REGIONE LAZIO

ALLEGATO OO([1])

PROCEDURA OPERATIVA PER LA GESTIONE DELLE VIOLAZIONI DEI DATI PERSONALI "PERSONAL DATA BREACH"

-versione 1.0-

[1] Allegato sostituito dall'articolo 40, comma 1, del r.r. 11 aprile 2024, n. 4, pubblicato sul Supplemento n. 1 del BUR Lazio 11 aprile 2024, n. 30

1. Premessa e obiettivi

1.1. Premessa

Il 24 maggio 2016 è entrato in vigore il "Regolamento (UE) 2016/679 (di seguito anche "RGDP"), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abrogava la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). A partire dal 25 maggio 2018 questo regolamento è pienamente applicabile in tutti gli Stati membri. Elemento cardine di questa normativa è il concetto di "responsabilizzazione totale del Titolare" con il quale viene introdotta la responsabilizzazione dei soggetti convolti 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 delle "Violazioni 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 personali[2] trattati dalla Giunta della Regione Lazio nel ruolo di Titolare (di seguito anche "***Personal Data Breach***" o "**Violazione dei dati personali**")[3].

In particolare, secondo quanto previsto dalle Linee Guida 9/2022 sulla gestione e la notifica della violazione di dati personali ("*Personal Data Breach*") gli eventi di possibile violazione dei dati personali possono essere classificati in tre macrocategorie:

- "**Violazione di confidenzialità**" o anche detta "**Violazione di riservatezza**": 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;

[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)

- "**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.

A norma 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.

A norma dell'art. 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 Linee guida EDPB[4] 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 "*Personal Data Breach*".

Il documento contiene le indicazioni operative e le informazioni necessarie per garantire il governo e l'attuazione del processo di gestione dei *Personal Data Breach*. Il presente documento si articola in due differenti sezioni:

A. DEFINIZIONE DELLA PROCEDURA, RUOLI E RESPONABILITÀ 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 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

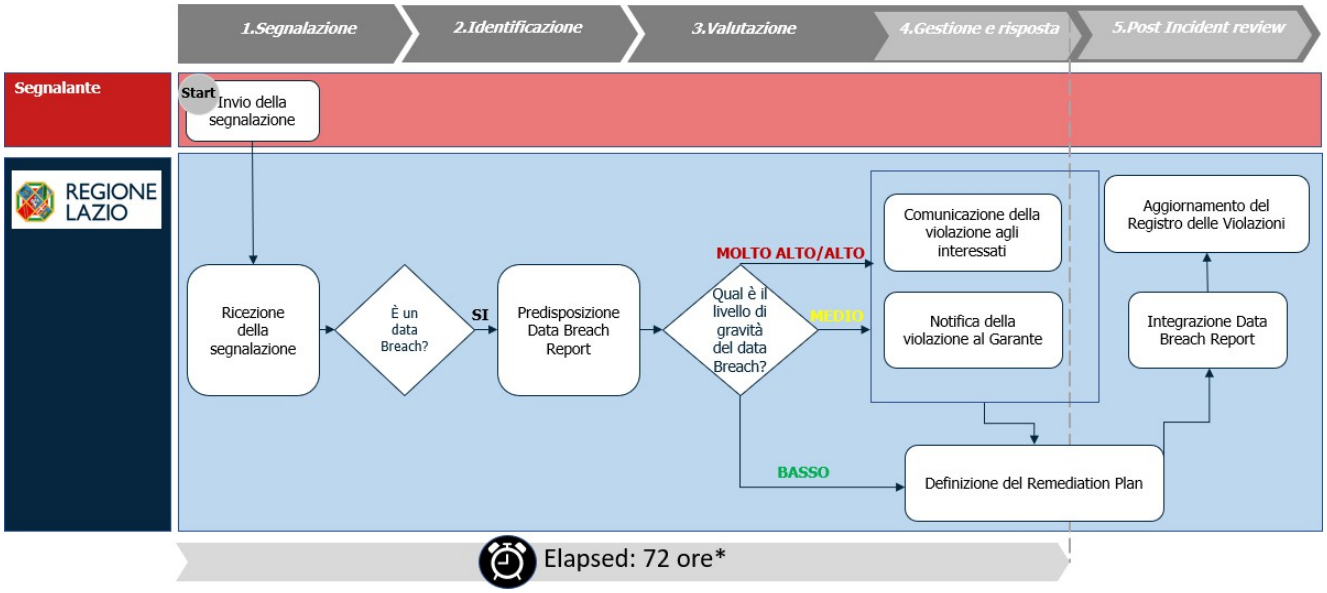
[4] European Data Protection Board (https://edpb.europa.eu/edpb_it)

