INAPP
ISTITUTO NAZIONALE PER L'ANALISI
DELLE POLITICHE PUBBLICHE

Procedura per la gestione delle violazioni di dati personali (*Data Breach*)

Adottata con Determina del Direttore generale (n. 287 del 14.07.2022)

Indice

Premessa

Il processo di gestione delle violazioni di dati personali (*Data Breach*), descritto nella presente procedura, ha la finalità di definire e regolamentare le attività che devono essere poste in essere, nell'ambito del contesto operativo di INAPP, per gestire ed applicare gli adempimenti prescritti dal Regolamento UE 2016/679 del Parlamento e del Consiglio Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito GDPR).

In particolare, **l'articolo 33 del GDPR**, "***Notifica di una violazione dei dati personali all'autorità di controllo***", impone al Titolare del trattamento di notificare l'avvenuta violazione di dati personali all'Autorità di Controllo Competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è 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. Nel caso in cui la notifica all'autorità di controllo non sia effettuata entro 72 ore, la stessa deve essere corredata dei motivi del ritardo.

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.

L'articolo 34 del GDPR: "***Comunicazione di una violazione dei dati personali all'interessato***", impone al Titolare del trattamento, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, la comunicazione della violazione all'interessato senza ingiustificato ritardo.

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

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.

Si considerano, dunque, eventi di *Data Breach* quelli che comportano in modo accidentale o illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trattati da INAPP.

L'obbligo di notifica all'Autorità si impone se la violazione comporta, ragionevolmente, un rischio per i diritti e le libertà delle persone fisiche; qualora, poi, il rischio fosse elevato, o se richiesto o disposto dall'Autorità, il Titolare sarà tenuto a darne comunicazione all'interessato.

Le sanzioni previste dal GDPR per omessa notifica di *Data Breach* all'Autorità di Controllo o omessa comunicazione agli interessati o entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 GDPR, può comportare l'applicazione in capo all'INAPP di una sanzione amministrativa pecuniaria fino a 10 milioni di euro o fino al 2% del "fatturato" annuo totale dell'esercizio precedente, anche accompagnata da una misura correttiva ai sensi dell'art. 58 par. 2.

I principali rischi sono i seguenti:

- perdita del controllo dei dati degli interessati;
- limitazioni dei diritti/discriminazione;
- furto o usurpazione di identità;
- perdite finanziarie/danno economico o sociale o reputazionale (sia per l'interessato che per il Titolare);
- decifratura non autorizzata della eventuale pseudonimizzazione applicata ai dati;
- perdita di riservatezza dei dati personali particolari ("sensibili").

1 Scopo e campo di applicazione

La procedura di *Data Breach* è disponile sulla Intranet dell'Istituto, in modo da favorirne la consultazione a tutti i dipendenti Inapp, nonché nella sezione "Privacy" del sito Istituzionale per consentirne la consultazione dall'esterno.

Tutto il personale si fa parte diligente per la SEGNALAZIONE di eventuali *Data Breach*. La mail di contatto per le segnalazioni è direzione@inapp.org e ogni segnalazione verrà reindirizzata nella casella di posta elettronica del DPO.

2 Responsabilità e Ruoli

Per la GESTIONE della crisi conseguente ad un evento di *Data Breach* è necessario costituire un ***Data Breach Management Team*** (di seguito, il "*Team*"), chiamato a svolgere una funzione di guida in merito alle modalità operative che tutta l'organizzazione dovrà adottare e con particolare riferimento all'attività di comunicazione.

Solitamente il *Team* è composto dalle seguenti figure:

- DPO (*che, di solito, funge da responsabile del Team*) interfaccia con il Garante;
- Titolare del trattamento (*Rappresentate Legale o soggetto designato dal Rappresentante legale*);
- Privacy Manager della funzione/Unità Organizzativa (U.O.) coinvolta;

nonché un riferimento per ciascuna Unità Organizzativa:

- Responsabile del Servizio Sistemi Informativi Automatizzati (S.I.A.);
- Responsabile del Servizio Statistico;
- Responsabile dell'Ufficio Dirigenziale Gestione e Valorizzazione delle Risorse Umane;
- Responsabile del Servizio per la Comunicazione, che ha il compito di comunicare con eventuali persone che usano i canali di informazioni e reclami, nel caso in cui l'evento coinvolga i dati degli utenti del sito;
- R.P.C.T., nel caso in cui l'evento coinvolga profili legati alla trasparenza amministrativa.

