GRUPPO CASSA CENTRALE
CREDITO COOPERATIVO ITALIANO

METODOLOGIA DI GRUPPO per la valutazione del Data Breach

Fonte Normativa: Metodologia

Approvato dal Consiglio di Amministrazione

Data della Delibera: 20 gennaio 2021

Owner		Autore
DPO		Servizio Data Protection
Destinatari		
Capogruppo e Società del Gruppo		
N° Versione	Data di approvazione in CdA di Capogruppo	Note
1	20 gennaio 2021	Prima versione

3. Sommario

1. Glossario 4

2. Premessa 5

2.1. Obiettivi del documento 5

2.2. Adozione, aggiornamento e diffusione del documento 6

2.3. Contesto Normativo di riferimento 6

3. Criteri di valutazione del Data Breach: Riservatezza 6

3.1 PROBABILITÀ E GRAVITÀ DELLE VIOLAZIONI DEI DATI 7

3.2 CONTESTO DEL TRATTAMENTO (DPC): Natura e carattere sensibile dei dati personali 8

3.3 CONTESTO DEL DATA BREACH (DBC) 8

3.4 ULTERIORI FATTORI LEGATI AL CONTESTO DELLA VIOLAZIONE 10

3.5 FACILITÀ DI IDENTIFICAZIONE (EI) 11

3.6 CARATTERISTICHE DELLA VIOLAZIONE (CV) 11

3.7 CALCOLO DEL RISCHIO 13

4. Criteri di valutazione nei casi di violazione della disponibilità ed integrità dei dati personali 14

4.1 PREMESSA 14

4.2 CRITERI DI VALUTAZIONE INDISPONIBILITÀ E VIOLAZIONE INTEGRITÀ 16

5. Notifiche al Garante e agli interessati 17

5.1 NOTIFICA ALLE AUTORITÀ COMPETENTI 17

5.2 NOTIFICA AI SOGGETTI INTERESSATI 18

1. Glossario

Banca/Banche affiliata/e: singolarmente ovvero collettivamente le Banche di Credito Cooperativo, le Casse Rurali e/o le Casse Raiffeisen aderenti al Gruppo Bancario Cooperativo, in quanto soggette all'attività di direzione e coordinamento da parte della Capogruppo in virtù della sottoscrizione del Contratto di Coesione.

Capogruppo: Cassa Centrale Banca – Credito Cooperativo Italiano S.p.A. in qualità di Capogruppo del Gruppo Bancario Cooperativo.

Consiglio di Amministrazione (CdA): Organo con funzione di supervisione strategica.

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.

Data Breach: la 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.

Data Protection Officer o DPO: il soggetto designato dal Titolare o dal Responsabile del trattamento per assolvere funzioni di supporto e controllo, consultive, formative e informative relativamente all'applicazione del GDPR.

Garante: l'Autorità garante italiana per la protezione dei Dati personali.

GDPR: indica il Regolamento UE 679/2016 in materia di protezione dei Dati personali.

Gruppo: Gruppo Cassa Centrale – Credito Cooperativo Italiano;

Incidente: qualsiasi evento che implica la violazione o l'imminente minaccia di violazione delle norme e delle prassi aziendali in materia di sicurezza delle informazioni (ad es. frodi informatiche, attacchi attraverso internet e malfunzionamenti e disservizi). La gestione degli Incidenti è disciplinata dalla normativa interna in materia di gestione degli incidenti ICT.

Policy: la Policy in materia di protezione dei Dati personali.

Regolamento di Gruppo per la gestione degli incidenti ICT: la normativa adottata ai sensi della parte I, titolo IV, capitolo 4, sezione IV della Circolare Banca d'Italia n. 285 del 17 dicembre 2013 al fine di disciplinare, tra il resto, il processo di gestione degli Incidenti.

"Registro delle violazioni" o **"Registro**": il registro adottato dal Titolare al fine di documentare le violazioni di Dati personali e le motivazioni sottese alle decisioni assunte di conseguenza.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati personali per conto del titolare del trattamento.

