



*Procedura operativa per la gestione
delle violazioni dei dati personali
"Personal Data Breach"*

-versione 1.0-

¹ Allegato inserito dall'art. 23, comma 1, del r.r., 27 aprile 2023, n. 3, pubblicato sul Bur Lazio del 2 maggio 2023, n.35.

Sommario

- 1. Premessa e obiettivi**
 - 1.1. Premessa**
 - 1.2. Ambito di applicazione**
 - 1.3. Obiettivi**
 - A. DEFINIZIONE DELLA PROCEDURA, RUOLI E RESPONSABILITÀ**
 - 1. Procedura operativa generale**
 - 2. Ruoli e Responsabilità**
 - B. PROCEDURA OPERATIVA**
 - 1. Segnalazione**
 - 2. Identificazione**
 - 3. Valutazione**
 - 4. Gestione e risposta**
 - 5. Post Incident Review**
 - 6. ALLEGATI**
 - Allegato A: Registro Data Breach**
 - Allegato B: Data Breach Report**
 - Allegato C: Metodologia di valutazione della gravità di un Data Breach**
 - 1. Premessa e Obiettivi**
 - 2. Approccio metodologico**
 - 2.1. Valutazione del contesto dell'elaborazione dei dati (CED)**
 - 2.2. Determinazione del punteggio per la facilità di identificazione (FI)**
 - 2.3. Valutazione delle Circostanze della violazione (CV)**
 - 2.4. Calcolo della Gravità**

1. Premessa e obiettivi

1.1. Premessa

Il 24 maggio 2016 è entrato in vigore il "Regolamento (UE) 2016/679 (RGDP), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). A partire dal 25 maggio 2018 tale regolamento è pienamente applicabile in tutti gli Stati membri. Elemento cardine della suddetta normativa è il concetto di "accountability" con il quale viene introdotta la responsabilizzazione dei soggetti coinvolti nella protezione dei dati personali e la capacità di rendere conto delle proprie azioni.

Una delle novità introdotte dal RGDP è costituita dal processo di gestione dei Data Breach, eventi di violazione dei dati personali. Il presente documento descrive la procedura che la Giunta della Regione Lazio adotta per la gestione degli eventi anomali e degli incidenti di violazione dei dati personali.

1.2. Ambito di applicazione

La presente procedura si applica ad ogni evento che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali² trasmessi, conservati o trattati dalla Giunta della Regione Lazio nel ruolo di Titolare. (di seguito anche "Data Breach" o "Violazione dei dati personali")³.

In particolare, secondo quanto previsto dal WP250 "Guidelines on Personal Data Breach notification under Regulation 2016/679", gli eventi di possibile violazione dei dati personali possono essere classificati in tre macrocategorie:

- "Violazione di confidenzialità": in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali;
- "Violazione di disponibilità": in caso di perdita accidentale o non autorizzata dell'accesso ai dati o la distruzione di dati personali;
- "Violazione di integrità": in caso di alterazione non autorizzata o accidentale dei dati personali.

Inoltre, una violazione potrebbe comportare contemporaneamente una compromissione della confidenzialità, della disponibilità e dell'integrità dei dati personali.

² «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; (art. 4, n.1, RGPD)

³ «violazione dei dati personali»: 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, n.12, RGPD)

Ai sensi dell'articolo 33 del RGPD, la **notifica** della violazione **al Garante per la Protezione dei Dati Personali** (nel seguito anche "Garante") deve avvenire senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui si venga a conoscenza della violazione**, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Ai sensi dell'articolo 34 del RGPD, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento **comunica la violazione all'interessato senza ingiustificato ritardo**.

Si rinvia alle PB⁴ 01/2021 per gli esempi riguardanti la notifica di violazione dei dati.

1.3. Obiettivi

Nel presente documento vengono definite ed individuate le attività, i ruoli e le responsabilità nella gestione dei "Data Breach".

Il documento contiene le indicazioni operative e le informazioni necessarie per garantire il governo e l'attuazione del processo di gestione dei Data Breach.

Il presente documento si articola in due differenti sezioni:

A. DEFINIZIONE DELLA PROCEDURA, RUOLI E RESPONSABILITÀ che ha l'obiettivo di:

- definire la procedura operativa generale di gestione delle violazioni di dati personali trasmessi, conservati o trattati dalla Giunta della Regione Lazio nel ruolo di Titolare;
- individuare i ruoli e le responsabilità degli attori coinvolti nella procedura;

B. PROCEDURA OPERATIVA DI GESTIONE che ha l'obiettivo di:

- declinare analiticamente le fasi di gestione operativa delle potenziali violazioni di dati personali.