trattati dalla Giunta Regionale nel ruolo di Titolare, deve essere gestita secondo quanto previsto nelle fasi descritte di seguito:

- **Segnalazione**: fase di segnalazione/ricezione di un potenziale *Personal Data Breach*;
- **Identificazione**: fase in cui la segnalazione ricevuta viene identificata come un *Personal Data Breach* o come altro incidente di sicurezza (falso positivo); se si tratta di ***Personal 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 *Personal 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 nel seguito, in funzione di nuove informazioni rilevate.

- **Gestione e risposta**: in base al livello di gravità del Personal Data Breach, la Giunta regionale dovrà comunicare la violazione agli interessati e/o al Garante; inoltre, in tale fase, viene definito il piano di mitigazione (Remediation Plan) al fine di porre rimedio alla violazione e per attenuarne i possibili effetti negativi;
- **Analisi post incidente (*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.*

Nel caso in cui la Giunta Regionale agisca in qualità di Responsabile per conto di un altro Titolare, è tenuto a informare tempestivamente il titolare in modo che, qualora la violazione costituisca un *Personal Data Breach*, lo stesso possa attivarsi per le fasi del processo di gestione dello stesso.

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**	Il Titolare del trattamento, ovvero la Giunta Regionale, ha la responsabilità ultima della corretta gestione delle violazioni dei dati personali trattati. A seguito della ricezione della segnalazione di una possibile violazione, la Giunta regionale, si avvale dei soggetti designati di cui all'art. 474 ter del regolamento regionale 1/2002, per le fasi di **Identificazione**, **Valutazione**, **Gestione e Risposta** alle violazioni di dati personali e per la fase di ***Analisi post incidente (post incident review).***
TDB	**Team Data Breach**	Il team *Data Breach*, formato da alcuni soggetti designati e dal DPO regionale, si attiva nella fase di identificazione, con la seguente composizione: • DPO regionale; • Soggetto designato competente in materia di protezione dei dati personali (SDP); • Soggetto designato competente in materia di sistemi informativi (ICT); • Soggetto designato competente rispetto al trattamento per il quale si è verificata una violazione (SDC); Il *Team Data Breach* segue tutte le fasi della presente procedura.
DPO	**Data Protection Officer - DPO**	Il DPO supporta i Soggetti designati nell'intero processo di gestione del *Personal Data Breach*.