Società del Gruppo/Società: le Banche affiliate, le società da queste controllate, direttamente o indirettamente, e le altre Banche, Società prodotto, Società finanziarie, Società servizi e strumentali controllate, direttamente e/o indirettamente, dalla Capogruppo.

Soggetto Designato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che – singolarmente o insieme ad altri – determina le finalità e i mezzi del trattamento di Dati personali.

2. Premessa

2.1. OBIETTIVI DEL DOCUMENTO

L'obiettivo del presente Documento è fornire le necessarie istruzioni metodologiche per determinare, tramite lo strumento messo a disposizione unitamente alla presente Metodologia[1], se un evento, identificabile come Data Breach, può rappresentare un rischio per i diritti e le libertà degli interessati. Ciò anche al fine di adempiere correttamente ai conseguenti obblighi in tema di notifica alle autorità competenti e agli interessati coinvolti dalla violazione. Lo strumento, in secondo luogo, permette di rendere maggiormente efficiente il processo decisionale connesso all'individuazione delle più corrette contromisure, atte a limitare i danni derivanti dalla violazione dei dati.

Esso non è inteso come strumento esaustivo e generale, ma i suoi esiti vanno piuttosto assunti quali indicazioni operative. Per i casi più complessi, quindi, la valutazione non potrà essere affidata

[1] "Tool-Data-Breach" elaborato su file Excel.

esclusivamente agli algoritmi presenti all'interno dello strumento di calcolo fornito, in quanto la stima:

- delle probabilità delle conseguenze del data breach;
- e la gravità delle stesse;

dovranno tenere conto delle particolarità e specificità di ogni caso concreto.

2.2. ADOZIONE, AGGIORNAMENTO E DIFFUSIONE DEL DOCUMENTO

La presente metodologia e i suoi relativi aggiornamenti sono approvati dal Consiglio di Amministrazione della Capogruppo.

Il DPO verifica nel continuo e comunque con cadenza annuale la complessiva idoneità del Documento ad ottemperare a quanto previsto dalla vigente Normativa Privacy, tenendo conto, tra l'altro, delle modifiche eventualmente intervenute, degli assetti organizzativi del Titolare del Trattamento, nonché dell'efficacia dimostrata dalle procedure nella prassi applicativa.

La Metodologia si applica a tutte le Società del Gruppo e le Banche affiliate ed è trasmessa alle stesse per il recepimento e la relativa attuazione.

2.3. CONTESTO NORMATIVO DI RIFERIMENTO

- Regolamento europeo 2016/679 "General Data Protection Regulation (GDPR)";
- Recommendations for a methodology of the Assessment of Severity of personal data Breaches realizzato da Enisa (European Union Agency for Network and Information Security);
- Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 nonché WP 250.

3. Criteri di valutazione del Data Breach: Riservatezza

Nel seguito sono esplicitati i criteri utilizzati per valutare il Data Breach nel caso in cui l'evento (trattamento non autorizzato o illecito) derivi dalla divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.

3.1 PROBABILITÀ E GRAVITÀ DELLE VIOLAZIONI DEI DATI

L'analisi del rischio deve avere come esito la determinazione dei seguenti due parametri (considerando 76 GDPR):

1. La probabilità delle conseguenze del data breach per l'interessato;
2. La gravità delle stesse.

La **gravità di una violazione** è considerata, come la "*stima dell'entità del potenziale impatto che una violazione dei dati potrebbe avere sulle persone interessate*".

Il considerando 75 del GDPR specifica che i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

La stima della Gravità della violazione è calcolata considerando diversi fattori come di seguito indicati.

3.2 CONTESTO DEL TRATTAMENTO (DPC): NATURA E CARATTERE SENSIBILE DEI DATI PERSONALI

Per stabilire se una violazione dei dati trattati può comportare un rischio per i diritti e le libertà dell'interessato è necessario analizzare qual è la tipologia dei dati violati e le caratteristiche delle informazioni oggetto della violazione.

La variabile, contesto del trattamento (DPC), consente un primo elemento di valutazione per determinare la probabilità che l'evento abbia conseguenze per l'interessato.