A. Definizione della procedura, ruoli e responsabilità

1. Procedura operativa generale

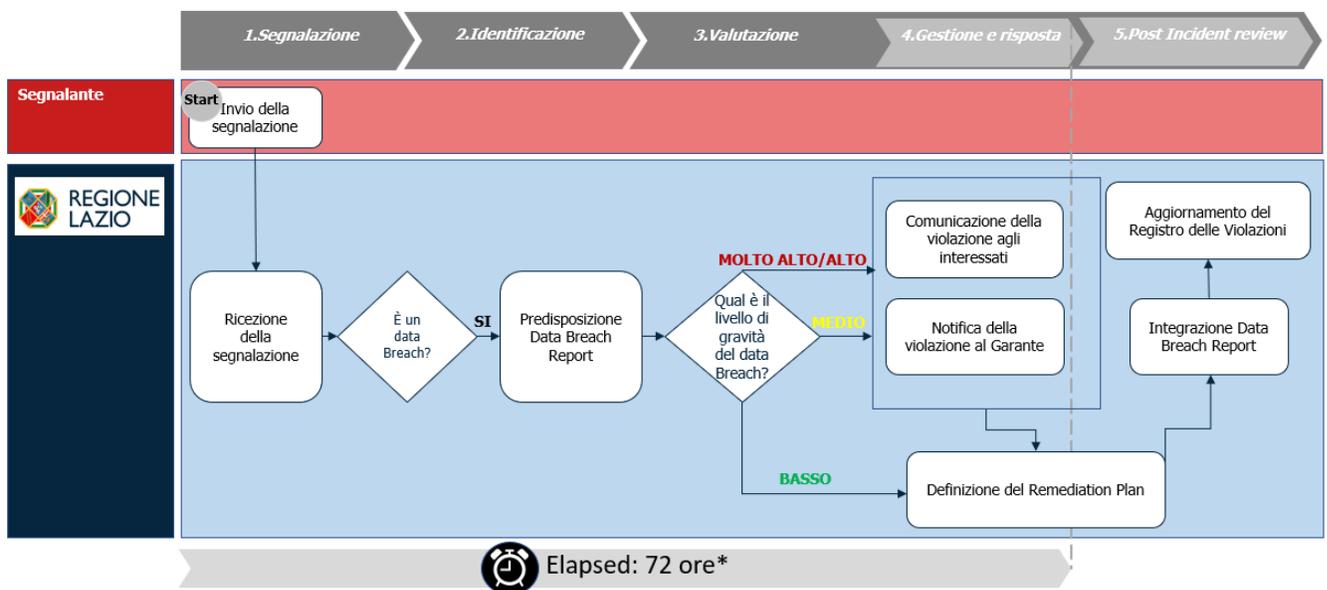
Ogni violazione dei dati personali, occorsa nell'ambito di trattamenti di dati personali trasmessi, conservati o trattati dalla Giunta della Regione Lazio nel ruolo di Titolare, deve essere gestita secondo quanto previsto nelle fasi descritte di seguito:



⁴ European Data Protection Board (https://edpb.europa.eu/edpb_it)

- **Segnalazione:** fase di segnalazione/ricezione di un potenziale Data Breach;
- **Identificazione:** fase in cui la segnalazione ricevuta viene identificata come un Data Breach o come altro incidente di sicurezza (*falso positivo*); se si tratta di Data Breach, viene predisposto il **Data Breach Report** sulla base delle informazioni al momento disponibili e si procede alle fasi successive;
- **Valutazione:** fase di analisi e stima della gravità del Data Breach con riferimento ai diritti ed alle libertà delle persone fisiche coinvolte, sulla base delle informazioni al momento disponibili. Tale fase si protrae anche in seguito, in funzione di nuove informazioni rilevate.
- **Gestione e risposta:** in base al livello di gravità del Data Breach, la Giunta della Regione Lazio dovrà comunicare la violazione agli interessati e/o al Garante; inoltre, in tale fase, viene definito il **Remediation Plan** al fine di porre rimedio alla violazione e per attenuarne i possibili effetti negativi;
- **Post Incident Review:** fase conclusiva di analisi ex post della violazione al fine di comprendere le cause, apprendere dagli errori e valutare le opportunità di miglioramento; in tale fase viene ulteriormente integrato il **Data Breach Report**.

Nella figura seguente è rappresentato il diagramma di flusso del processo di gestione delle violazioni dei dati personali.



* Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

2. Ruoli e Responsabilità

La tabella seguente descrive i ruoli e le responsabilità previsti all'interno della presente procedura operativa.

Codice	Attore	Ruolo
TT	Titolare del Trattamento	<p>Il Titolare del trattamento, ovvero la Giunta della Regione Lazio, ha la responsabilità ultima della corretta gestione delle violazioni dei dati personali trasmessi, conservati o trattati. Si avvale delle strutture organizzative della Giunta regionale per la segnalazione, l'identificazione, la valutazione e gestione e risposta alle violazioni di dati personali e per il post incident review.</p>
TDB	Team Data Breach	<p>Il team Data Breach, formato da alcuni soggetti designati dal Titolare e dal DPO regionale, si attiva a seguito di ogni segnalazione, con la seguente composizione:</p> <ul style="list-style-type: none"> • DPO regionale • Soggetto designato competente in materia di protezione dei dati personali • Soggetto designato competente in materia di sistemi informativi • Soggetto designato competente per materia <p>Il Team segue tutte le fasi della presente procedura.</p>
DPO	Data Protection Officer - DPO	<p>Il DPO supporta il Titolare nell'intero processo di gestione del Data Breach.</p>
SDP	Soggetto designato competente in materia di protezione dei dati personali	<p>Il soggetto designato competente in materia di protezione dei dati personali, nella fase di Identificazione, con il supporto del Team, stabilisce se la segnalazione costituisca una violazione. Nella fase di Valutazione, supporta il Team nella valutazione del livello di gravità. Nella fase di Gestione e Risposta supporta il Team nella predisposizione della notifica al Garante e agli interessati, nonché nell'elaborazione del Remediation Plan.</p> <p>Nella fase di Post Incident review, con il supporto del Team, aggiorna il Data Breach Report ed il Registro delle Violazioni.</p>
ICT	Soggetto designato competente in materia di sistemi informativi	<p>Il soggetto designato competente in materia di sistemi informativi, nella fase di identificazione, supporta il Team per stabilire se la segnalazione costituisca una violazione. Nella fase di valutazione, supporta il Team nella valutazione del livello di gravità. Nella fase di gestione e risposta, in collaborazione con il Team, supporta la predisposizione della notifica al Garante e agli interessati. Nella medesima fase</p>

