regione campania
aslnapoli3sud

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
TEL 081/8490645- PROTOCOLLO@PEC.ASLNAPOLI3SUD.IT

METODOLOGIA DI VALUTAZIONE DELLA GRAVITA' DI UN PERSONAL DATA BREACH

Autori:	Dott.ssa Alessia Cifaldi Dott. Giuseppe Napolitano	**UOS Privacy**
Approvato da:	Avv. Stefano Rotondo	**DPO**
Accettato da:	Dott. Giuseppe Russo	**Direttore Generale ASL Napoli 3 Sud**

STORICO DELLE REVISIONI			
Vers.	**Data di rilascio**	**Motivo della revisione**	**Autore**
1	2025	Prima versione	UOS Privacy
L'ultima revisione sostituisce qualsiasi revisione precedente.			

SEDE LEGALE
VIA MARCONI N. 66 – 80059 TORRE DEL GRECO
DIREZIONE GENERALE
TEL 081/8490645- PROTOCOLLO@PEC.ASLNAPOLI3SUD.IT

Metodologia di valutazione della gravità di un Personal Data Breach

Di seguito viene riportata la metodologia per la valutazione della gravità delle violazioni dei dati personali adottata. Tale metodologia è stata definita sulla base delle indicazioni fornite **dall'ENISA (European Union Agency for Network and Information Security)** contenute all'interno del documento "Recommendations for a methodology of the assessment of severity of personal *data breach*[1]".

Gli elementi chiave da tenere in considerazione in sede di valutazione della gravità, anche con riferimento al dominio di monitoraggio, risultano essere i seguenti:

- *Contesto dell'elaborazione dati* ovvero la natura dei dati violati valutata nel contesto in cui gli stessi vengono utilizzati (**DPC: Contesto elaborazione dati**)[2]
- *Facilità di identificazione dell'individuo* in base ai dati violati (**EI: Facilità di identificazione**); [3]
- *Circostanze della violazione* (violazione di riservatezza, integrità e disponibilità dei dati), che hanno un'influenza aggiuntiva sulla gravità di una violazione (**CB: Circostanze della violazione**)[4]

La valutazione della gravità della violazione, secondo la metodologia, è articolata nelle seguenti fasi operative:

- **Fase 1: Valutazione del DPC**: in questa fase si definisce il perimetro dei dati personali oggetto della violazione e si classificano gli stessi sulla base dell'appartenenza ad una delle categorie di dati previste dall' ENISA (Dati Ordinari, Dati Comportamentali, Dati Patrimoniali, Dati Particolari). La classificazione comporta l'attribuzione di un punteggio base che può essere aumentato o diminuito in funzione della presenza di fattori contestuali relativi all'elaborazione dei dati;
- **Fase 2: Determinazione della EI**: rappresenta il fattore di correzione del DPC. Infatti la criticità complessiva di una violazione dei dati può essere ridotta in base al valore di EI, ovvero in relazione alla facilità con cui, il soggetto che entra in possesso dei dati oggetto della violazione, può ricondurli o meno all'interessato a cui appartengono;
- **Fase 3: Valutazione delle CB:** in questa fase si valutano gli scenari di violazione (violazione di riservatezza, violazione di integrità, violazione di disponibilità, o eventuali intenzioni

[1] https://www.enisa.europa.eu/publications/dbn-severity

[2] Data Processing Context (DPC): Addresses the type of the breached data, together with a number of factors linked to the overall context of processing (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