Le voci delle tipologie disponibili per l'attribuzione del **DPC sono le seguenti:**

- Dati comuni identificativi: in questo caso nella violazione sono coinvolti solo dati "semplici" quali il nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro;
- Dati comportamentali: i dati oggetto di violazione potrebbero fornire alcune informazioni circa le abitudini e comportamenti dell'individuo (ad esempio tramite l'esame della cronologia degli acquisiti laddove questa fosse stata divulgata);
- Dati Finanziari / Patrimoniali: qualunque tipo di dato finanziario (Dati economico-patrimoniale o di pagamento, estratto conto corrente, patrimonio e situazione finanziaria, dettagli carta di credito);
- Dati Particolari, Dati Giudiziari (relativi a condanne penali o reati); Dati di Minori: (art. 9 GDPR): dati relativi alla salute (es. malattie, appartenenza a categorie protette), dati che rivelino l'origine razziale o etnica, convinzioni religiose e filosofiche, opinioni politiche, appartenenza sindacale, vita sessuale o orientamento sessuale.

Per ciascuna tipologia di voce è abbinato un valore, da zero a quattro (0-4) legato ai potenziali effetti della violazione sulle libertà e diritti degli interessati. Più i dati rivelati forniscono informazioni atte a dare un quadro complessivo dell'interessato, ad esempio in merito al suo stato finanziario, di salute, ecc... maggiore sarà la gravità e la probabilità che l'evento dia luogo a un rischio per i diritti e le libertà dell'interessato. Tale informazione è comunque un primo elemento che va contestualizzato all'interno del panorama generale nel quale si è verificato l'evento.Il compilatore deve quindi indicare quali tra le tipologie dei dati proposti nel tool messo a disposizione, sono state interessate dall'evento.

3.3 CONTESTO DEL DATA BREACH (DBC)

Il **contesto della violazione (DBC)** descrive eventuali fattori, derivanti dalle circostanze specifiche della violazione, che possono **attenuare** o **aggravare** il rischio per i diritti e le libertà dell'interessato.

Tra i fattori che possono **aggravare** la portata del data breach vi sono:

- **Il volume dei dati violati (per la stessa persona):** questo fattore può aumentare il punteggio DPC di base, a causa dell'incremento della quantità delle informazioni violate (cioè fungendo da fattore aggravante). Il volume dovrebbe essere considerato sia in termini di tempo (ad es. Stesso tipo di dati per un certo periodo di tempo) che di contenuto (integrando dati dello stesso tipo). Ad esempio, in caso di violazione dei dati finanziari, il punteggio DPC sarebbe più alto (per la stessa persona) se i dati coprono un periodo di un anno rispetto o se fossero limitati a una settimana (tempo). Oppure se ad essere rivelata fosse la completa situazione patrimoniale del cliente rispetto ad una semplice operazione.
- **Caratteristiche del database di provenienza.** Ad esempio, la semplice lista di nomi e cognomi se raccolta dal database di gestione degli accertamenti della magistratura o della procedura whistleblowing, sarebbe più a rischio rispetto alla semplice lista dei dipendenti della banca.
- **Caratteristiche speciali degli individui**: il punteggio DPC di base di un determinato set di dati potrebbe anche essere aumentato nel caso in cui gli individui appartengano a un gruppo sociale con esigenze particolari (es. Minori, individui di un particolare gruppo con caratteristiche speciali). Ad esempio, il punteggio DPC di un elenco di numeri di telefono aumenterebbe se riguardasse membri noti del parlamento nazionale

Tra i fattori che possono **attenuare** la portata del Data Breach vi sono:

