiplicato per il valore 1, al fine di determinare il punteggio iniziale della gravità della violazione dei dati.	Tabella 2 Facilità di identificazione

Di seguito riportiamo le tabelle da utilizzare **per la valutazione del secondo valore (valutazione 2):**

Tabella 2 - Facilità di identificazione		**Punteggio**	**Livello**
	Definizione: Facilità con cui possono essere identificati gli interessati (FI)		

Descrizioni (a titolo esemplificativo)	L'aggressione riguarda dati identificativi o dati personali **non direttamente identificabili (ad esempio: nome/cognome molto diffuso in un paese)**	**0,25**	Trascurabile
	L'aggressione riguarda i dati identificativi **di un individuo ma non facilmente identificabile (ad esempio: nome/cognome condiviso da poche persone in un intero paese)**	**0,5**	Limitata
	L'aggressione riguarda dati identificativi e **rivela ulteriori informazioni di identificazione dell'individuazione (ad esempio: nome completo con l'indicazione dell'indirizzo email di questa persona)**	**0,75**	Significativo
	L'aggressione riguarda dati identificativi o dati personali **direttamente identificativi (ad esempio: nome completo con l'indicazione della data di nascita e l'indirizzo email di questa persona)**	**1**	Massimo

La definizione del punteggio per la facilità di identificazione (Valutazione 2) è il punteggio più alto raggiunto. Se i dati corrispondono a più di una categoria, è necessario prendere in considerazione il punteggio della categoria a cui è stato attribuito il valore più alto.

Definizione del punteggio per le Circostanze della violazione (Valutazione 3)

Il punteggio della valutazione 3 quantifica le **circostanze specifiche della violazione** che possono essere presenti o meno in una particolare situazione.

Nella tabella seguente sono riassunte le attività inerenti alla **Valutazione 3 :**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
6	RPD	Quantificare le circostanze specifiche della violazione	Attribuisce il punteggio relativo **alle circostanze della violazione** classificate secondo le seguenti macro categorie: • violazione di riservatezza; • violazione di disponibilità; • violazione di integrità dei dati; • eventuali intenzioni malevole.	Tabella 3

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
			Le circostanze possono avere solo un'influenza aggiuntiva sulla gravità di una violazione. Il pt.3 può incrementare il punteggio iniziale delle gravità di 0,25 o 0,5 a seconda dei casi.	

Di seguito riportiamo la tabella da utilizzare **per la valutazione del terzo punteggio (*di seguito "pt.3"):***

Tabella 3 - Circostanze della violazione		**Punteggio**
Violazione di riservatezza	**Definizione:** La perdita di riservatezza si verifica quando le informazioni s**ono accessibili da parti che non sono autorizzate o che non hanno uno scopo legittimo** di 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.	
	Esempi di dati esposti a rischi di riservatezza **senza prove che l'elaborazione illegale si è verificata:** - Un file cartaceo o un laptop si perde durante il transito; - L'attrezzatura è stata smaltita senza distruzione dei dati personali.	**0**
	Esempi di dati trasmessi verso un certo numero **di destinatari conosciuti:** - Un'e-mail con dati personali è stata inviata erroneamente a un certo numero di destinatari conosciuti; - Alcuni soggetti esterni (es. cittadini, rappresentanti legali di un ente) possono accedere agli account di altri in un servizio online.	**0,25**
	Esempi di dati trasmessi verso un certo numero **di destinatari sconosciuti:** - I dati sono pubblicati su una bacheca internet; - I dati vengono caricati su un sito P2P; - Un dipendente vende un CD ROM con i dati del cittadino; - Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni.	**0,5**
Violazione di integrità	**Definizione:** La 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 che potrebbe danneggiare l'individuo.	
	Esempi di **dati modificati** ma **senza alcun uso errato o illegale** identificato: - Le registrazioni di un database con dati personali sono state	**0**