Altre funzioni saranno coinvolte in base all'incidente di sicurezza (Responsabili esterni, ecc.)

3 Modalità Operative

3.1 Gestione evento di *Data Breach*

3.1.1 Segnalazioni

Dall'Interno – nel caso si abbia anche soltanto il sospetto di una violazione di dati (*compiuta dall'interno o dall'esterno*) o si venga a conoscenza di una comunicazione da parte di un interessato/terzo (*anche esterno*), ogni dipendente deve:

- eseguire la segnalazione alla casella di posta elettronica direzione@inapp.org, descrivendo l'evento in modo da attivare la procedura di valutazione dello stesso, evidenziando la massima priorità nella mail; la segnalazione può avvenire con qualsiasi forma documentabile, purché avvenga nel minor tempo possibile;

- segnalare anche soltanto un sospetto, che deve essere comunicato al fine di procedere con la valutazione.

Dall'Esterno (interessato/Garante/stampa)

- il DPO raccoglie le segnalazioni di possibile *Data Breach* provenienti dall'esterno in qualsiasi forma;
- il DPO consulta regolarmente il sito del Garante e gli organi di stampa specializzata per verificare eventuali situazioni di potenziale rischio;
- in entrambi i casi, il DPO comunica via e-mail con la Direzione generale e procede, quindi, a qualsiasi comunicazione utile per accertarsi della presa conoscenza della comunicazione a mezzo mail.

La Direzione generale una volta ricevuta la segnalazione sia dall'interno che dall'esterno dovrà farsi carico, nel più breve tempo possibile, di inviare la stessa alla casella di posta elettronica del Team teamdatabreach@inapp.org e, sulla base della descrizione dell'evento, anche alla casella di posta elettronica dei singoli Privacy manager e/o Responsabili di U.O. che ritiene debbano essere coinvolti per competenza rispetto all'evento, e per conoscenza alla casella di posta elettronica della Presidenza.

Tutte le comunicazioni che provengono da fonte interna o esterna saranno gestite dalla Direzione generale e dovranno essere identificate con l'orario e la fonte di provenienza (riportando, quando possibile, documentazione a supporto).

Ad ogni segnalazione è assegnato un numero univoco (ID) formato dal numero progressivo/anno. Questo numero permetterà di identificare in modo univoco tutta la documentazione che riguarda l'incidente e va sempre riportato.

Appena ricevuta la segnalazione deve essere aggiornato, da parte del DPO, il **Registro degli incidenti** (modulo *M02 – Registro incidenti Data Breach*).

3.1.2 Tempistica

Il calcolo della tempistica (*considerando che il GDPR fornisce 72 ore al Titolare per la eventuale notifica al Garante e la comunicazione all'interessato*) decorre dal ricevimento della segnalazione da parte della Direzione generale.

3.2 Valutazione di pertinenza della segnalazione Raccolta

Tutte le segnalazioni e conseguenti valutazioni vengono registrate e documentate nel modulo **Gestione *Data Breach*** (*M01 - Gestione Data Breach*).

La Direzione generale convoca, entro massimo 24 ore dalla segnalazione, una riunione coinvolgendo tutti i membri del Team disponibili, ed eventuali altri soggetti potenzialmente coinvolti, sulla base delle informazioni raccolte. Qualora qualche membro non fosse disponibile si procede, comunque, con la riunione anche utilizzando canali di comunicazione telematici e virtuali per concertare la gestione del *Data Breach*.

3.2.1 Esecuzione Analisi del Rischio e registrazione risultati

Il *Team* procede alla ***stima della gravità del Data Breach***, utilizzando i criteri descritti al paragrafo 5.2, e alla documentazione della violazione dati personali, completando la compilazione del modulo **Gestione *Data Breach*** (*M01 - Gestione Data Breach*).