		<p>collabora alla stesura del Remediation Plan e, in attuazione dello stesso, adotta le conseguenti azioni ricadenti nell'ambito della gestione dei sistemi informativi.</p> <p>Nella fase di Post Incident review fornisce, collaborando con il Team, informazioni per l'aggiornamento del Data Breach Report e del registro delle violazioni.</p>
SDC	Soggetto designato competente	<p>Il soggetto designato che ha competenza sul trattamento rispetto al quale è stata segnalata una potenziale violazione, nella fase di Identificazione, supporta il Team per stabilire se la segnalazione costituisca una violazione. Nella fase di valutazione, con il supporto del Team, valuta il livello di gravità della violazione. Nella fase di gestione e risposta, in collaborazione con il Team, predispone e trasmette la notifica al Garante e agli interessati. Nella medesima fase collabora alla stesura del Remediation Plan e, in attuazione dello stesso, adotta le conseguenti azioni ricadenti nell'ambito organizzativo di propria competenza.</p> <p>Nella fase di Post Incident review fornisce, collaborando con il Team, informazioni per l'aggiornamento del Data Breach Report e del registro delle violazioni.</p>
DG	Direttore Generale	<p>Il Direttore Generale viene informato dal Team in tutte le fasi del processo, a seguito dell'identificazione di un data breach. Emanava eventuali disposizioni di competenza che dovessero rendersi necessarie nelle azioni di remediation.</p>
SS	Soggetto che effettua la segnalazione	<p>Soggetto che segnala all'Amministrazione un potenziale Data Breach.</p>

B. PROCEDURA OPERATIVA

In questa Sezione vengono declinate in modo analitico le fasi del processo di gestione del Personal Data Breach adottate dal Titolare.



Per ogni step del processo vengono definiti mediante la matrice RACI⁵ i ruoli e le responsabilità degli attori coinvolti nella procedura di gestione dei Data Breach.

⁵ La matrice RACI specifica il tipo di relazione fra la risorsa e l'attività: Responsible, Accountable, Consulted, Informed. Responsible (R)= è colui che esegue e assegna l'attività; **Accountable (A)** è colui che ha la responsabilità sul risultato dell'attività. A differenza degli altri tre ruoli, per

1. Segnalazione



R	A	C	I
SS	SS	TDB	

R=Esecutore A=Responsabile C=Coinvolto I=Informato

In qualsiasi momento i dipendenti e/o il personale della Giunta della Regione Lazio o altri possibili soggetti segnalanti, che rilevino un potenziale Data Breach, devono darne tempestivamente comunicazione attraverso l'indirizzo e-mail dedicato databreach@regione.lazio.legalmail.it

E' possibile che le segnalazioni, soprattutto qualora provenienti da terze parti esterne alla Giunta di Regione Lazio (es. utenti, fornitori), vengano ricevute attraverso un canale di comunicazione diverso da quello sopra indicato, quale ad esempio:

- o Posta ordinaria;
- o Posta elettronica;
- o Indirizzo PEC diverso da quello sopra indicato
- o Comunicazione allo sportello - URP della Giunta della Regione Lazio

In questi casi, il soggetto incaricato della Giunta della Regione Lazio che ha ricevuto la segnalazione, di un potenziale Data Breach informa tempestivamente e senza ingiustificato ritardo il Soggetto designato (ad esempio il Direttore regionale) e contestualmente trasmette la segnalazione all'indirizzo databreach@regione.lazio.legalmail.it.

Stante il limitato arco temporale a disposizione del Titolare, per comunicare all'Autorità l'eventuale Data Breach (72 ore solari dalla ricezione della segnalazione) tutti i soggetti incaricati ricevuti le segnalazioni sono tenuti a trasmetterle tempestivamente all'indirizzo

ciascuna attività deve essere univocamente assegnato.; **Consulted (C)**= è la persona che aiuta e collabora con il *Responsible* per l'esecuzione dell'attività; **Informed (I)**= è colui che deve essere informato, al momento dell'esecuzione dell'attività o (spesso) al suo completamento.

databreach@regione.lazio.legalmail.it e a fornire prontamente il proprio supporto in caso di qualsiasi dubbio sulla natura della richiesta.

Si riportano di seguito alcune caratteristiche che possano aiutare a rilevare un evento anomalo che possa rappresentare un potenziale Data Breach:

- Qualsiasi evento di un sistema o servizio che tratti dati personali o di rete che sia indicativo di una possibile violazione della politica di sicurezza delle informazioni;
- Un fallimento di una misura di sicurezza;
- Un malfunzionamento del pc o dei programmi utilizzati (ad esempio antivirus, firewall, sistemi di rilevamento delle intrusioni);
- Una situazione anomala o precedentemente sconosciuta che potrebbe essere rilevante per la sicurezza.
- La rilevazione di dati personali diffusi pubblicamente in Internet

A titolo esemplificativo e non esaustivo vengono riportate di seguito alcune tipologie di violazione che potrebbero tradursi in Data Breach qualora dovessero coinvolgere i dati personali:

- **distruzione di dati informatici o documenti cartacei** (intesa come indisponibilità irreversibile di dati con accertata impossibilità di ripristino degli stessi), conseguente ad eliminazione logica (es. errata cancellazione dei dati nel corso di un intervento manuale o automatizzato) o fisica (es. rottura di dispositivi di memorizzazione informatica, incendio/allagamento locali dove sono archiviati i contratti ed altri documenti dei clienti);
- **perdita di dati, conseguente a smarrimento/furto di supporti** informatici (es. laptop, HD, memory card) o di documentazione contrattuale o altri documenti cartacei (in originale o in copia);
- **accesso non autorizzato o intrusione a sistemi informatici**, lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione oppure attraverso la compromissione o rilevazione abusiva di credenziali di autenticazione (es. userid e password) per l'accesso ai sistemi;
- **modifica non autorizzata di dati**, derivante ad esempio da un'erronea esecuzione di interventi sui sistemi informatici o da intervento umano;
- **rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati, conseguenti ad esempio, al fornire informazioni, anche verbali, a persone diverse dal soggetto legittimato (in assenza di delega formale di quest'ultimo), all'invio di fatture o altri documenti di valore contrattuale a soggetti diversi dall'effettivo destinatario o alla errata gestione di supporti informatici.

A seguito della segnalazione, il Soggetto designato competente in materia di dati personali convoca, anche per le vie brevi, il Team Data Breach che si occuperà della gestione di tutte le fasi successive del processo.