SDP	**Soggetto designato competente in materia di protezione dei dati personali**	Il soggetto designato competente in materia di protezione dei dati personali, nella fase di **Identificazione**, ha la responsabilità di stabilire se la segnalazione costituisca o meno una violazione. Nelle fasi di **Valutazione**, **Gestione e Risposta**, all'interno del Team Data Breach, supporta il SDC nella valutazione del livello di gravità, nonché nell'elaborazione del piano di mitigazione. Nella fase di **Analisi post incidente (post incident review)**, ha la responsabilità di aggiornare il **Registro delle Violazioni**.
ICT	**Soggetto designato competente in materia di sistemi informativi**	Il soggetto designato competente in materia di sistemi informativi, nelle fasi di **Identificazione** e **Valutazione**, supporta, all'interno del Team Data Breach, il SDC nella valutazione del livello di gravità. Nella fase di **Gestione e risposta,** in collaborazione con il *Team Data breach*, supporta il SDC nella redazione della notifica al Garante e agli interessati. Nella medesima fase collabora alla stesura del piano di mitigazione e, in attuazione dello stesso, adotta le conseguenti azioni ricadenti nell'ambito della gestione dei sistemi informativi. Nella fase di **Analisi post incidente (post incident review)** fornisce, collaborando con il *Team data brach*, informazioni per l'aggiornamento del *Data Breach Report*.
SDC	**Soggetto designato competente rispetto al trattamento per il quale si è verificata una violazione**	Il SDC, nella fase di **Identificazione** con il supporto del *Team Data breach* raccoglie tutte le informazioni disponibili, predisponendo il *Data Breach Report*. Nella fase di **Valutazione** ha la responsabilità di valutare il livello di gravità della violazione. Nella fase di **Gestione e Risposta**, con il supporto del *Team Data Breach*, ha la responsabilità di predisporre e trasmettere la notifica al Garante e agli interessati. Inoltre, al termine di tale fase, il SDC compila e trasmette il *Data Breach Report* al SDP. Nella medesima fase collabora alla stesura del **piano di mitigazione (remediation plan)** e, in attuazione dello stesso, adotta le conseguenti azioni ricadenti nell'ambito organizzativo di propria competenza.

DG	**Direttore Generale**	Il Direttore Generale, a seguito dell'identificazione di un *Personal Data Breach*, viene informato dal SDC in tutte le fasi del processo.
SS	**Soggetto che effettua la segnalazione**	Soggetto che segnala un potenziale *Personal Data Breach.*

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 fase del processo vengono definiti mediante la matrice RACI[5] i ruoli e le responsabilità degli attori coinvolti nella procedura di gestione dei *Personal Data Breach*.

1. Segnalazione

R	A	C	I
SS	SS	SDP	SDP

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

In qualsiasi momento in cui i dipendenti, il personale della Giunta Regionale, il Soggetto Designato anche nell'ambito delle attività di trattamento svolte dalla Giunta Regionale per conto

[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 3 ruoli, per 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.

di un altro titolare e altri possibili soggetti, rilevino un potenziale *Personal Data Breach*, devono darne tempestivamente comunicazione al SDP attraverso l'indirizzo e-mail dedicato databreach@regione.lazio.legalmail.it.

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

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

In questi casi, il soggetto che ha ricevuto la segnalazione di un potenziale *Personal Data Breach*, informa tempestivamente e senza ingiustificato ritardo il Soggetto Designato (es. 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 Personal Data Breach (72 ore solari dalla ricezione della segnalazione) **tutti i soggetti riceventi le segnalazioni sono tenuti a trasmetterle tempestivamente all'indirizzo** databreach@regione.lazio.legalmail.it e **a fornire prontamente il proprio supporto in caso di qualsivoglia dubbio sulla natura della richiesta.**

Si riportano di seguito alcune caratteristiche che possano aiutare a rilevare un evento anomalo che possa rappresentare un potenziale *Personal 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.

Inoltre, a titolo esemplificativo e non esaustivo vengono riportate di seguito alcune tipologie di violazione che potrebbero tradursi in *Personal 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 intervento umano;
- **rivelazione di dati e documenti a soggetti terzi non legittimati**, anche non identificati, conseguenti ad esempio, alla fornitura di 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 errata gestione di supporti informatici.

2. Identificazione

R	A	C	I
SDP	SDP	TDB	DG

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

Dopo aver raccolto tutte le informazioni necessarie e disponibili, il SDP valuta la segnalazione ricevuta e:

- se ritiene che **non** si tratti di un *Personal Data Breach*, conclude il procedimento, dandone comunicazione al SS.
- se ritiene che si tratti di un *Personal Data Breach*, convoca, anche per le vie brevi, *il team data breach* (TDB) che si occuperà di tutte le fasi successive e informa il Direttore Generale.

A seguito dell'identificazione di un *Personal Data Breach*, il SDC con il supporto del *Team Data breach*:

- raccoglie tutte le informazioni disponibili, predisponendo il ***Data Breach Report*** (**Allegato B**), coinvolgendo eventualmente anche altri soggetti designati ed eventuali responsabili del trattamento.