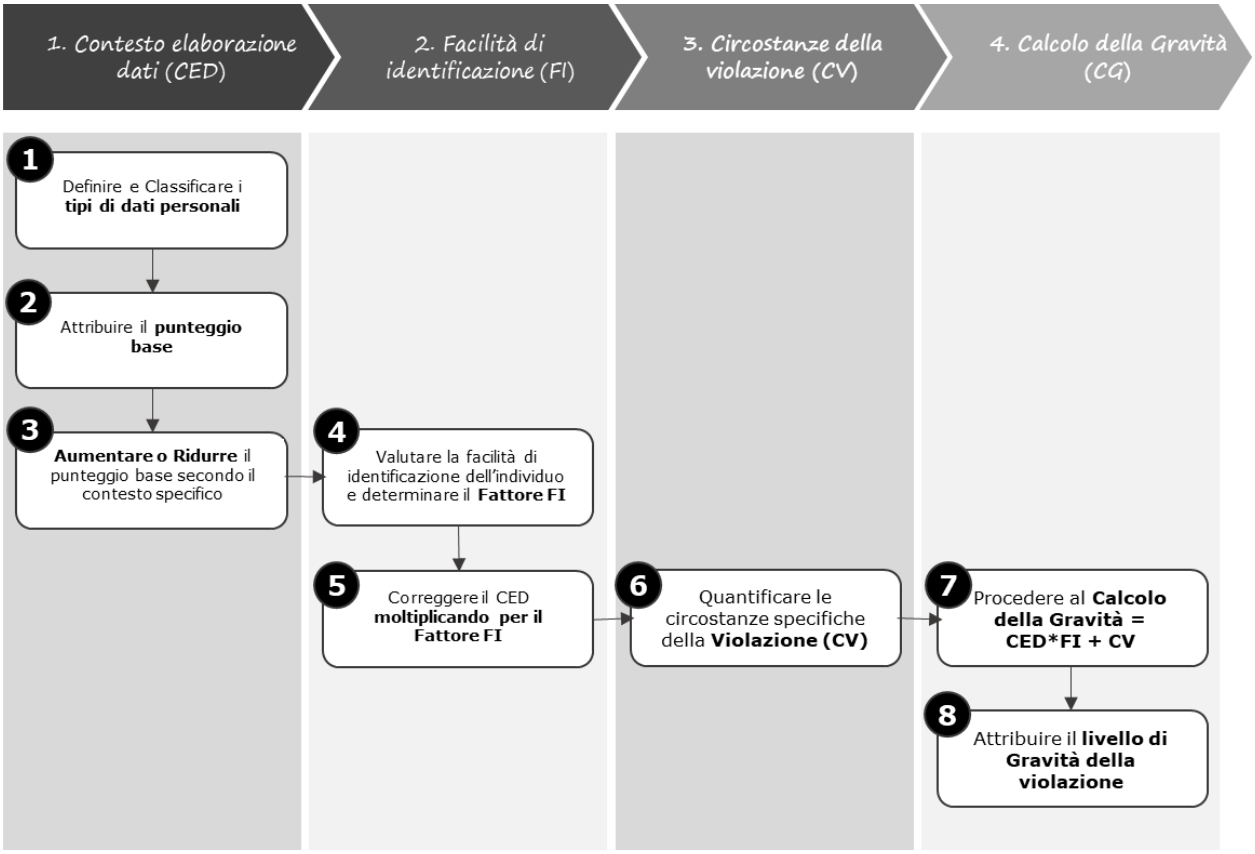
[3] Ease of Identification (EI): Determines how easily the identity of the individuals can be deduced from the data involved in the breach (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

[4] Circumstances of breach (CB): Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security

malevole) interessati o meno in seguito al Personal Data Breach. Pertanto il fattore CB, laddove presente, può solo incrementare la gravità di una specifica violazione;

- **Fase 4: Calcolo della gravità:** si giunge al calcolo della gravità della violazione sulla base dei 3 precedenti elementi DPC, EI, CB.

Viene riportata di seguito una rappresentazione del processo di valutazione della gravità della violazione sotto forma di diagramma di flusso:



Fase 1: Valutazione del contesto dell'elaborazione dei dati DPC

Il punteggio attribuito al DPC è al centro della Metodologia in quanto consente di valutare la criticità e la dimensione della violazione nel contesto di trattamento specifico.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti
1- Definire e Classificare i tipi di dati personali	Definire e classificare la tipologia di dato trattato che ha subito una violazione sulla base delle seguenti quattro macro-categorie: • Dati Ordinari; • Dati Comportamentali; • Dati Patrimoniali; • Dati Particolari.	*Procedura Operativa Gestione Data Breach)*
2- Attribuire il punteggio base	Attribuisce il punteggio base secondo la **Tabella 3 - DPC**	*TABELLA 3 – CONTESTO ELABORAZIONE DATI (DPC)*
3- 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 del DPC può variare da 1 a 4.	*TABELLA 3 – CONTESTO ELABORAZIONE DATI (DPC)*