Tabella 3 - Circostanze della violazione		Punteggio
	erroneamente aggiornate ma è stata effettuata una copia dell'originale prima del verificarsi della modifica.	
	Esempi di dati modificati ed **eventualmente usati in modo errato o illegale ma con possibilità di recupero**: - Un dato necessario per la fornitura di un servizio online è stato modificato e l'individuo deve richiedere il servizio in modalità offline. - È stato modificato un dato importante per l'accuratezza del file di un individuo in un servizio medico online.	**0,25**
	Esempi di dati modificati ed **eventualmente usati in modo errato o illegale senza possibilità di recupero**: - Valgono gli esempi precedenti con l'aggravante che i dati originali non possono essere recuperati.	**0,5**
Violazione di disponibilità	**Definizione:** La **perdita di disponibilità** si verifica quando non è possibile accedere ai dati originali quando ce n'è bisogno. Può essere temporaneo (i dati sono recuperabili ma richiederà un periodo di tempo e questo può essere dannoso per l'individuo) o permanente (i dati non possono essere recuperati).	
	Esempi di dati che **possono essere recuperati senza difficoltà**: - Una copia del file è persa ma sono disponibili altre copie. - Un database è danneggiato ma può essere facilmente ricostruito da altri database.	**0**
	Esempi di **indisponibilità temporale**: - Un database è corrotto ma può essere ricostruito da altri database, sebbene sia richiesta qualche elaborazione. - Un file è perso ma l'informazione può essere fornita di nuovo dall'individuo	**0,25**
	Esempi di **indisponibilità totale** (i dati non possono essere recuperati dal controllore o dai singoli): - Un file è perso / database danneggiato, non c'è il backup di queste informazioni e non può essere fornito dall'individuo.	**0,5**
Intenzioni malevole	**Definizione:** La violazione è **dovuta a un'azione intenzionale malevola**, ad esempio al fine di causare problemi al Titolare o danneggiare gli interessati.	
	Esempi di violazione dovuta a un'azione intenzionale: - Un dipendente condivide intenzionalmente dati privati dai cittadini in un sito pubblico di social media. - Un dipendente vende dati privati dei cittadini a una società. - Un membro di un social network invia intenzionalmente delle	**0,5**

Tabella 3 - Circostanze della violazione		Punteggio
	informazioni sugli altri membri ai propri familiari al fine di danneggiarli.	

La definizione del punteggio per le Circostanze della violazione (Valutazione 3) è data dalla somma dei punteggi ottenuti per ciascuna tipologia di circostanza.

> Esempio: se è stato quantificato un punteggio di 0,5 per la violazione di riservatezza, di 0,5 per la violazione di integrità, di 0,5 per la violazione di disponibilità, di 0,5 per la violazione di intenzioni malevole, il punteggio da tenere in conto per le Circostanza della violazione (Valutazione 3) è 2.

Calcolo della gravità (Valutazione 4)

Il punteggio finale mostra il livello di gravità di una determinata violazione, tenendo conto dell'impatto sui diritti e libertà delle persone fisiche.

Nella tabella seguente sono riassunte le attività inerenti alla **fase di Calcolo della gravità (CG):**

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
7	Gruppo di gestione data breach / RPD	Procedere al Calcolo della ***Gravità = pt.1* pt.2 + pt.3***	Calcola la gravità della violazione applicando la formula definita dalla metodologia	Formula
8	RPD	Definire il livello di gravità della violazione	Definisce il livello di gravità (basso, medio, alto e molto alto) secondo il risultato finale della valutazione. Il risultato viene classificato secondo quattro livelli di gravità: • Basso (punteggio finale è inferiore a 2) • Medio (punteggio finale è tra 2 e 3) • Alto (punteggio finale è tra 3 e 4) • Molto alto (punteggio finale è superiore a 4)	Tabella livello gravità della violazione

Di seguito riportiamo le tabelle da utilizzare **per la valutazione del livello di gravità:**

Punteggio	Livello	Descrizione	Esito valutazione
Gravità < 2	**Basso**	Gli individui non saranno interessati dalla violazione o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso a reinserire informazioni, fastidi, etc.).	Non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma l'incidente deve essere annotato all'interno del registro delle violazioni.
2 ≤ Gravità < 3	**Medio**	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi dell'ente, paura, mancanza di comprensione, stress, disturbi fisici minori, etc.).	Non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma devono essere adottate ulteriori misure organizzative e tecniche al fine di migliorare la sicurezza dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni.
3 ≤ Gravità < 4	**Alto**	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.).	È necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni.
4 ≤ Gravità	**Molto Alto**	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, etc.).	È necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, darne comunicazione ai soggetti interessati e annotare l'incidente all'interno del registro delle violazioni.