Nella compilazione del modulo, si deve tenere conto del significato associato a:

- **Riservatezza**: stima del danno/impatto che la perdita di riservatezza riguardante l'*asset* comporterebbe, per il *business* dell'INAPP, in bilanciamento con la tutela dell'interessato;
- **Integrità**: stima del danno/impatto che la perdita di integrità riguardante l'*asset* comporterebbe, per il compito di interesse pubblico di INAPP, in bilanciamento con la tutela dell'interessato;
- **Disponibilità**: stima del danno/impatto che la perdita di disponibilità riguardante l'*asset* comporterebbe, per i servizi erogati da INAPP, in bilanciamento con la tutela dell'interessato.

Dell'esito della decisione si informa il Titolare del trattamento.

A seguito del confronto tra il DPO e il Titolare del trattamento, il DPO riporta l'esito della casistica, entro la quale ricade la segnalazione, nel **Registro degli incidenti** (Modulo *M02 - Registro incidenti Data Breach).*

3.2.2 Registrazione Evento/Segnalazione:

Segnalazione

Il Team, se del caso, procede alla raccolta di ulteriori informazioni (*es. tramite organi di stampa, richieste di approfondimento*) al fine di chiarire la veridicità, la portata e la reale sussistenza dell'evento segnalato.

Conseguenza dell'evento

Il Team valuta eventuali azioni per contenere gli effetti dell'evento, attivando e documentando le risorse e le azioni necessarie:

- informare il Titolare del trattamento;
- valutare la conseguenza dell'evento [*dati personali colpiti, portata (n. e/o % interessati e n. dati), arco temporale, dati/interessati coinvolti*].

Decisione di non procedere

Qualora fosse accertata, anche dopo eventuali approfondimenti, l'inesistenza di situazioni che mettono a rischio i dati degli interessati, il Team registra la decisione nel modulo **Gestione *Data Breach*** (*M01 - Gestione Data Breach)*, nella sezione dedicata e comunica la medesima al Titolare (*che ha la facoltà, comunque, di richiedere un ulteriore approfondimento*).

In caso di esito positivo (*violazione accertata*), il Team procede con la Analisi del rischio e valuta la necessità di procedere con una eventuale "Azione Correttiva".

Contestualmente, il DPO riporta le risultanze della valutazione di pertinenza, nonché la segnalazione sul **Registro degli Incidenti** (modulo *M02 - Registro incidenti Data Breach*).

3.3 Il Team e la verbalizzazione delle attività

Tutte le attività e le riunioni del Team devono essere documentate ed i verbali sono conservati dalla Direzione generale.

Almeno annualmente, il DPO predispone una relazione sulle attività svolte dal Team nel corso dell'anno. Tale relazione viene trasmessa al Rappresentante Legale e/o al soggetto dallo stesso designato.

La relazione dovrà, per quanto possibile, essere integrata da dati numerici per comprendere l'entità degli eventi ed i relativi tempi di reazione.

3.4 Aspetti decisionali

Il Titolare del trattamento deve essere sempre informato degli sviluppi e delle decisioni del Team in ogni fase dell'indagine ed ha il potere di imporre misure più restrittive a tutela dei diritti degli interessati.

Il Titolare del trattamento può in ogni caso assumere una determinazione diversa rispetto alle decisioni proposte dal Team o dal DPO. In questo caso, il Team verbalizzerà la decisione del Titolare

nel Modulo **Gestione *Data Breach*** *(M01* - Gestione del *Data Breach),* sezione - Decisione di interruzione dell'analisi da parte del Titolare, nonché la posizione del Team ed archivierà la documentazione senza procedere ulteriormente. Le relative comunicazioni dovranno avere data certa (es. tramite PEC al Titolare).

In ogni caso, il DPO è autonomo nel valutare, in caso di contrasto con il Titolare del Trattamento, se comunicare l'evento occorso direttamente al Garante nelle forme e modi che ritiene opportuni.