Di seguito si riporta la Tabella da utilizzare **per la valutazione del DPC:**

Contesto Elaborazione Dati (DPC):		Punteggio
Dati Ordinari	**Esempio Dati Ordinari: Nome, Cognome Numero di Telefono, Indirizzo, Email, Fotografia, Data di nascita, Stato di famiglia, Titolo di Studi, Lavoro, Inquadramento lavorativo, etc.**	
	Punteggio Base: quando la violazione riguarda "Dati Ordinari" e non si è a conoscenza di alcun fattore aggravante.	**1**
	Il punteggio DPC potrebbe essere **aumentato di 1**, ad esempio quando il volume di "Dati Ordinari e/o le caratteristiche del Titolare sono tali da ricavare un profilo della persona o possono essere formulate assunzioni sullo stato sociale/finanziario dell'individuo.	**2**
	Il punteggio DPC potrebbe essere **aumentato di 2**, ad esempio quando i "Dati Ordinari" 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**
	Il punteggio DPC 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 di Dati Comportamentali: Abitudini, preferenze personali e interessi, vita sociale, affidabilità, spostamenti, ubicazione etc.**	
	Punteggio Base: quando la violazione comporta "Dati Comportamentali" e non si è a conoscenza di fattori aggravanti o di diminuzione.	**2**
	Il punteggio DPC 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 DPC 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 DPC può essere **aumentato di 2**, ad esempio se è possibile creare un profilo basato sui dati sensibili di una persona.	**4**
Dati Patrimoniali	**Esempio di Dati Patrimoniali: IBAN, Numero di conto, Saldo conto, Transaction History, Informazione di base sulla carta di credito (senza CVC), Complete informazioni sulla carta di credito (con CSV), Dati sui mutui/prestiti**	
	Punteggio Base: quando la violazione riguarda "Dati Patrimoniali" e non si è a conoscenza di fattori aggravanti o di diminuzione.	**3**
	Il punteggio DPC potrebbe essere **diminuito di 2**, ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni patrimoniali dell'individuo (ad esempio, il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	**1**
	Il punteggio DPC potrebbe essere **diminuito di 1**, ad esempio quando il set di dati specifici include alcune informazioni patrimoniali ma non fornisce ancora informazioni significative sullo stato / sulla situazione patrimoniale dell'individuo (ad esempio: i numeri di conti bancari semplici senza ulteriori dettagli).	**2**
	Il punteggio DPC 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 patrimoniali (ad esempio: informazioni complete sulla carta di credito con il codice CVC)	**4**
Dati Particolari	**Esempio di Dati Particolari: 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 non si è a conoscenza di alcun fattore di diminuzione.	**4**

	Il punteggio DPC 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 DPC potrebbe essere **diminuito di 2**, ad esempio quando la natura dei dati può portare a ipotesi generali e non specifiche di un individuo.	**2**
	Il punteggio DPC potrebbe essere **diminuito di 1**, ad esempio quando la natura dei dati può portare a supposizioni su informazioni sensibili di un individuo.	**3**

TABELLA 3 – CONTESTO ELABORAZIONE DATI (DPC)

Se i dati corrispondono a più di una categoria, è necessario seguire i passaggi sopra indicati per ogni categoria applicabile. In questi casi il valore da utilizzare per il calcolo complessivo della gravità **sarà il punteggio massimo raggiunto.**

Fase 2: Determinazione del punteggio per la facilità di identificazione (EI)

Il punteggio del EI è il fattore di correzione del DPC e consente di valutare, secondo la Tabella 4, la facilità di identificazione del soggetto interessato in base ai dati violati.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti
4- Valutare la facilità di identificazione del soggetto interessato e determinare il fattore EI	Valuta la **facilità di identificazione** del soggetto interessato ed attribuisce un punteggio secondo la **Tabella 4 - EI** definita dalla Metodologia secondo i seguenti quattro livelli: • trascurabile (0,25); • limitato (0,5); • significativo (0,75); • massimo (1). Il fattore di correzione EI può variare da 0,25 a 1. Il **punteggio più basso** viene attribuito quando la possibilità di identificare il soggetto interessato 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 4 – FACILITÀ DI IDENTIFICAZIONE (EI)*

5- Correggere il DPC moltiplicando con il fattore EI	Una volta individuato il fattore di correzione, esso viene moltiplicato per il DPC, al fine di determinare il punteggio iniziale della gravità della violazione dei dati.	***DPC * EI***

Di seguito si riporta la Tabella da utilizzare per la **valutazione del criterio (EI):**

Facilità di identificazione (EI)	Punteggio	Livello
La violazione riguarda dati identificativi o dati personali **non direttamente identificabili (ad esempio: nome/cognome molto diffuso in un paese, indirizzo email che non rileva altre informazioni come il nome dell'individuo e che non è usato come indirizzo email principale nei siti internet, nei forum o per i social networks, immagine non nitida e vaga)**	**0,25**	**Trascurabile**
La violazione riguarda i dati identificativi **di un individuo ma non facilmente identificabile (ad esempio: nome/cognome condiviso da poche persone in un intero paese, immagine non chiara e nitida ma che contiene informazioni aggiuntive come uno specifico luogo)**	**0,5**	**Limitata**
La violazione riguarda dati identificativi e **rivela ulteriori informazioni di identificazione dell'individuazione (ad esempio: nome completo con l'indicazione dell'indirizzo email di questa persona, indirizzo email che non rileva altre informazioni come il nome dell'individuo ma è usato come indirizzo email principale nei siti internet, nei forum o per i social networks, immagina nitida ma che non fornisce informazioni aggiuntive)**	**0,75**	**Significativo**
La violazione 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, indirizzo email che rileva il nome dell'individuo e che è usato come indirizzo email principale nei siti internet, nei forum e per i social networks, immagine chiara che rileva ulteriori informazioni sull'appartenenza di un individuo ad uno specifico gruppo o indirizzo di casa)**	**1**	**Massimo**