2. Identificazione

1. Segnalazione

2. Identificazione

3. Valutazione

4. Gestione e risposta

5. Post Incident review

R	A	C	I
SDP	TT	TDB	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

- Dopo aver raccolto tutte le informazioni necessarie e disponibili, il Soggetto designato in materia di protezione dei dati personali valuta la segnalazione ricevuta e:
 - se ritiene che non si tratti di un Data Breach, informa il Team Data Breach e, salve obiezioni e/o contestazioni che comportino la necessità di una rivalutazione della segnalazione come violazione dei dati personali, conclude il procedimento, dandone comunicazione al soggetto che ha segnalato il potenziale data breach;
 - se ritiene che si tratti di un **Data Breach**, lo notifica al Team e informa il Direttore Generale.
- A seguito della identificazione di un Data Breach, il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con la collaborazione del TDB:
 - raccoglie tutte le informazioni disponibili, predisponendo il **Data Breach Report (Allegato B)** e coinvolgendo eventualmente anche altri soggetti designati e nominati responsabili del trattamento;

In ogni caso, se la segnalazione riguarda una violazione di natura informatica, il Team Data Breach ed in particolare la Direzione regionale competente in materia di sistemi informativi provvedono ad attivare la specifica procedura adottata dalla Giunta regionale per la gestione incidenti di sicurezza informatica.

3. Valutazione

1. Segnalazione

2. Identificazione

3. Valutazione

4. Gestione e risposta

5. Post Incident review

R	A	C	I
SDC	SDC	TDB	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

In base alle informazioni raccolte nel Data Breach Report (**Allegato B**), il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con il supporto del Team, valuta la "gravità" (severity) del Data Breach mediante la "**Metodologia di valutazione della gravità di un Data Breach**" (**Allegato C**), stimando il potenziale rischio per i diritti e le libertà delle persone fisiche.

In alternativa, è utilizzabile lo strumento di auto-assesment di valutazione per la notifica di una violazione dei dati personali (Data Breach) presente sul sito web del Garante al seguente link <https://servizi.gpdp.it/databreach/s/self-assessment>.

Ai fini del calcolo del punteggio di gravità dei Data Breach vengono utilizzati i criteri fondamentali stabiliti dalla metodologia e dalle raccomandazioni stilate da ENISA (European Union Agency for Network and Information Security), "*Recommendations for a methodology of the assesment of severity of personal data breaches*" (by Enisa – European Union Agency for Network and Information Security).

All'esito di questa fase, il livello di "gravità" (severity) del Data Breach potrà essere:

Livello	Descrizione
Basso	Gli interessati non sono stati impattati o potrebbero incontrare alcuni inconvenienti superabili senza particolari difficoltà (tempo trascorso a reinserire informazioni, disagi minori, etc.).
Medio	Gli interessati possono incontrare taluni disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, discriminazione lieve, incomprendione, stress, etc.).
Alto	Gli interessati possono subire 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.).
Molto Alto	Gli interessati possono incontrare conseguenze significative, o addirittura irreversibili, che difficilmente riusciranno a superare (difficoltà finanziarie, debito sostanziale, incapacità lavorativa, disturbi psicologici o fisici a lungo termine, gravi lesioni o morte, etc.).

4. Gestione e risposta



R	A	C	I
SDC	SDC	TDB	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

In base al livello di gravità del Data Breach definito nella fase precedente, il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione procede con:

- la comunicazione agli interessati coinvolti nella violazione dei dati
- la notifica al Garante della violazione dei dati personali

secondo le regole sintetizzate in tabella:

Livello di rischio	Ove possibile entro le 72 ore	Senza ingiustificato ritardo
	<i>Notifica al garante</i>	<i>Comunicazione all'interessato</i>
Rischio molto alto/alto	SI	SI
Rischio medio	SI	NO
Rischio basso	NO	NO

Comunicazione agli interessati

Qualora la valutazione della "gravità" (severity) del Data Breach presenti un rischio alto/molto alto per i diritti e le libertà delle persone fisiche, il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con il supporto del Team, dà comunicazione agli interessati senza ingiustificato ritardo tramite opportuno strumento di comunicazione.

Possano verificarsi i seguenti casi:

1. sono state adottate preventivamente dal titolare del trattamento, 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;
2. la Giunta della Regione Lazio ha adottato misure successive alla violazione, che garantiscano la riduzione del rischio ad un livello considerato come medio/basso per i diritti e le libertà degli interessati;
3. la comunicazione all'interessato comporta sforzi sproporzionati.

Ai sensi dell'articolo 34, paragrafo 5, del RGPD:

- Nei casi 1 e 2 non dovrà essere effettuata alcuna comunicazione agli interessati.
- Nel caso 3 il soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con il supporto del Team Data Breach, dovrà valutare una modalità consona per darne comunicazione pubblica in modo tale che gli interessati vengano informati in modo efficace.

Notifica al Garante Privacy

A norma dell'articolo 33 del RGPD è prevista la notifica della violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare ne sia venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

La notifica viene effettuata dal soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione, con il supporto del Team Data Breach, attraverso l'apposita procedura telematica resa disponibile dal Garante nel portale dei servizi online dell'Autorità, raggiungibile all'indirizzo <https://servizi.gpdp.it/databreach/s/> (*Provvedimento del 27 maggio 2021*).