All'occorrenza, possono essere coinvolti esperti esterni che saranno incaricati della valutazione dell'evento, previa sottoscrizione di un vincolo di riservatezza.

3.4.1 Azioni a seguito delle decisioni

Sulla base della casistica in cui si ricade, debbono essere svolte le seguenti azioni:

- **caso A – Basso rischio calcolato (livello di gravità della violazione dati: basso)**
  - si aggiorna il modulo **Gestione *Data Breach*** *(M01* - Gestione del *Data Breach)* e si chiude l'evento senza eseguire ulteriori comunicazioni;
- **caso B - Rischio che implica l'adozione di trattamento dell'evento ed eventuale Azione Correttiva (livello di gravità della violazione dati: medio)**
  - si aggiorna il modulo **Gestione *Data Breach*** *(M01* - Gestione del *Data Breach)* e si procede con le eventuali "Azioni Correttive", comunicando internamente l'adozione delle azioni di trattamento convenute;
- **caso C - Rischio che implica l'adozione di trattamento dell'evento, l'Azione Correttiva e la notifica obbligatoria all'Autorità di controllo**
  - si aggiorna il modulo **Gestione *Data Breach*** *(M01* - Gestione del *Data Breach)* ed il **Registro degli incidenti** (*M02 - Registro incidenti Data Breach*);
  - si procede con l'adozione di azioni di trattamento dell'evento con le Azioni Correttive;
  - si procede con la notifica all'Autorità di controllo;
- **caso D - Rischio che implica, oltre a quanto previsto dal "caso C" anche la comunicazione obbligatoria agli interessati coinvolti**
  - si prepara un comunicato stampa da predisporre e verificare con il DPO e il Titolare del trattamento.

Le notifiche all'autorità garante e le comunicazioni obbligatorie agli interessati devono avvenire massimo entro 8 ore dall'adozione della decisione.

3.4.2 Gestione dell'evento e Azioni Correttive

Quando è prevista un'attività di mitigazione dell'incidente volta a minimizzare gli impatti per gli interessati e, ove possibile, ripristinare la situazione precedente all'incidente, il Team definisce modalità, responsabilità e tempi.

Il Team valuta la necessità di aggiornare l'analisi dei rischi ed eventualmente la valutazione di impatto del trattamento (DPIA - *Data Protection Impact Assessment*), se prevista per tale trattamento, e la documentazione (es. *procedure di riferimento nomina a responsabile esterno del trattamento*).

Il Team monitora lo stato di avanzamento delle azioni di mitigazione previste e tiene aggiornato il modulo di **Gestione del *Data Breach*** (*M01 - Gestione Data Breach*) ed il **Registro incidenti *Data Breach*** (*M02 - Registro incidenti Data Breach*).

3.4.3 Situazioni anomale o di emergenza

In caso di segnalazioni in situazioni anomale o di emergenza, quali:

- chiusura temporanea delle sedi (*es. periodo di ferie*);
- assenza di figure apicali del Team;
- assenza di possibilità di collegamento telematico;

devono essere considerate le seguenti misure:

- il Team può operare anche in composizione parziale rispetto a quella prevista (non inferiore a tre membri);
- le riunioni del Team possono essere tenute in luoghi diversi dalla sede e tramite altre tipologie di strumenti elettronici (*conference call, video call*).

4 Comunicazioni al Garante e agli interessati

A seguito di un evento di *Data Breach*, deve essere effettuata la comunicazione all'Autorità Garante e, nei casi previsti (*es. caso D*), anche agli interessati.

La comunicazione è coordinata dal Team. Le evidenze di tutte le comunicazioni devono essere conservate.

4.1 Comunicazioni al Garante

La comunicazione al Garante deve essere eseguita esclusivamente tramite procedura on line reperibile al seguente link: https://servizi.gpdp.it/databreach/s/scelta-auth ed è necessario allegare l'analisi del rischio estrapolata dal modulo **Gestione del *Data Breach*** (*M01* - Gestione del *Data Breach)* e l'eventuale comunicazione inviata agli interessati.