TABELLA 4 – FACILITÀ DI IDENTIFICAZIONE (EI)

Fase 3: Valutazione delle Circostanze della Violazione (CB)

Il punteggio del CB quantifica le **circostanze specifiche della violazione,** ovvero gli scenari di ambiti di violazione, che possono essere presenti o meno in una particolare situazione.

Nella tabella seguente sono riassunte le attività svolte in questa fase:

Attività	Descrizione	Strumenti
6- Quantificare le circostanze specifiche della violazione (CB)	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. Le circostanze possono avere solo un'influenza aggiuntiva sulla gravità di una violazione. Il punteggio del CB può incrementare il punteggio precedentemente ottenuto delle gravità di 0,25 o 0,5 a seconda dei casi.	*TABELLA 5 – CIRCOSTANZE DELLA VIOLAZIONE (CB)*

Di seguito si riporta la tabella da utilizzare per la **valutazione del terzo indicatore (CB):**

Circostanze della violazione (CB)		Punteggio
Violazione di riservatezza	**Definizione:** La perdita di riservatezza si verifica quando le informazioni **sono 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 clienti possono accedere agli account di altri clienti 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 degli utenti;	**0,5**

	- Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni.	
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 erroneamente aggiornate ma è stata effettuata una copia dell'originale prima del verificarsi della modifica.	**0**
	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 di un'azienda condivide intenzionalmente dati privati dai clienti in un sito pubblico di social media. - Un dipendente di un'azienda vende dati privati dei clienti a un'altra società. - Un membro di un social network invia intenzionalmente delle informazioni sugli altri membri ai propri familiari al fine di danneggiarli.	**0,5**

TABELLA 5 – CIRCOSTANZE DELLA VIOLAZIONE (CB)

Fase 4: Calcolo della Gravità

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 **la fase di Calcolo della gravità (CG):**

Attività	Descrizione	Strumenti
7- Procedere al Calcolo della Gravità	Calcola la gravità della violazione applicando la formula definita dalla Metodologia	*Formula:* ***CG = DPC * EI + CB***
8- 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 6 – LIVELLO DI GRAVITÀ*

Di seguito si riporta la tabella da utilizzare **per la valutazione del livello di gravità:**

Punteggio	Livello	Descrizione
Gravità < 2	**Basso**	È **improbabile** che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, che potrebbero solamente subire degli inconvenienti minori facilmente risolvibili (necessità di inserire nuovamente i propri dati personali, disagi minori, irritazione, etc.)
2 ≤ Gravità < 3	**Medio**	È **probabile** che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare taluni disagi, che saranno in grado di superare nonostante alcune difficoltà (costi

		aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, discriminazione lieve, stress, etc.).
3 ≤ Gravità < 4	**Alto**	È **probabile** che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in black-list, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento delle condizioni di salute, etc.).
4 ≤ Gravità	**Molto Alto**	È **probabile** che si verifichi una violazione dei diritti e delle libertà per gli individui interessati, i quali potrebbero incontrare conseguenze significative, o addirittura irreversibili, che difficilmente riusciranno a superare (difficoltà finanziarie, incapacità lavorativa, disturbi psicologici o fisici a lungo termine, gravi lesioni o morte, etc.).

TABELLA 6 – LIVELLO DI GRAVITÀ

<u>Ulteriori valutazioni</u>

Ai sensi delle "*Guidelines on Personal data breach notification under Regulation 2016/679*"[5] (WP250rev.01) qualora la violazione di dati personali subita riguardi:

- **Dati personali adeguatamente cifrati** (i) con algoritmi considerati sufficientemente sicuri e adeguati (ii) dove la chiave di sicurezza non risulti in alcun modo compromessa;

E, al contempo:

- Siano presenti **copie e/o backup dei dati** coinvolti nella violazione, che ne consentono un pronto ripristino.

si può affermare che i dati personali non sono accessibili da terze parti non autorizzate al trattamento e che **non sussistono** - o che sono improbabili **- rischi per i diritti e le libertà degli interessati.**

Pertanto, in tale ipotesi il livello finale di gravità di una determinata violazione sarà automaticamente valutato come **Basso**.

[5] Si veda pag. 18 del WP250 rev.01