- **Disponibilità pubblica**: il punteggio DPC di base di un set di dati può essere ridotto anche nel caso in cui i dati violati fossero già disponibili pubblicamente prima della violazione o possano essere facilmente raccolti e / o accessibili tramite fonti pubblicamente disponibili.
- **Natura dei dati:** un altro fattore attenuante potrebbe essere, in alcuni casi, la natura stessa di un particolare set di dati che, nonostante il suo punteggio DPC iniziale, è di minore importanza in termini di informazioni che può rivelare sull'individuo, ad esempio:
    - il caso di un certificato medico che attesta solo che l'individuo è in buono stato di salute senza rivelare altre informazioni. In questo caso, sebbene il punteggio di base sarebbe 4 poiché i dati sanitari sono dati particolari, il punteggio DPC finale del set di dati specifico sarebbe 1, in quanto non può di per sé influenzare la vita personale dell'individuo. Questo fattore, tuttavia, dovrebbe essere considerato con grande attenzione motivando comunque il motivo per cui un particolare trattamento dei dati è, per sua natura, inferiore al suo punteggio DPC di base;
    - I dati violati, in relazione al contesto della violazione, non sono utili o non possono essere utilizzati per azioni malevoli e/o frodi e/o il set di dati coinvolti include alcune informazioni finanziarie che comunque non forniscono ancora caratteristiche

significative sullo stato / situazione finanziaria dell'individuo (ad es. numeri di conto bancario semplici senza ulteriori dettagli oppure una contabile di prelievo o versamento);

- I dati violati consentono una comprensione parziale delle informazioni dell'interessato; sono rivelate informazioni finanziarie che NON consentono comunque di ricostruire l'effettiva situazione patrimoniale del cliente o rivelare dati particolari o creare un profilo preciso dell'interessato (attraverso la comprensione e le abitudini dell'interessato).

3.4 ULTERIORI FATTORI LEGATI AL CONTESTO DELLA VIOLAZIONE

Notorietà dell'interessato (VIP)

I personaggi pubblici (VIP), comprese le persone politicamente esposte (PEP), quando coinvolti nella violazione, potrebbero essere soggetti, per via della loro notorietà quasi sempre collegata ad una buona posizione patrimoniale e reputazionale, a notevoli disagi.

Le voci delle tipologie disponibili per l'attribuzione del VIP sono le seguenti:

- Interessato comune, valore uno (1);
- Interessato con caratteristiche particolari, valore due (2).

Il coinvolgimento di un personaggio pubblico (VIP) raddoppia la gravità della violazione.

Numero di Interessati Coinvolti (NR)

Il **numero degli interessati** (**NR**) coinvolto nella violazione esprime la portata della violazione rispetto al numero degli interessati.

I dati di un soggetto, violati nel contesto di un incidente di maggiori dimensioni, possono essere potenzialmente rivelati con maggior facilità. Inoltre, l'elevato numero di interessati coinvolti influenza la probabilità che uno di questi possa avere delle conseguenze negative.

Il livello della gravità della violazione rimane immutato se il numero di interessati coinvolti nella violazione **non** comporta un aumento delle conseguenze del Data Breach.

Tale parametro assume un valore compreso fra 1 e 2:

- Valore 1 (costante), quando il numero di interessati coinvolti nella violazione **non** producono un aumento della portata delle conseguenze del Data Breach;

- Valore 2 (moltiplicatore), quando il numero di interessati coinvolti nella violazione **producono** un aumento consistente della portata delle conseguenze del Data Breach;

3.5 FACILITÀ DI IDENTIFICAZIONE (EI)

Questo fattore esprime la facilità con cui chi ha accesso ai dati violati può identificare i soggetti interessati; i valori sono stati distinti in quattro livelli:

- è impossibile risalire all'identità dell'interessato tramite l'analisi dei dai violati. I dati violati potrebbero infatti essere stati cifrati, o trovarsi su un supporto protetto da crittografia (ad esempio tramite BitLocker);
- è possibile risalire all'identità dell'interessato con un impegno oneroso. Quando ad esempio non vengono fornite informazioni specifiche dell'individuo e non è possibile trovare informazioni aggiuntive se non si ottiene l'accesso al database di riferimento per individuare a chi si riferisce (ad esempio perché il cognome è ampiamente diffuso nel contesto di riferimento);
- è possibile risalire all'identità dell'interessato con un impegno minimo;
- è possibile risalire direttamente all'identità dell'interessato.