4.2 Comunicazione agli interessati

La comunicazione agli interessati può avvenire con modalità diverse, tra le quali:

- comunicazione diretta agli interessati;
- comunicato stampa;
- comunicazione tramite sito *WEB*/*social media;*
- altre forme.

La comunicazione deve essere congruente con quanto di seguito indicato.

4.2.1 Linee Guida per la redazione delle comunicazioni verso gli interessati

Aspetti generali:

- definire il tono della comunicazione, che può essere più o meno informale (*dichiarazione ufficiale*, *comunicato*);
- fornire un titolo "giornalistico" che, per quanto possibile, rassicuri gli interessati o perlomeno riduca il livello di allarme, utilizzando parole chiave facilmente rintracciabili sui motori di ricerca qualora venissero ricercate informazioni con tali modalità; le comunicazioni potrebbero non riguardare soltanto l'evento di *Data Breach*, ma anche le informazioni sull'andamento dello stesso nel tempo;
- assicurare forme di comunicazione oneste, concrete e trasparenti;
- fare riferimento al Team, al suo ruolo ed al suo impegno;
- mettere in evidenza la storia e l'impegno dell'INAPP nell'assicurare l'attenzione al tema, gli investimenti realizzati a livello di tutela della privacy, le misure applicate;
- descrivere l'evento in modo facilmente comprensibile, il livello di impatto che ha avuto sui dati (o quale impatto presumibile può avere – informazioni perse, violate, comunicate a terzi

non autorizzati, diffuse, ecc.), come lo si sta affrontando/è stato affrontato, e specificare cosa l'Istituto sta facendo concretamente per proteggere i dati degli interessati;

- indicare quali misure tecniche sono state/saranno implementate per affrontare la violazione dei dati;
- indicare come e quando è stata coinvolta l'Autorità Garante della Protezione dei dati personali;
- inserire un contatto diretto per contattare l'Istituto;
- considerare di attivare un numero dedicato per rispondere agli interessati;
- prevedere un *link* alla pagina del sito istituzionale dove sono reperibili ulteriori informazioni sul *Data Breach* ed anche lo stato dell'andamento dello stesso nel tempo.

5 Altri riferimenti

5.1 Moduli

M01 - Modulo Gestione Data Breach

M02 – Modulo Registro incidenti Data Breach

M03 – Comunicazione Data Breach all'Autorità Garante (modulo online sito istituzionale)

5.2 Stima della gravità del *Data Breach*

I **principali criteri** che si devono prendere in considerazione durante la valutazione della gravità di una violazione dei dati personali (*Personal Data Breach*) sono:

a. **Contesto del trattamento dei dati:** tipologia di dati violati insieme a una serie di fattori collegati al contesto generale della loro elaborazione. Il contesto è un elemento centrale della metodologia e valuta la criticità di un determinato insieme di dati in un ambito di elaborazione specifico.

b. **Facilità di identificazione:** facilità con cui l'identità degli individui può essere dedotta dai dati coinvolti nella violazione. Tale parametro è un fattore di correzione del Contesto di elaborazione dati; infatti, la criticità complessiva di un *Personal Data Breach* può essere ridotta in base al valore di facilità di identificazione degli interessati. In altre parole, minore è la facilità di identificazione dell'individuo, minore è il punteggio complessivo da attribuire alla violazione del dato. Pertanto, la combinazione di Facilità di identificazione e Contesto

dell'elaborazione dati (moltiplicazione) fornisce il punteggio iniziale della gravità della violazione dei dati.

c. **Circostanze di violazione:** criterio che tiene conto delle specifiche circostanze della violazione, inclusa principalmente la perdita di sicurezza dei dati violati, nonché qualsiasi intento malevolo coinvolto. Questo parametro quantifica le circostanze specifiche della violazione che possono essere presenti o meno in una particolare situazione.

Sulla base dei criteri di cui sopra, il punteggio finale della valutazione della gravità della violazione di dati Personali (*Personal Data Breach*) è estratto utilizzando la seguente formula:

Gravità = (Contesto di trattamento dati* Facilità identificazione) + Circostanze violazione

Il risultato finale della gravità corrisponde a uno dei seguenti quattro livelli: basso, medio, alto e critico (cfr. Tabella A.4).

