PROCEDURA DATA BREACH E NIS 2

Redazione	Approvazione	Verifica formale	Emissione
Gruppo privacy aziendale	Amministratori: **DALILA PETRILLO** **STEFANO PETRILLO** **GAETANO PETRILLO**	Responsabile HSE Responsabile per la Qualità, Responsabile IT Punto di contatto NIS	Responsabile HSE Responsabile per la Qualità, Responsabile IT Punto di contatto NIS

SOMMARIO

1 PREMESSA....3

2 SCOPI/OBIETTIVI....3

3 CAMPO DI APPLICAZIONE....3

4 MODIFICHE/ REVISIONI PRECEDENTI....3

5 GLOSSARIO....4

6 MATRICE DELLE RESPONSABILITA'....5

7 DESCRIZIONE DELLE ATTIVITA'....5

8 RIFERIMENTI E ALLEGATI....19

9 VERIFICA / INDICATORI / PARAMETRI DI CONTROLLO....19

10 DIFFUSIONE DELLA PROCEDURA PER IL DATA BREACH....19

1 Premessa

La procedura illustra le azioni da compiere in caso di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti interessati o di incidenti rilevanti, a chi devono essere comunicate e in che modo, secondo le disposizioni del Regolamento UE 2016/679 in materia di protezione dei dati personali e il D.Lgs. 138/2024 che recepisce la Direttiva UE 2022/2555 (c.d. Direttiva NIS 2).
La Procedura è adottata alla luce delle Linee-guida EDPB 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali, delle prescrizioni EDPB "*Guidelines on Personal data breach notification under Regulation 2016/679*" adottate il 03/10/2017 e da ultimo aggiornate il 28 marzo 2023.

2 Obiettivo

Definire il processo di gestione delle violazioni di dati personali ai sensi degli artt. 33 e 34 del GDPR, nonché degli incidenti informatici rilevanti ai sensi del D.Lgs. 138/2024 (ovvero incidenti che comportano un impatto significativo sulla fornitura del servizio).

3 Campo di applicazione

La procedura deve essere applicata:

- Ai sensi della normativa in materia di protezione dei dati personali, in tutti i casi in cui si verifichi sui dati personali una perdita di confidenzialità, integrità o riservatezza, (i.e. distruzione o diffusione indebita, a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi che possano comportare pericoli significativi per la protezione dei dati degli interessati);
- Ai sensi della DIRETTIVA (UE) 2022/2555 e del Decreto Legislativo n. 138/2024, nel caso di incidenti che hanno un impatto significativo sulla fornitura dei servizi.

4 Modifiche / revisioni precedenti

Revisione	**Data**	**Motivo dell'aggiornamento**
0	Gennaio 2026	Prima emissione

La procedura rimane in vigore come descritta fino a che non ve ne sia una revisione o necessità di modificarla nei suoi contenuti a fronte di nuove indicazioni normative, linee guida specifiche o criticità emergenti dalla sua applicazione; è prevista una sua revisione ogni cinque anni per riconferma o modifica.

5 Glossario

Termine e Abbreviazione	Definizione
S.C. e S.S.	Struttura Complessa e Struttura semplice
GDPR	Regolamento (Reg) UE 2016/679 in materia di protezione dei dati personali
Decreto NIS 2	Il Decreto Legislativo 138/2024 che recepisce la Direttiva NIS 2 2022/2555
EDPB e EDPB	Working Party Art. 29 - Gruppo di lavoro Art. 29 - dal 25/05/2018 EDPB (European Data Protection Board – Comitato Europeo per la Protezione dei Dati)
DPO	Data Protection Officer
ACN	Agenzia per la Cybersicurezza Nazionale
CSIRT	Computer Security Incident Response Team - Gruppo di intervento per la sicurezza informatica in caso di incidente
NIS	Network and Information Security
TITOLARE DEL TRATTAMENTO	La società Prestige Group S.r.l. che determina la finalità e i mezzi del trattamento dei dati personali. L'art. 4 n. 7 del GDPR in particolare definisce 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 di trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
INTERESSATO	La persona fisica identificata o identificabile (Art. 4, n. 1, del GDPR) a cui si riferisce il dato personale oggetto di trattamento.
RESPONSABILE ESTERNO	La persona fisica o giuridica, l'Autorità Pubblica, il servizio o altro organism, che tratta dati personali per conto del Titolare del trattamento (ex Art.4, n.8 del GDPR)