Per ciascuna tipologia di voce è abbinato un valore, da zero a uno (0-1), in funzione della facilità di identificazione dell'interessato.

3.6 CARATTERISTICHE DELLA VIOLAZIONE (CV)

La probabilità che l'evento possa comportare un rischio per i diritti e le libertà dell'individuo è determinata dalla natura e dal contesto della violazione nonché da informazioni in possesso del Titolare che gli consentono di ponderare, stimare e valutare i rischi per gli interessati.

Per determinare quindi la probabilità che l'evento possa comportare dei rischi sui diritti e le libertà dell'individuo, il compilatore del Tool in formato Excel, dovrà descrivere in modo puntuale le caratteristiche dell'evento stesso, indicando in particolare se tali eventi possono essere di natura accidentale o intenzionale scegliendo uno dei valori riportato nella tabella seguente:

Caratteristiche Violazione: Descrive eventuali fattori, derivanti dalle circostanze specifiche della violazione, che possono attenuare o aggravare gli effetti della violazione.
Accidentale: ad esempio i dati sono stati forniti a un numero contenuto di soggetti identificabili (inferiore a 4) considerati non pericolosi (es. Errore interno) e non c'è evidenza che i dati rivelati conducano a uno dei rischi indicati nella legenda sottostante. Sono state adottate inoltre le misure necessarie per mitigare il rischio

Accidentale: ad esempio i dati sono stati forniti a un numero NON contenuto di soggetti identificabili (superiore a 4) considerati non pericolosi (es. Errore interno) e non c'è evidenza che i dati rivelati conducano a uno dei rischi indicati nella legenda sottostante. Sono state adottate inoltre le misure necessarie per mitigare qualsiasi rischio.
Accidentale: ad esempio i dati sono stati forniti a soggetti identificabili considerati non pericolosi (es. Errore interno) ma l'evento potenzialmente potrebbe avere delle conseguenze sull'interessato nonostante le misure adottate.
Accidentale: i dati sono forniti a soggetti non identificabili come per lo smarrimento di dati personali a causa di un errore accidentale; l'evento potenzialmente potrebbe avere delle conseguenze sull'interessato. Oppure, quando i dati sono stati divulgati accidentalmente a soggetti considerati pericolosi ma data la natura dei dati oggetto della violazione e le misure adottate per contenere il rischio, le conseguenze per gli interessati sono contenute e difficilmente possono avere delle conseguenze per l'interessato.
Intenzionale: I dati sono stati acquisiti da soggetti considerati pericolosi ma data la natura dei dati oggetto della violazione le conseguenze per gli interessati sono contenute e difficilmente possono dare corso a uno dei rischi evidenziati nella legenda sottostante.
Intenzionale: i dati sono stati acquisiti da soggetti considerati pericolosi che potrebbero dare corso a una delle conseguenze evidenziate nella legenda sottostante.

Nello scegliere una delle caratteristiche della violazione sopra indicate, l'operatore dovrà considerare anche i possibili rischi che sono indicati nella tabella seguente:

Legenda rischi per i diritti e le libertà dell'individuo
Il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo
Gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o che venga loro impedito l'esercizio del controllo sui dati personali che li riguardano
Sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza
In caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali
Sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

Si evidenzia che l'adozione di misure tempestive può ridurre la probabilità che l'vento abbia conseguenze avverse. Per tale motivo il compilatore dovrà indicare nel tool, le misure adottate per diminuire o contenere la probabilità che l'evento comporti dei rischi per i diritti e le libertà dell'individuo.