Al fine di garantire uniformità delle notifiche/comunicazioni dirette rispettivamente all'Autorità di controllo e agli interessati, il legislatore europeo ha indicato le seguenti informazioni minime che le stesse devono contenere:

Contenuto notifica diretta all'autorità di controllo ⁶	Contenuto comunicazione all'interessato
<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Descrizione con linguaggio semplice e chiaro della natura della violazione dei dati personali

⁶ Qualora e nella misura in cui **non sia possibile fornire le informazioni contestualmente**, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

<ul style="list-style-type: none"> • Nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni 	<ul style="list-style-type: none"> • Nome e i dati di contatto del DPO o di altro punto di contatto presso cui ottenere più informazioni
<ul style="list-style-type: none"> • Probabili conseguenze della violazione dei dati personali 	<ul style="list-style-type: none"> • Probabili conseguenze della violazione dei dati personali
<ul style="list-style-type: none"> • Descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi 	<ul style="list-style-type: none"> • Descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

Remediation Plan

Il soggetto designato competente in materia di protezione dei dati personali, con il supporto del Team, definisce in questa fase un piano per porre rimedio alla violazione e attenuarne i possibili effetti negativi, con il supporto del Team e, in particolare:

- per la componente del Data Breach di natura tecnico-informatica, del soggetto designato competente in materia di sistemi informativi, tenendo in considerazione e/o integrando il piano con le risultanze dell'attività di gestione degli incidenti di sicurezza informatica ("Identificare e definire le modalità di risoluzione dell'incidente");
- per la componente del Data Breach di natura fisica e organizzativa, del soggetto designato che ha competenza sul trattamento rispetto al quale è stata identificata una violazione.

Ciascun soggetto designato ed eventualmente le altre strutture regionali interessate, per la parte di propria competenza, attuano le azioni definite nel remediation plan.

5. Post Incident Review



R	A	C	I
SDP	SDP	TDB	DG

R=Esecutore A=Responsabile C=Coinvolto I=Informato

La fase di Post Incident Review è la fase conclusiva di integrazione del Data Breach Report e di analisi *ex post* della violazione al fine di comprendere le cause del Data Breach, apprendere dagli errori e valutare le opportunità di miglioramento.

Il Data Breach Report (**Allegato B**) confluisce nel **Registro Data Breach (Allegato A)** che consentirà al Titolare di documentare "qualsiasi violazione dei dati personali, comprese le

circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.”
(articolo 35, paragrafo 5, del RGPD).

Tale Registro consentirà al Garante di verificare, in caso di ispezione o richiesta di specifica, il rispetto degli adempimenti in capo al Titolare nella gestione delle violazioni dei dati personali.

6. Allegati

ID	Allegato	
A	Registro Data Breach	
B	Data Breach Report	
C	Metodologia di valutazione della gravità di un Data Breach	

Allegato A



REGIONE LAZIO

Registro Data Breach

ID	Data	Ora	Struttura segnalante	Descrizione della segnalazione	E' un Data Breach?	Motivazioni della scelta	Data Breach Report	Valutazione del livello di gravità del Data Breach	Notifica al Garante	Comunicazione agli interessati	Documenti a supporto
002_2022			<input type="checkbox"/> Interna a Regione Lazio: <i>[specificare]</i>	<i>Inserire contenuto della segnalazione o link alla stessa</i>	SI	<i>Inserire le motivazioni che hanno portato alla decisione di considerare la segnalazione come Data Breach</i>	<i>Inserire/Inviare il Data Breach Report</i>	Medio	SI	NO	<i>Inserire/Inviare i documenti a supporto della notifica/comunicazione del Data Breach</i>
			<input type="checkbox"/> Esterna a Regione Lazio: <i>[specificare se fornitore o terzo]</i>								
003_2022			<input type="checkbox"/> Interna a Regione Lazio: <i>[specificare]</i>	<i>Inserire contenuto della segnalazione o link alla stessa</i>	SI	<i>Inserire le motivazioni che hanno portato alla decisione di considerare la segnalazione come Data Breach</i>	<i>Inserire/Inviare il Data Breach Report</i>	Molto Alto	SI	SI	<i>Inserire/Inviare i documenti a supporto della notifica/comunicazione del Data Breach</i>
			<input type="checkbox"/> Esterna a Regione Lazio: <i>[specificare se fornitore o terzo]</i>								



in azzurro sono indicate le informazioni da fornire in caso di comunicazione agli interessati ai sensi dell'art. 34

in grigio sono indicate le informazioni, in aggiunta alle informazioni in azzurro, da fornire nella notifica al Garante ai sensi dell'art. 33

Data Breach Report

ID progressivo	001/2022
Data Breach riportato da:	Inserire Nome e Cognome dell'Utente che ha segnalato la violazione o del soggetto terzo (es.fornitore)
Contatti dell'utente:	Inserire l'indirizzo email o il numero di telefono dell'utente che ha segnalato la violazione
Data e ora:	Indicare la data della segnalazione (gg/mese/anno) e l'ora (hh:mm)
Struttura di appartenenza:	Inserire la struttura di appartenenza dell'utente
Data Protection Officer	
Breve descrizione della violazione	Hacker entra in possesso delle credenziali, perdita o furto di un laptop, modifica dolosa dei dati di un cliente, etc.
Dispositivo oggetto di violazione	Server, dispositivo mobile, documento cartaceo, file o parte di un file, strumento di backup, strumento di rete, etc.
Tipologia di violazione	<input type="checkbox"/> Violazione, intenzionale o accidentale, alla riservatezza dei dati personali (accesso illegittimo)
	<input type="checkbox"/> Violazione, intenzionale o accidentale, all' integrità dei dati personali (modifica indesiderata)
	<input type="checkbox"/> Violazione, intenzionale o accidentale, alla disponibilità dei dati personali (scomparsa/distruzione).
Interessati	numero di interessati coinvolti <i>Indicare, ove possibile, il numero approssimativo dei soggetti impattati dalla violazione</i>
	<input type="checkbox"/> Dipendenti
	<input type="checkbox"/> Familiari dei dipendenti
	<input type="checkbox"/> Collaboratori e professionisti esterni
	<input type="checkbox"/> Fornitori
	<input type="checkbox"/> Soci
	<input type="checkbox"/> Visitatori
	<input type="checkbox"/> Clienti
	<input type="checkbox"/> Clienti potenziali
	<input type="checkbox"/> Amministratori/Sindaci
	<input type="checkbox"/> Familiari Amministratori/sindaci
	<input type="checkbox"/> Candidati all'assunzione
	<input type="checkbox"/> Stagisti/interinali
	<input type="checkbox"/> Minori
<input type="checkbox"/> Soggetti terzi	
Tipologie di Dati personali	<input type="checkbox"/> Dati ordinari
	<input type="checkbox"/> Dati particolari - sensibili
	<input type="checkbox"/> Dati particolari - giudiziari
	<input type="checkbox"/> Dati particolari - patrimoniali
	<input type="checkbox"/> Dati di videosorveglianza
	<input type="checkbox"/> Dati biometrici
	<input type="checkbox"/> Dati CRIF
	<input type="checkbox"/> Dati CR Banca d'Italia
	<input type="checkbox"/> Dati di geolocalizzazione
	<input type="checkbox"/> Dati comportamentali
<input type="checkbox"/> Log di sistema	
Volume dei dati coinvolti <i>Indicare, ove possibile, il numero approssimativo di registrazioni di dati personali oggetto di data breach</i>	
Misure di sicurezza tecnico-organizzative (ex ante)	Indicare se i dati oggetto di data breach sono protetti da tecniche di cifratura/crittografia o protetti da altre misure tecnico/organizzative che limitano ex ante gli effetti negativi per i diritti e le libertà degli interessati.
Misure di sicurezza tecnico-organizzative (ex post)	Descrivere le misure tecnico/organizzative di cui si propone l'adozione, o già adottate subito, per porre rimedio alla violazione e per attenuare i possibili effetti negativi
Conseguenze della violazione	Indicare le probabili conseguenze della violazione dei dati personali