RESPONSABILE CYBERSICUREZZA	Il responsabile della cybersicurezza ha il compito di gestire la sicurezza informatica e proteggere i dati sensibili relativi ai pazienti e alle operazioni interne dell'ente. Le sue principali responsabilità includono: • **Protezione dei dati**: Garantire che i dati personali e altre informazioni sensibili siano protetti contro accessi non autorizzati, perdite o danni, in conformità con le normative sulla protezione dei dati (come il GDPR). • **Gestione delle minacce**: Monitorare e rilevare potenziali minacce informatiche (virus, malware, attacchi informatici) e intervenire tempestivamente per mitigare i rischi. • **Implementazione di politiche di sicurezza**: Definire e implementare politiche e procedure di sicurezza informatica interne, stabilendo linee guida utili a gestire, trattare e proteggere le informazioni. Con determina del C.d.A. del 07.10.2025 è stato nominato il sig. Antonio Lapiccirella come "Punto di contatto" di cui all'articolo 7, comma 1, lettera c) del decreto NIS, quale Referente per la cyber sicurezza.

PUNTO DI CONTATTO	Il Punto di Contatto NIS 2 agisce come la porta di ingresso e il canale principale per la gestione della sicurezza informatica all'interno di un'organizzazione, coordinando con le autorità competenti e supportando le attività di risposta agli incidenti in caso di minacce o attacchi. Con determina del C.d.A. del 07.10.2025 è stato nominato il sig. Antonio Lapiccirella come "Punto di contatto" di cui all'articolo 7, comma 1, lettera c) del decreto NIS, quale Referente per la cyber sicurezza.
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 (Ex Art. 4, n. 1, del GDPR)
TRATTAMENTO	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione (Ex Art. 4, n. 2, del GDPR).
DATA BREACH	La violazione dei dati personali è 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.(Ex Art. 4, n.12, del GDPR)
INCIDENTE	Un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi (art. 2 D.Lgs. 138/2024).
INCIDENTE SIGNIFICATIVO	Ai sensi dell'art. 25 del D.Lgs. 138/2024, si intende una violazione che può comportare: a) una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) ripercussioni su altre persone fisiche o giuridiche, causando perdite materiali o immateriali considerevoli.

6 Matrice delle responsabilità

L'adozione delle misure descritte nel presente documento deve avvenire, da parte del personale, in relazione alle attività condotte e nel rispetto delle specifiche competenze professionali.

7 Descrizione delle attività

7.1 Premessa

Per ***data breach*** si intende 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 (tale definizione è data all'art. 4 punto 12) del GDPR), che fa sì che il Titolare del trattamento non sia più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali (come da art. 5 del GDPR e art. 3 del D.Lgs 51/2018).

La sicurezza (come si evince dall'Art. 32 par. 1 GDPR) ha tre componenti:

1. la riservatezza o confidenzialità,
2. l'integrità
3. la disponibilità.

La violazione di confidenzialità descrive la fuoriuscita di dati personali rispetto ai soggetti autorizzati; viene declinata sia in forma di divulgazione, sia di accesso non autorizzato: nel primo caso, si tratta di dare conoscenza di dati personali a terzi; nel secondo, prendere conoscenza di dati personali.

La violazione di integrità indica, invece, l'alterazione delle informazioni, inclusa la perdita di completezza delle stesse o anche l'aggiunta arbitraria di elementi; si tratta quindi di modifica non autorizzata di dati personali.

La violazione di disponibilità coglie l'elemento della raggiungibilità o utilizzabilità dei dati personali: l'inutilizzabilità dei dati personali è conseguenza della distruzione o perdita degli stessi.

L'*European Data Protection Board* (EDPB) specifica che "perdita" non significa solo cessazione del possesso (ad esempio, per smarrimento o furto), ma anche perdita della facoltà di accesso ai dati personali, ad esempio dovuta a corruzione irrecuperabile del file system o da attacco ransomware. Nelle linee guida dell'EDPB si parla anche di indisponibilità temporanea, ad esempio per interruzione temporanea di un servizio.