In ogni caso, se la segnalazione riguarda una violazione di natura informatica, il Team Data Breach e, in particolare, il Soggetto designato competente in materia di sistemi informativi (ICT), provvedono ad attivare la specifica procedura adottata dalla Giunta Regionale per la gestione degli incidenti di sicurezza informatica.

3. Valutazione

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 SDC, coadiuvato dal TDB, ha la responsabilità di valutare la *gravità* della violazione dei dati personali 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*" del *Personal Data Breach*, che deve essere comunicato al Direttore Generale (DG), potrà essere:

Livello	Descrizione
Trascurabile	Il rischio non comporta conseguenze significative o danni considerevoli per gli individui interessati.
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, incomprensione, 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.).

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 *Personal Data Breach* definito nella fase precedente, il SDC, coadiuvato dal TDB, ha la responsabilità di procedere con:

- la redazione del modulo per la notifica preliminare, integrativa e definitiva;
- l'invio al Garante della notifica della violazione dei dati personali;
- la comunicazione agli interessati coinvolti nella violazione dei dati.

Il SDC procede secondo le regole sintetizzate in tabella:

Livello di rischio	Ove possibile entro le 72 ore	Senza ingiustificato ritardo
	Notifica al Garante	*Comunicazione all'interessato*
Rischio alto	SI	SI
Rischio medio	SI	NO
Rischio basso	NO	NO
Rischio trascurabile	NO	NO

Comunicazione agli interessati

Qualora il *Personal Data Breach* presenti un rischio alto per i diritti e le libertà delle persone fisiche, il SDC ha la responsabilità di dare comunicazione agli interessati senza ingiustificato ritardo tramite opportuno strumento di comunicazione.
Tuttavia, qualora sussista una delle seguenti condizioni, non è necessaria la comunicazione agli interessati:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia

autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Notifica al Garante per la protezione dei Dati Personali

A norma dell'articolo 33 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 SDC, 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 all'interessato/i, il legislatore europeo ha indicato le informazioni minime che le stesse devono contenere, così come di seguito indicato:

Contenuto notifica diretta all'autorità di controllo[65]	Contenuto comunicazione all'interessato
• **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	• **Descrizione** con linguaggio semplice e chiaro circa la **natura della violazione** dei dati personali
• **Nome e i dati di contatto del DPO** o di altro punto di contatto presso cui ottenere più informazioni	• **Nome e i dati di contatto del DPO** o di altro punto di contatto presso cui ottenere più informazioni
• **Probabili conseguenze della violazione** dei dati personali	• **Probabili conseguenze della violazione** dei dati personali
• 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	• 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

[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.

possibili effetti negativi	

Piano di mitigazione

Il SDC definisce in questa fase un piano per porre rimedio alla violazione e attenuarne i possibili effetti negativi. Inoltre, per la componente del *Personal Data Breach* di natura fisica e organizzativa, assume gli atti di propria competenza.
Inoltre, si avvale del supporto del ICT per la componente del *Personal Data Breach* di natura tecnico-informatica, tenendo in considerazione e/o integrando il piano con le risultanze dell'attività di gestione degli incidenti di sicurezza informatica.
Ciascun soggetto designato ed eventualmente le altre strutture regionali interessate, per la parte di propria competenza, attuano le azioni definite nel remediation plan.

Al termine di questa fase il SDC invia al SDP il **Data Breach Report** aggiornato.