Valutazioni del Comitato Privacy

Valutazione del livello di gravità del Data Breach		$CG = CED * FI + CV$ (ref. Metodologia di valutazione della gravità di un Data Breach)
Deve essere notificato al Garante?		Se Sì allegare il documento con il quale si è notificato il Data Breach al Garante Privacy
Deve essere comunicato agli interessati?		Se Sì, allegare il documento con il quale si è comunicato il Data Breach agli interessati
Piano di Remedation	Descrizione del piano e delle azioni puntuali di remediation che il Team Data Breach ha valutato di intraprendere per porre rimedio alla violazione e attenuarne i possibili effetti negativi	

Post incident review

Descrizione completa della violazione	Inserire la descrizione completa dell'incident e delle attività intraprese per gestirlo
cause della violazione	Inserire il risultato della root cause analysis: - cosa è successo? - come è successo? - perchè è successo?
Lezioni apprese	Indicare le "lesson learned" apprese durante la gestione dell'incidente.
Opportunità di miglioramento	Inserire le misure da porre in essere per rendere più efficiente ed efficace la gestione dell'incidente

*Metodologia di valutazione
della gravità di un Data Breach*

- documento tecnico-metodologico di supporto-

Versione 1.0

1. Premessa e Obiettivi

Il presente documento ha l'obiettivo di declinare la "Metodologia di valutazione delle violazioni dei dati personali" (di seguito anche la *Metodologia*) di cui la Giunta della Regione Lazio, titolare del trattamento, si avvale per valutare la "gravità" (severity) potenziale di un eventuale violazione dei dati personali (di seguito anche *Data Breach*), ovvero la gravità della violazione per i diritti e le libertà delle persone fisiche. 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 assesment of severity of personal data breaches*"⁷.

All'interno del documento vengono pertanto descritte le fasi della Metodologia che consentono di identificare la gravità potenziale di un determinato Data Breach. Nell'ordine:

- Valutazione del Contesto di elaborazione dei dati (**CED**)⁸
- Determinazione della Facilità di Identificazione (**FI**)⁹
- Valutazione delle Circostanze della violazione (**CV**)¹⁰
- Calcolo della Gravità (**CG**)

2. Approccio metodologico

La Metodologia adottata dal titolare del trattamento, si basa su un approccio articolato secondo le seguenti fasi:

- **Fase 1: Valutazione del CED:** 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 Sensibili). 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 FI:** si tratta della determinazione del fattore di correzione del CED. La criticità complessiva di una violazione dei dati può essere ridotta in base al valore di FI, ovvero in relazione alla facilità con cui il soggetto che entra in possesso dei dati può ricondurli o meno all'individuo a cui appartengono;
- **Fase 3: Valutazione delle CV:** in questa fase si valutano le eventuali minacce (violazione di riservatezza, violazione di integrità, violazione di disponibilità, o eventuali intenzioni

⁷ <https://www.enisa.europa.eu/publications/dbn-severity>

⁸ **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")