Punteggio Contesto

Classificare i dati in almeno una delle quattro categorie: Personali/Anagrafici/identificativi, Rischiosi, Particolari / Relativi a condanne penali e reati.

Tabella A.1 - Punteggio Parametro "Contesto di trattamento dati"

Tipologia Dato	Descrizione Dato	Punteggio
Personale/ Anagrafico/ Identificativo	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	1
Rischioso	Qualsiasi informazione consistente nell'utilizzo di dati personali atti a valutare determinati aspetti personali relativi a una persona fisica. Ad esempio, per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica	2

Tipologia Dato	Descrizione Dato	Punteggio
Particolari e/o relativi a reati o condanne penali	In questa categoria rientrano una o più tipologie di seguenti informazioni: «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; «**dati relativi a condanne penali e reati**»: dati personali idonei a rilevare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 Novembre 2002, n. 313, in materia di casellario giudiziario, anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	3

Punteggio Facilità di identificazione

La facilità d'identificazione valuta quanto sarà facile abbinare univocamente i dati violati all'identità di una determinata persona.

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

Tabella A.2 - Punteggio Parametro: Facilità di identificazione

Livello	Descrizione	Punteggio
Trascurabile	Quando il dato oggetto di *Data Breach*, di per sé, non rileva l'identità dell'individuo e non è possibile associarvi ulteriori informazioni (es. dati cifrati).	0,25
Significativo	Quando il dato oggetto di *Data Breach*, di per sé, non rileva l'identità dell'individuo, ma ne rivela ulteriori informazioni identificative (ad es. la data di nascita) ed è collegato ad altri dati (ad esempio indirizzo postale).	0,75
Massimo	Quando i dati intercettati rivelano l'identità dell'individuo.	1

Punteggio Circostanze della violazione

Gli elementi considerati riguardanti le circostanze della violazione sono la perdita di sicurezza (riservatezza, integrità, disponibilità) e intenzione malevole:

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.

Perdita di integrità: si verifica quando le informazioni originali vengono alterate e la sostituzione dei dati può essere pregiudizievole per l'individuo. La situazione più grave si verifica quando esistono gravi possibilità che i dati modificati siano stati utilizzati in un modo tale da danneggiare l'individuo.

Perdita di disponibilità: la perdita di disponibilità si verifica quando non è possibile accedere ai dati originali 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).

Intento malevolo: questo elemento esamina se la violazione è dovuta a un errore, umano o tecnico, o è stata causata da un'azione intenzionale. Violazioni fraudolente includono casi di furto e hacking che mirano a danneggiare le persone (ad es. esponendo i loro dati personali a terzi non autorizzati). In altri casi, l'intento malevolo potrebbe includere il trasferimento di dati personali a terzi a scopo di lucro (ad esempio la vendita di elenchi di dati personali). In alcuni casi, l'intento malevolo potrebbe anche essere desunto da azioni volte a danneggiare il responsabile del trattamento dei dati (ad esempio attraverso il furto e l'esposizione dei dati personali a soggetti non autorizzati).

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

La tabella sottostante fornisce i diversi punteggi per ciascuna caratteristica della sicurezza dei dati e per i diversi tipi di circostanze.

Tabella A.3 - Punteggio Circostanze della violazione (CB)

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

Definizione del livello di gravità

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

Gravità (G) = (Contesto di trattamento dati * Facilità identificazione) + Circostanze violazione

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

Tabella A.4 – Definizione Livello di Gravità (G)

Livello di gravità del Data Breach			OBBLIGO
$G \leq 1$	Low Basso)	Gli individui non saranno impattati o potrebbero solo incontrare alcuni inconvenienti, che supereranno senza alcun	Registrazione interna

		problema (es. tempo trascorso a reinserire informazioni, fastidi).	
$1 < G \leq 2$	Medium (Medio)	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (es. costi aggiuntivi, rifiuto di accesso ai servizi).	Registrazione interna
$2 < G < 3$	High Alto)	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, etc.).	Notifica al Garante Privacy
$3 \leq G$	Critical (Critica)	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa etc.)	▪ Notifica al Garante Privacy ▪ Comunicazione all'Interessato*