5. Analisi post incidente (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 e di analisi *ex post* della violazione al fine di comprendere le cause del *Personal Data Breach*, apprendere dagli errori e valutare le opportunità di miglioramento.
Il SDP ha la responsabilità di far confluire il *Data Breach Report* 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." (art. 35, paragrafo 5, 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 *Personal Data Breach***	

Allegato A

Registro Data Breach

REGIONE LAZIO

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
☐ Interna a Regione Lazio: *[specificare]* ☐ Esterna a Regione Lazio: *[specificare se fornitore o terzo]*	*Inserire contenuto della segnalazione o link alla stessa*	**NO**	*inserire le motivazioni che hanno portato alla decisione di non considerare la segnalazione come Data Breach*	/		/	/	/
☐ Interna a Regione Lazio: *[specificare]* ☐ Esterna a Regione Lazio: *[specificare se fornitore o terzo]*	*Inserire contenuto della segnalazione o link alla stessa*	**SI**	*inserire le motivazioni che hanno portato alla decisione di considerare la segnalazione come Data Breach*	*Inserire / linkare il Data Breach Report*	Medio	SI	NO	*Inserire/ linkare i documenti a supporto della notifica /comunicazione del Data Breach*
☐ Interna a Regione Lazio: *[specificare]* ☐ Esterna a Regione Lazio: *[specificare se fornitore*	*Inserire contenuto della segnalazione o link alla stessa*	**SI**	*inserire le motivazioni che hanno portato alla decisione di considerare la segnalazione come Data Breach*	*Inserire/ linkare il Data Breach Report*	Molto Alto	SI	SI	*Inserire/ linkare i documenti a supporto della notifica/ comunicazione del Data Breach*

	o terzo]							

Allegato B

Data Breach Report

REGIONE LAZIO

in celeste 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 celeste, da fornire nella notifica al Garante ai sensi dell'art. 33

ID progressivo	**001/ 2022**	
Data Breach riportato da: **Contatti dell' utente:** **Data e ora:** **Struttura di appartenenza:**	*Inserire Nome e Cognome dell'Utente che ha segnalato la violazione o del soggetto terzo (es.fornitore) Inserire l'indirizzo email o il numero di telefono dell'utente che ha segnalato la violazione* *Indicare la data della segnalazione (gg/mese/anno) e l'ora (hh:mm)* *Inserire la struttura di appartenenza dell'utente*	
Data Protection Officer		
Breve descrizione della violazione	*Es. Hacker entra in possesso delle credenziali, perdita o furto di un laptop, modifica dolosa dei dati di un cliente, etc.*	
Dispositivo oggetto di violazione	*Es. Server, dispositivo mobile, documento cartaceo, file o parte di un file, strumento di bakcup, strumento di rete, etc.*	
Tipologia di violazione	☐	Violazione, intenzionale o accidentale, alla riservatezza dei dati perso nali (accesso illegittimo)
	☐	Violazione, intenzionale o accidentale, all' integrità dei dati personali (modifica indesiderata)
	☐	Violazione, intenzionale o accidentale, alla disponibilità dei dati personali (scomparsa/distruzio ne).
	numero di interessati coinvolti	*Indicare, ove possibile, il numero approssimativo dei soggetti impattati dalla violazione*

Interessati	☐	Dipendenti
	☐	Familiari dei dipendenti
	☐	Collaboratori e professionisti esterni
	☐	Fornitori
	☐	Soci
	☐	Visitatori
	☐	Clienti
	☐	Clienti potenziali
	☐	Amministratori/Sindaci
	☐	Familiari Amministratori/sindaci
	☐	Candidati all'assunzione
	☐	Stagisti/interinali
	☐	Minori
	☐	Soggetti terzi
Tipologie di Dati personali	☐	Dati ordinary
	☐	Dati particolari - sensibili
	☐	Dati particolari - giudiziari
	☐	Dati particolari - patrimoniali
	☐	Dati di video sorveglianza
	☐	Dati biometrici
	☐	Dati CRIF
	☐	Dati CR Banca d'Italia
	☐	Dati di geo localizzazione
	☐	Dati comportamentali
	☐	Log di Sistema
	Volume dei dati coinvolti	*Indicare, ove possibile, il numero approssimativo di registrazioni di dati personali oggetto di data breach*
Misure di sicurezza tecnico - organizzative (ex ante)	*Indicare se i dati oggetto di data breach so no 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 SI allegare il documento con il quale si è no tificato il Data Breach al Garante Privacy*
Deve essere comunicato agli interessati?	*Se SI, 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'incidente delle attività intraprese per gestirlo*
Cause della violazione	*Inserire il risultato della root cause analysis:* • *cosa è successo ?* • *come è successo ?* • *perché 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*