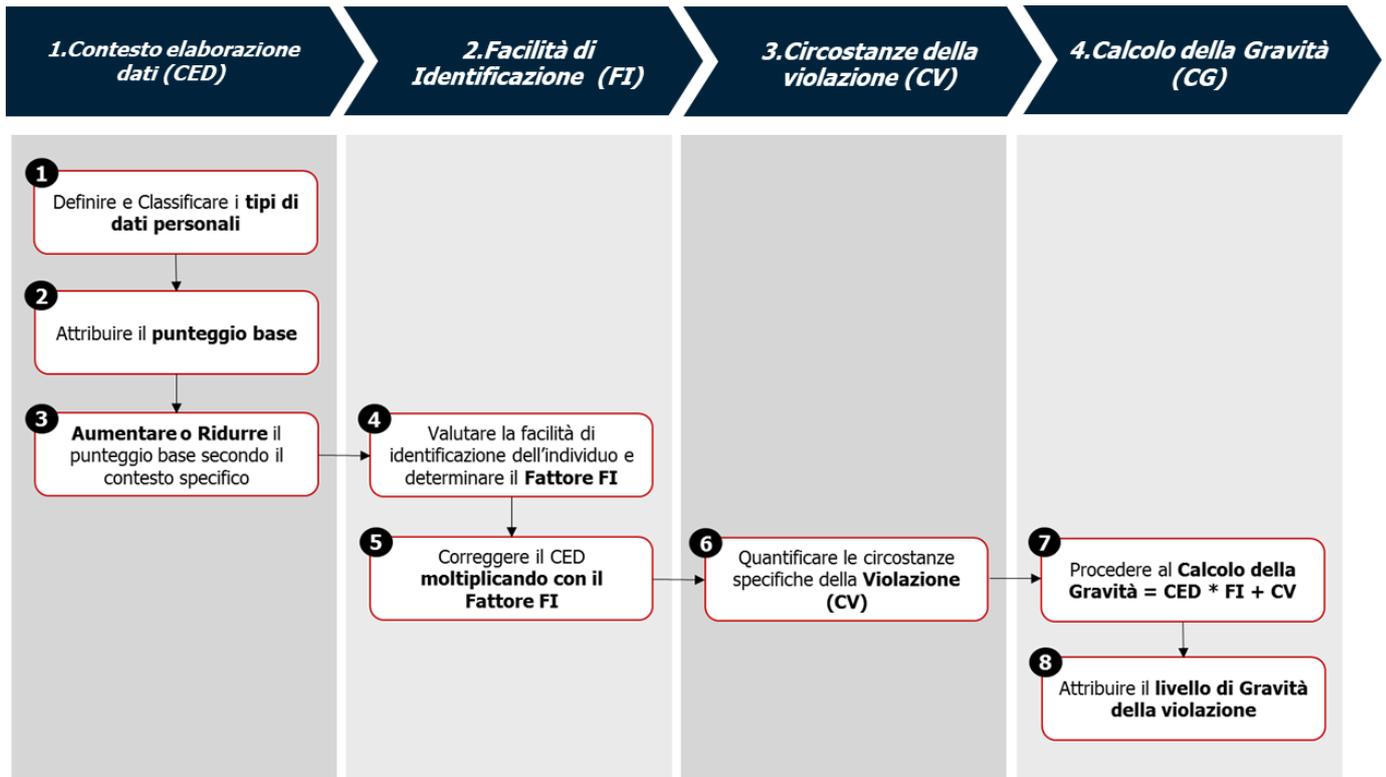
⁹ **Ease of Identification (EI):** Determines how easily the identity of the individuals can be deduced from the data involved in the breach (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

¹⁰ **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 of the breached data, as well as any involved malicious intent (cfr. "Recommendations for a methodology of the assessment of severity of personal data breaches")

malevole) causate o meno in seguito al Data Breach. Il fattore CV, laddove presente, può solo incrementare la gravità di una specifica violazione.

- **Fase 4: Calcolo della gravità:** si giunge al valore finale della gravità della violazione sulla base dei 3 precedenti elementi CED, FI, CV.

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



2.1. Valutazione del contesto dell'elaborazione dei dati (CED)

Il punteggio attribuito al CED è al centro della Metodologia in quanto consente di valutare la criticità dell'insieme di dati violati in un contesto di elaborazione specifico.

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

Attività	Descrizione	Strumenti
1- Definire e Classificare i tipi di dati personali	<p>Definisce e classifica la tipologia di dato trattato che ha subito una violazione sulla base delle seguenti quattro macrocategorie:</p> <ul style="list-style-type: none"> • Dati Ordinari; • Dati Comportamentali; • Dati Patrimoniali; • Dati Particolari. 	Data Breach Report
2- Attribuire il punteggio base	Attribuisce il punteggio base secondo la Tabella 1 - CED	TABELLA 1 – CONTESTO ELABORAZIONE DATI (CED)
3- Aumentare o Ridurre il punteggio base secondo il contesto specifico	<p>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).</p> <p>Il punteggio del CED può variare da 1 a 4.</p>	TABELLA 1 – CONTESTO ELABORAZIONE DATI (CED)

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

Contesto Elaborazione Dati (CED)		Punteggio
Dati Ordinari	Esempi di dati ordinari: nome, cognome, numero di telefono, indirizzo, e-mail, NDG, fotografia, data di nascita, stato di famiglia, titolo di studio, lavoro, inquadramento lavorativo, etc.	
	Punteggio Base: quando la violazione riguarda "Dati Ordinari" e il Titolare non è a conoscenza di alcun fattore aggravante.	1
	Il punteggio CED potrebbe essere aumentato di 1 , ad esempio quando il volume di "Dati Ordinari" e/o le caratteristiche del Titolare sono tali da consentire l'abilitazione di determinati profili o possono essere formulate assunzioni sullo stato sociale/patrimoniale dell'individuo.	2
	Il punteggio CED 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 CED 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, interessi, vita sociale, affidabilità, spostamenti, ubicazione, etc.	
	Punteggio Base: quando la violazione comporta "Dati Comportamentali" e il Titolare non è a conoscenza di fattori aggravanti o di diminuzione.	2
	Il punteggio CED 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 CED può essere umentato di 1 , ad esempio quando il volume di " Dati Comportamentali " e / o le caratteristiche del Titolare 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 CED può essere umentato di 2 , ad esempio se è possibile creare un profilo basato sui dati particolari di una persona.	4
Dati Patrimoniali	Esempio di Dati Patrimoniali: IBAN, numero di conto, saldo conto, transaction history, informazioni su carta di credito/debito (con o senza CVC), dati sui mutui/prestiti, dati Crif, dati CR Banca d'Italia, etc.	
	Punteggio Base: quando la violazione riguarda "Dati Patrimoniali" e il Titolare non è a conoscenza di fattori aggravanti o di diminuzione.	3
	Il punteggio CED 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 CED 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 CED potrebbe essere umentato 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 Sensibili	Esempio di Dati Sensibili: dati sanitari o relativi alla salute, origine razziale/etnica, orientamento politico e religioso, convinzioni religiose o filosofiche, appartenenza a sindacati, orientamenti sessuali, procedimento penale / condanna, dati biometrici, dati genetici.	