* In conformità all'art. 34 del GDPR, la comunicazione all'Interessato **NON** andrà comunque effettuata se è soddisfatta una delle seguenti condizioni:

- il Titolare del trattamento ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione; in particolare, quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura (es. l'inintelligibilità sotto forma di crittografia forte e senza compromissione chiave, può ridurre sostanzialmente l'impatto sugli individui, poiché riduce notevolmente la possibilità che parti non autorizzate accedano ai dati);
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Istruzioni per il calcolo

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

$$Contesto\ del\ trattamento\ (C) = \{1; 2; 3\}$$
$$Facilità\ identificazione\ (ID) = \{0.25; 0.75; 1\}$$
$$Circostanze\ del\ data\ breach\ (CDB) = \{0.25; 0.50; 0.75\}$$

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

Tabella A.5 – $\boldsymbol{DPC \cdot EI}$

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

Tabella A.6 – Definizione $G = (C * ID) + CDB$

Per procedere al calcolo, dunque, attribuire un punteggio al Contesto del trattamento e alla Facilità di identificazione degli interessati, e calcolare il prodotto; aggiungere dunque il punteggio della tabella A.3 con le tipologie di violazione (in caso di concomitanza di più fattori, scegliere il punteggio più alto) e aggiungere tale valore al risultato del prodotto calcolato in precedenza.

ESEMPIO:

Smarrimento/furto smartphone (con accesso al display bloccato e protetto); lo smartphone è configurato con il client per la posta dell'Istituto (accesso all'APP con ulteriore password).

Nel Modulo **Gestione del *Data Breach*** (*M01* - Gestione del *Data Breach)*, nelle indicazioni di contesto, si inserisce sicuramente una X per i dati personali/identificativi/anagrafici; se il dispositivo è in uso a personale che può avere dati personali del contesto "rischiosi" o "particolari", si attribuisce il punteggio più alto; mettiamoci nel peggiore dei casi, supponendo che siano presenti messaggi di posta con dati particolari, e in questo caso il punteggio è 3.

Si inserisce poi la Facilità di identificazione, che in questo caso, essendo lo Smartphone protetto con sistema di crittografia (pin e altro), è trascurabile: 0,25 di punteggio.

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

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

INAPP
ISTITUTO NAZIONALE PER L'ANALISI
DELLE POLITICHE PUBBLICHE

M01- Modulo gestione Data Breach

Indice

STEP 1 – Registrazione Evento/Segnalazione

Segnalazione

ID N°/anno	
Data	
Segnalante	
Modalità di comunicazione	
Descrizione Segnalazione	
Eventuali Allegati (es. mail)	

Conseguenze dell'evento

N° interessati e/o n° dati coinvolti	
Contesto del trattamento dei dati personali	
Data e/o Arco temporale della violazione	
Portata dell'evento	
Formato dati	Elettronico ☐ Cartaceo ☐
Tipo di Violazione	*Es. Lettura, Copia, Alterazione, Cancellazione, Furto, …*
Dati protetti da crittografia o pseudonimizzati	
Esistenza copia di backup dei dati	
Eventuali azioni per contenere effetti dell'evento	

Natura dei Dati Violati

		Eventuali commenti
Dati anagrafici/codice fiscale	☐ SI ☐ NO	
Dati di accesso e di identificazione (username, password, customer ID, altro)	☐ SI ☐ NO	
Numeri carte di credito	☐ SI ☐ NO	
Brevetti, strategie di marketing, segreti professionali	☐ SI ☐ NO	
Reddito, fatturato	☐ SI ☐ NO	
Dati relativi a minori	☐ SI ☐ NO	
Dati sulle abitudini/preferenze dell'interessato	☐ SI ☐ NO	
Dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale	☐ SI ☐ NO	
Dati personali idonei a rivelare lo stato di salute e la vita sessuale	☐ SI ☐ NO	
Dati giudiziari	☐ SI ☐ NO	
Dati sulla localizzazione dell'interessato	☐ SI ☐ NO	
Immagini su supporto informatico di documenti analogici	☐ SI ☐ NO	
altro _____	☐ SI ☐ NO	