Allegato C

REGIONE LAZIO

Metodologia di valutazione

della gravità di un Personal Data Breach

- documento tecnico-metodologico di supporto-

Versione 1.0

1. Premessa, Obiettivi e Definizioni

Il presente documento ha l'obiettivo di declinare la "Metodologia di valutazione delle violazioni dei dati personali" (di seguito anche la *Metodologia*) di cui il titolare del trattamento, Giunta della Regione Lazio, si avvale per valutare la "*gravità*" potenziale di un eventuale violazione dei dati personali (di seguito anche *Personal 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 Personal Data Breach. Nell'ordine:

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

Definizioni

a) "rischio": uno scenario che descrive un evento e le sue conseguenze, stimato in termini di

[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")

gravità e probabilità (WP 248). È la potenzialità che uno scenario, un'azione o un'attività scelta (includendo la scelta di non agire) porti a una perdita o ad un evento indesiderabile. La nozione implica che una scelta influenzi il risultato. Le stesse perdite potenziali possono anche essere chiamate "rischi";

b) "gestione dei rischi": l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi;

c) "rischio potenziale": il rischio che si potrebbe manifestare in assenza di ogni contromisura volta a mitigare il rischio stesso;

d) "rischio residuo": il rischio esistente (effettivo) dopo l'applicazione delle contromisure/delle misure volte ad attenuare il rischio;

e) rischio effettivo: il rischio effettivamente esistente, misurato in un determinato istante temporale;

f) "processo di gestione dei rischi": l'insieme delle regole, delle procedure, delle risorse (umane, tecnologiche e organizzative) e delle attività di controllo volte a identificare, misurare o valutare, monitorare, prevenire o attenuare nonché comunicare ai livelli gerarchici competenti tutti i rischi assunti o assumibili nelle diverse attività, in una logica integrata, nonchè le interrelazioni reciproche anche con l'evoluzione del contesto esterno;

g) "controllo" qualsiasi azione o insieme di azioni, (attività, procedura, blocco, limite) in grado di abbassare il livello del rischio (per raggiungere un livello che sia accettabile).