	Punteggio Base: quando la violazione riguarda "Dati Sensibili" e il Titolare non è a conoscenza di alcun fattore di diminuzione.	4
	Il punteggio CED potrebbe essere diminuito di 3 , ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni sui Dati Particolari 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 CED potrebbe essere diminuito di 2 , ad esempio quando la natura dei dati può portare a ipotesi generali.	2
	Il punteggio CED potrebbe essere diminuito di 1 , ad esempio quando la natura dei dati può portare a supposizioni su informazioni particolari.	3

TABELLA 1 – CONTESTO ELABORAZIONE DATI (CED)

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 CED da utilizzare corrisponde al valore più elevato di gravità tra tutte le categorie di dati trattati.

2.2. Determinazione del punteggio per la facilità di identificazione (FI)

Il punteggio FI è il fattore di correzione del CED e consente di valutare la facilità di identificazione dell'individuo 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 dell'individuo e determinare il fattore FI	<p>Valuta la facilità di identificazione dell'individuo ed attribuisce un punteggio secondo la Tabella 2 - FI definita dalla Metodologia secondo i seguenti quattro livelli:</p> <ul style="list-style-type: none"> • trascurabile (0,25); • limitato (0,5); • significativo (0,75); • massimo (1). <p>Il fattore di correzione FI può variare da 0,25 a 1.</p> <p>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 a determinate condizioni.</p> <p>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.</p>	TABELLA 2 – FACILITÀ DI IDENTIFICAZIONE (FI)
5- Correggere il CED moltiplicando con il fattore FI	Una volta individuato il fattore di correzione, esso viene moltiplicato per il CED, al fine di determinare il punteggio iniziale della gravità della violazione dei dati.	$CED * FI$

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

Facilità di identificazione (FI)	Punteggio	Livello
La violazione riguarda dati identificativi o dati personali non direttamente identificabili (ad esempio: nome/cognome molto diffuso in un paese)	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)	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 e-mail di questa persona)	0,75	Significativo

<p>La violazione riguarda dati identificativi o dati personali direttamente identificativi (ad esempio: nome completo con l'indicazione della data di nascita e l'indirizzo e-mail di questa persona)</p>	<p>1</p>	<p>Massimo</p>
--	-----------------	----------------

TABELLA 2 – FACILITÀ DI IDENTIFICAZIONE (FI)

2.3. Valutazione delle Circostanze della violazione (CV)

Il punteggio del CV quantifica le **circostanze specifiche della 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
<p>6- Quantificare le circostanze specifiche della violazione (CV)</p>	<p>Attribuisce il punteggio relativo alle circostanze della violazione classificate secondo le seguenti macrocategorie:</p> <ul style="list-style-type: none"> • violazione di riservatezza; • violazione di disponibilità; • violazione di integrità dei dati; • eventuali intenzioni malevole. <p>Le circostanze possono avere solo un'influenza aggiuntiva sulla gravità di una violazione.</p> <p>Il punteggio del CV può incrementare il punteggio precedentemente ottenuto delle gravità di 0,25 o 0,5 a seconda dei casi.</p>	<p>TABELLA 3 – CIRCOSTANZE DELLA VIOLAZIONE (CV)</p>

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

Circostanze della violazione (CV)		Punteggio
<p>Violazione di riservatezza</p>	<p>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.</p>	
	<p>Esempi di dati esposti a rischi di riservatezza senza prove che l'elaborazione illegale si è verificata:</p> <ul style="list-style-type: none"> - Un file cartaceo o un laptop si perde durante il transito; - L'attrezzatura è stata smaltita senza distruzione dei dati personali. 	<p>0</p>
	<p>Esempi di dati trasmessi verso un certo numero di destinatari conosciuti:</p> <ul style="list-style-type: none"> - Una 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. 	<p>0,25</p>

Circostanze della violazione (CV)		Punteggio
	<p>Esempi di dati trasmessi verso un certo numero di destinatari sconosciuti:</p> <ul style="list-style-type: none"> - 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 cliente; - Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni. 	0,5
Violazione di integrità	<p>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.</p>	
	<p>Esempi di dati modificati ma senza alcun uso errato o illegale identificato:</p> <ul style="list-style-type: none"> - 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
	<p>Esempi di dati modificati ed eventualmente usati in modo errato o illegale ma con possibilità di recupero:</p> <ul style="list-style-type: none"> - 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
	<p>Esempi di dati modificati ed eventualmente usati in modo errato o illegale senza possibilità di recupero:</p> <ul style="list-style-type: none"> - Valgono gli esempi precedenti con l'aggravante che i dati originali non possono essere recuperati. 	0,5
Violazione di disponibilità	<p>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).</p>	
	<p>Esempi di dati che possono essere recuperati senza difficoltà:</p> <ul style="list-style-type: none"> - Una copia del file è persa ma sono disponibili altre copie. - Un database è danneggiato ma può essere facilmente ricostruito da altri database. 	0
	<p>Esempi di indisponibilità temporale:</p> <ul style="list-style-type: none"> - 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
	<p>Esempi di indisponibilità totale (i dati non possono essere recuperati dal controllore o dai singoli):</p> <ul style="list-style-type: none"> - 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	<p>Definizione: La violazione è dovuta a un'azione intenzionale malevola, ad esempio al fine di causare problemi al Titolare o danneggiare gli interessati.</p>	

Circostanze della violazione (CV)		Punteggio
	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 3 – CIRCOSTANZE DELLA VIOLAZIONE (CV)

2.4. 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: Gravità = CED * FI + CV
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: <ul style="list-style-type: none"> • 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 4 – LIVELLO DI GRAVITÀ

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

Punteggio	Livello	Descrizione
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.).

$2 \leq Gravità < 3$	Medio	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, etc.).
$3 \leq Gravità < 4$	Alto	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in black-list, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.).
$4 \leq Gravità$	Molto Alto	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie, incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, etc.).

TABELLA 4 – LIVELLO DI GRAVITÀ