Indicatori di contesto per valutazione Livello di Gravità

Tipologia Dato	Descrizione Dato	Selezione (X)
Personale/ Anagrafico/ Identificativo	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale	
Rischioso	Qualsiasi informazione consistente nell'utilizzo di dati personali atti a valutare determinati aspetti personali relativi a una persona fisica. Ad esempio, per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica	
Particolari e/o relativi a reati o condanne penali	In questa categoria rientrano una o più tipologie di seguenti informazioni: «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici; «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute; «**dati relativi a condanne penali e reati**»: dati personali idonei a rilevare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 Novembre 2002, n. 313, in materia di casellario giudiziario, anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del c.p.p.	

Indicatori di facilità di identificazione degli interessati per valutazione Livello di Gravità

Livello	Descrizione	Selezione (X)
Trascurabile	Quando il dato oggetto di Data Breach, di per se, non rileva l'identità dell'individuo e non è possibile associarvi ulteriori informazioni (es. dati cifrati).	
Significativo	Quando il dato oggetto di Data Breach, di per se, non rileva l'identità dell'individuo, ma ne rivela ulteriori informazioni identificative (ad es. la data di nascita) ed è collegato ad altri dati (ad esempio indirizzo postale).	
Massimo	Quando i dati intercettati rivelano l'identità dell'individuo.	

Indicatori di circostanze della violazione per valutazione Livello di Gravità

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

STEP 2 – Esecuzione Analisi del Rischio e registrazione risultati

Risultati Valutazione della gravità del Data Breach e del rischio per gli interessati

violazione di riservatezza	☐ SI	☐ NO	
violazione di accessibilità	☐ SI	☐ NO	
violazione di integrità	☐ SI	☐ NO	
Valore del Livello di rischio calcolato	Riportare il valore calcolato con le modalità della procedura.		
Livello di gravità e tipologia di Rischio individuato – Azioni a seguito delle decisioni	Sulla base delle indicazioni fornite al par. 3.4.3 della procedura (Procedura Data Breach) Indicare il livello di classificazione individuata (es, Caso A, caso B, Caso C o caso D)		
Trattamento del Rischio	Indicare le modalità di trattamento del rischio, es. accettazione, riduzione, trasferimento del rischio		

Azione Correttiva

Data	
Azione Correttiva	
Responsabile della Azione Correttiva	
Tempi di effettuazione	
Comunicazione a Titolare del Trattamento	
Valutazione di efficacia ed azioni in caso di esito negativo	
Eventuale aggiornamento documentazione	

STEP 3 – Registrazione Notifiche/Comunicazioni/Decisioni

Notifica all'autorità di controllo dello stato in cui è avvenuta la violazione

Modalità di invio	
Data e ora	

Comunicazione agli interessati

Comunicazione obbligatoria	☐ SI ☐ NO	*Motivazione:*
Mezzo di comunicazione		
Data e ora		

Decisione a non procedere da parte del Team

Data	
Motivazione	
Membri presenti del Team	
Comunicazione a Titolare del Trattamento	
Eventuale azione correttiva? (vai a tabella Azione Correttiva)	

Decisione a non procedere da parte del Titolare

Data	
Motivazione	
Membri presenti del Team	
Comunicazione in data certa	
Allegato	

INAPP
ISTITUTO NAZIONALE PER L'ANALISI DELLE POLITICHE PUBBLICHE

M02 – Registro incidenti Data Breach

				NOTIFICA ALL'AUTORITA' GARANTE			
Data e Ora Segnalazione	ID segnalazione (formato dal numero progressivo/anno)	Valutazione della segnalazione	Tipologia Caso (A B C D)	Data e ora comunicazione al Garante (Casi C e D)	Data e ora comunicazione agli interessati (Caso D)	Data completamento dell'azione correttiva	Altre informazioni