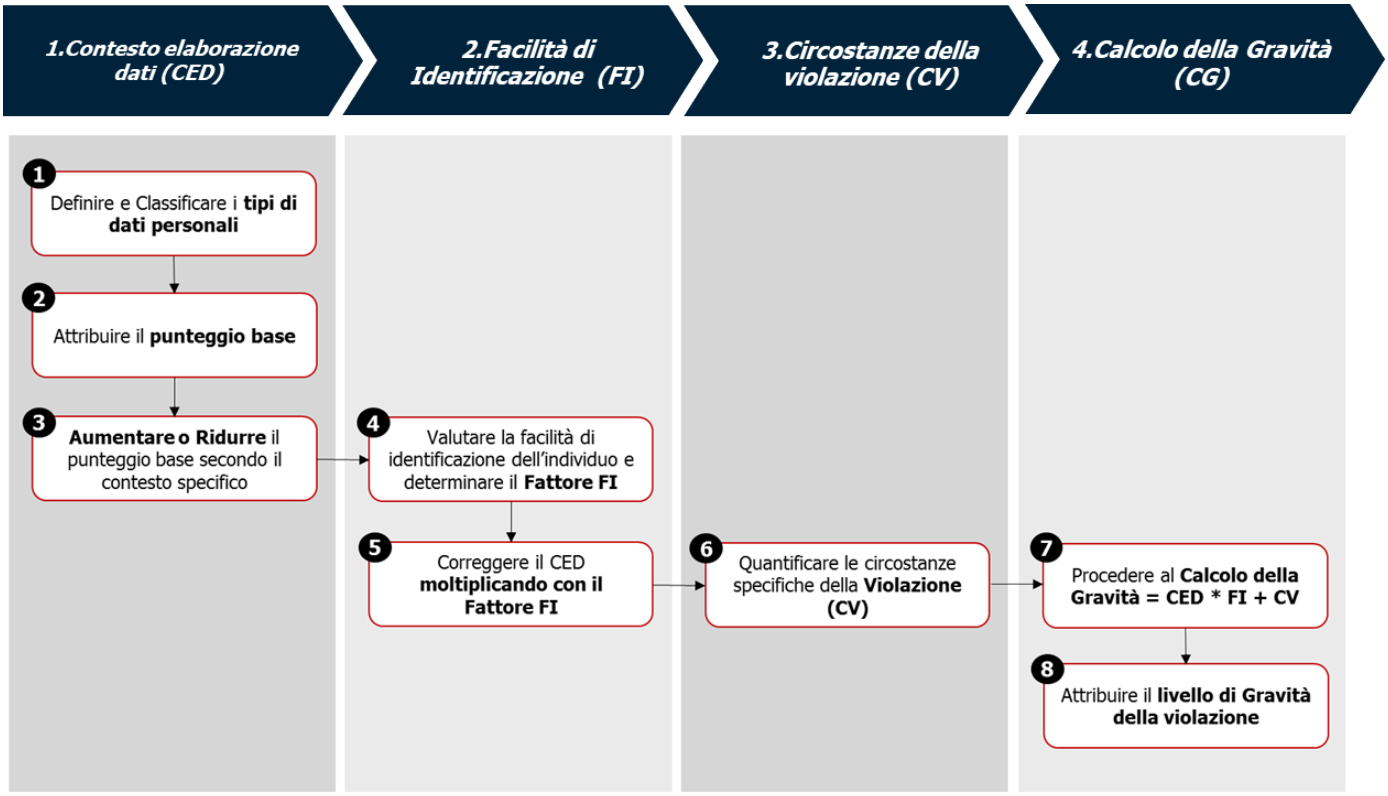
2. Approccio metodologico

La Metodologia adottata dal titolare del trattamento, Giunta della Regione Lazio, volta a consentire di valutare/individuare il livello di rischio esistente (effettivo) in relazione ai dati personali oggetto della violazione dei dati, 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 al rischio residuo/esistente di un punteggio base (tenuto conto delle misure di sicurezza in essere/effettive) 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 malevole) causate o meno in seguito al Personal Data Breach. Il fattore CV, laddove presente, può solo incrementare la gravità di una specifica violazione.

- **<u>Fase 4: Calcolo della gravità:</u>** 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	Definire e classificare la tipologia di dato trattato che ha subito una violazione sulla base delle seguenti quattro macrocategorie: • 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	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 CED può variare da 1 a 4.	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 Studi, 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**

Contesto Elaborazione Dati (CED)	**Punteggio**

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 **aumentato 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 **aumentato 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**

Contesto Elaborazione Dati (CED)		Punteggio
	Il punteggio CED 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 Sensibili	**Esempio di Dati Particolari/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 particolari/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 del 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	Valuta la **facilità di identificazione** dell'individuo ed attribuisce un punteggio secondo la **Tabella 2 - FI** definita dalla Metodologia secondo i seguenti quattro livelli: • trascurabile (0,25); • limitato (0,5); • significativo (0,75); • massimo (1). Il fattore di correzione FI può variare da 0,25 a 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 (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
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)**	**1**	Massimo

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

6- Quantificare le circostanze specifiche della violazione (CV)	Attribuisce il punteggio relativo **alle circostanze della violazione** classificate secondo le seguenti macrocategorie: • 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 CV può incrementare il punteggio precedentemente ottenuto delle gravità di 0,25 o 0,5 a seconda dei casi.	TABELLA 3 – CIRCOSTANZE DELLA VIOLAZIONE (CV)

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

Circostanze della violazione (CV)		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 del cliente; Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni.	**0,5**
	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.	

Violazione di integrità	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**

Circostanze della violazione (CV)		Punteggio
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	**0,5**

	danneggiarli.	

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 in correlazione con le contromisure/misure di sicurezza in essere.
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: • 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 ≤ 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 ≤ 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 ≤ 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