Si riporta a titolo d'esempio anche quanto indicato dal WP29 all'interno delle "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679", in merito ai fattori che possono influenzare la probabilità che l'evento comporti un rischio per i diritti e le libertà dell'individuo:

"Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Prendiamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un terzo di cui all'articolo 4, punto 10, o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o a un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e potrebbe essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. Anche se i dati fossero stati consultati, il titolare del trattamento potrebbe comunque confidare nel fatto che il destinatario non intraprenderà ulteriori azioni in merito agli stessi e restituirà tempestivamente i dati al titolare del trattamento e coopererà per garantirne il recupero. In tali casi, questo aspetto può essere preso in considerazione nella valutazione del rischio effettuata dal titolare del trattamento in seguito alla violazione; il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione, anche se questo non significa che non si sia verificata una violazione. La probabilità che detta violazione presenti un rischio per le persone fisiche verrebbe però meno, quindi non sarebbe più necessaria la notifica all'autorità di controllo o alle persone fisiche interessate. Ancora una volta, tutto dipenderà dalle circostanze del caso concreto. Ciò nonostante, il titolare del trattamento deve comunque conservare informazioni relative alla violazione nel contesto del suo dovere generale di conservare registrazioni in merito alle violazioni (cfr. seguente sezione V).

3.7 CALCOLO DEL RISCHIO

Il valore di rischio stimato è determinato dalla seguente formula:

RISCHIO= [(DPC corretto) x NR x VIP x EI] x CV

Il risultato finale, determinato dall'applicazione della formula, sarà ricompreso in un *range* di valori, a loro volta riconducibili ad uno dei cinque livelli, ossia:

- Improbabile;
- Trascurabile;
- Limitato;
- Significativo;

- Massimo.

La seguente tabella di sintesi esprime, per ogni livello, le azioni conseguenti al risultato della valutazione.

La tabella ha una funzione indicativa; la valutazione della violazione deve considerare, oltre i fattori secondo il metodo descritto nel presente documento, le peculiarità di ogni singolo Data Breach nonché i potenziali rischi per l'Interessato.

INDICE	RISCHIO	Annotazione su Registro Data Breach	Notifica al Garante Privacy	Notifica agli interessati
0	Assente	NO	NO	NO
se < 1	Improbabile	Si	NO	NO
1 <= se < 2	Trascurabile	Si	SI	NO
2 <= se < 3	Limitato	SI	SI	SI
3 <= se < 4	Significativo	SI	SI	SI
se > 4	Massimo	SI	SI	SI

4. Criteri di valutazione nei casi di violazione della disponibilità ed integrità dei dati personali

4.1 PREMESSA

Riprendendo quanto previsto dall'art. 4.1.12 del GDPR, il WP29 ha espresso all'interno delle linee guida sul Data Breach le seguenti definizioni di violazione di disponibilità e integrità:

- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentale o non autorizzata di dati personali.

È opportuno precisare che la definizione di violazione di dati personali o Data Breach prescinde dalla considerazione della causa od origine della violazione, elemento che può acquisire rilevanza in relazione alla valutazione della probabilità di rischio per i diritti degli interessati, della gravità della violazione e delle possibili conseguenze.

Si tenga inoltre presente che, mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente evidente, può essere meno ovvio determinare se vi è stata una violazione della disponibilità. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali.

Esempi
Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata permanente.

Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (denial of service) che rende i dati personali indisponibili.
Ci si potrebbe chiedere **se una perdita temporanea della disponibilità dei dati personali costituisca una violazione** e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".
Di conseguenza, **un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione**, in quanto la mancanza di accesso ai dati può **avere un impatto significativo sui diritti e sulle libertà delle persone fisiche**. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.
Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento

a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

4.2 CRITERI DI VALUTAZIONE INDISPONIBILITÀ E VIOLAZIONE INTEGRITÀ

Laddove si verifichi l'indisponibilità dei dati dell'interessato o una violazione dell'integrità degli stessi, come prima analisi l'incaricato deve verificare se l'evento in questione, può comportare uno dei seguenti impatti:

Impatto	Esempi	Gravità
Nessuno impatto o conseguenze effimere	Incidenti che, sebbene siano considerate violazioni dei dati personali, non arreca all'interessato disagi, ad esempio incidenti operativi o informatici, risolti in modo semplice e veloce, senza particolari riflessi per gli interessati.	**assente**
Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).	Esempi di impatti trascurabili sono: irritazione, ricevimento di fastidiose mail, mal di testa, perdita di tempo dovuta a ripetizione delle procedure o all'attesa della loro effettuazione, riutilizzo dei dati a scopo di pubblicità mirata per beni di consumo corrente, impressione di violazione della privacy, ecc.	**trascurabile**
Gli individui possono andare incontro a disagi e inconvenienti, che saranno in grado di superare nonostante alcune difficoltà.	Esempi di impatti sono paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc… pubblicità online mirata su un aspetto di vita privata che la persona voleva mantenere riservata ecc. Pagamenti imprevisti (es: multe inflitte erroneamente), costi aggiuntivi (es: spese bancarie, legali tasse), inadempienze di pagamento; Negazione dell'accesso a servizi amministrativi o servizi commerciali. Opportunità di comfort perse (es: annullamento acquisti, vacanze, cessazione di un account online) Mancata promozione della carriera Servizi online bloccati account (es: giochi, amministrazione) Ricezione di non richiesti invii mirati probabilmente danneggiare la reputazione di interessati Aumento dei costi (es: aumento prezzi assicurativi) Dati non aggiornati (es: posizione ricoperta in precedenza)	**Limitata**

Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà.	In questo caso l'evento rappresenta un rischio per i diritti e le libertà. Esempi di impatto sono grave affezione fisica che provochi danni a lungo termine; perdite monetarie non indennizzate, perdita di opportunità uniche e non ricorrenti (mutui immobiliari, studi, tirocini o occupazioni, interdizione da esami scolastici), perdita dell'abitazione, del posto di lavoro, ecc. appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).	**Significativa**
Gli individui possono subire conseguenze significative o irreversibili, che non sono in grado di superare.	Esempi di impatto sono: affezione fisica a lungo termine o permanente, alterazione permanente dell'integrità fisica, decesso; rischio finanziario, indebitamento ingente, impossibilità di lavorare, incapacità di ricollocazione, smarrimento di elementi di prova nell'ambito di un contenzioso, perdita di accesso a infrastrutture vitali (acqua, elettricità, disturbo psicologico a lungo termine o permanente, sanzione penale, allontanamento, perdita di legami familiari, perdita della capacità di agire, cambio di stato amministrativo e/o perdita dell'autonomia legale (tutela) ecc.	**Massima**

L'impatto potrà dipendere non solo dalla natura dei dati colpiti dall'evento ma anche da altri fattori quali ad esempio il loro contributo nel portare a termine servizi o richieste da parte dell'interessato, la presenza di una copia dei dati andati persi e il periodo di tempo durante il quale tali dati rimangono indisponibili, oppure eventuali conseguenze che potrebbero scaturire da una modifica che ha violato l'integrità dei dati.

Laddove, ad esempio, i clienti della banca, a causa di un malfunzionamento o altro evento tecnico che riguardasse l'operatività dell'intero servizio dei bonifici in uscita, non riuscissero ad effettuare le operazioni necessarie entro un determinato periodo di tempo e questa indisponibilità comportasse un impatto sugli interessati, allora si avrebbe un evento di data breach. In questo caso la probabilità che l'evento dia effettivamente luogo ad un data breach sarà funzione del tempo entro il quale i servizi che permettono l'accesso ai dati della clientela e ne permettono quindi la loro esecuzione sono ripristinati alla normale operatività.

5. Notifiche al Garante e agli interessati

5.1 NOTIFICA ALLE AUTORITÀ COMPETENTI

I valori ed i criteri impiegati mediante il tool in Excel, che esprime i criteri descritti all'interno della presente metodologia, possono essere integrati alla notifica inviata alle autorità competenti.

Se per qualche ragione il livello di gravità complessivo è ritenuto non congruo, la funzione deputata, indicata nella procedura di gestione dei data breach, dovrà dichiarare il livello ritenuto "corretto", corredando la segnalazione con gli argomenti che giustificano la differente valutazione; ogni cambiamento apportato al punteggio finale dovrà essere giustificato.

5.2 NOTIFICA AI SOGGETTI INTERESSATI

Il livello di gravità può essere altresì utilizzato dal titolare e dalle autorità competenti per valutare la necessità, o meno, di notificare la violazione anche ai soggetti interessati.