Le violazioni descritte possono verificarsi disgiuntamente o congiuntamente fra di loro, anche solo come effetto di un unico evento.

Il titolare del trattamento è obbligato ad adottare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio del trattamento (con l'obiettivo di evitare distruzione accidentale o illecita, perdita, modifica, rivelazione, accesso non autorizzato).

Con l'avvento del GDPR, la valutazione delle misure di sicurezza è rimessa al titolare. A tale scopo la società Prestige Group S.r.l. ha adottato come criterio le misure di sicurezza cosiddette AGID (Circolare 18 aprile 2017, n. 2/2017); ha costituito un gruppo di lavoro e un organigramma privacy (designati, referenti, autorizzati, responsabili ex-art. 28, ecc.), ed ha adottato una policy aziendale, che definisce anche la strategia per la protezione dei dati personali.

La presenza di policy che descrive come l'organizzazione prende in considerazione l'eventualità dell'occorrenza di incidenti di sicurezza che possano compromettere i dati personali trattati dall'Azienda, veicolando flussi informativi interni ed esterni, anche attraverso procedure come questa che hanno lo scopo di rispettare i dettami degli articoli 33 e 34 del GDPR, implica l'integrazione, sin dalla progettazione dei processi dell'organizzazione, di una sequenza di passaggi che rendono la stessa in grado di diminuire l'impatto di una violazione, di gestirne le fasi per limitare i danni sugli interessati, di regolare efficacemente le comunicazioni e la cooperazione con l'Autorità Garante per la Protezione Dati Personali, rispettando così anche il principio di *accountability* di cui all'art. 24 GDPR e il principio di *data protection by design* di cui all'art. 25 GDPR.

In proposito, si richiama il paragrafo 2 dell'art. 32 del Regolamento che recita: "*Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*".

Si fa inoltre riferimento al Considerando 76 del GDPR: "*La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*".

Un *data breach* può originare sia dall'esterno, sia dall'interno dell'Azienda: un incauto utente che modifica erroneamente un database o un malware, che crittografa una cartella di rete o un semplice smarrimento di una chiavetta USB / di un telefonino aziendale o l'invio di un dato personale inviato ad un terzo non autorizzato costituiscono tutte potenziali violazioni dei dati personali.

In caso di violazione dei dati personali, il GDPR (agli articoli 33 e 34) prevede espressamente l'obbligo in capo al Titolare di notificazione all'Autorità Garante per la protezione dei dati personali e comunicazione agli interessati.

Il GDPR, inoltre, attribuisce alla suddetta notifica una funzione essenziale di tutela degli interessati, con la volontà di affrontare e gestire nell'immediatezza una violazione, al fine di evitare l'insorgenza o l'aggravamento di danni materiali o immateriali alle persone interessate (perdita di controllo dei dati, limitazione dei diritti dell'interessato, discriminazione, furto o usurpazione dell'identità, perdite finanziarie, ecc.)

L'episodio pregiudizievole, pertanto, non deve mai essere celato, poiché l'oscuramento della notizia può amplificare gli effetti negativi dell'evento dannoso e inibire forme di intervento dell'Autorità di controllo così come dell'interessato i cui dati sono stati violati.

Il criterio dirimente per valutare la necessità di avviare una procedura di notifica è la probabilità che la violazione possa porre a rischio (per la notifica all'autorità) o ad elevato rischio (per la comunicazione agli interessati) le libertà e i diritti degli individui.

Appurato il rischio conseguente dalla violazione, gli artt. 33 e 34 del GDPR indicano ai titolari i termini, le modalità, i contenuti e le deroghe della notifica e della comunicazione di *data breach*. Inoltre, le linee guida dell'EDPB integrano gli articoli citati.

Secondo il GDPR, la notifica di eventuali violazioni di dati dovrà avvenire possibilmente senza ingiustificato ritardo ed entro le 72 ore dal momento in cui si è venuto a conoscenza della violazione.

Per incidente significativo, ai sensi dell'art. 25 del D.Lgs. 138/2024, si intende una violazione che può comportare:

a) una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) ripercussioni su altre persone fisiche o giuridiche, causando perdite materiali o immateriali considerevoli.

Si osserva inoltre che, ai sensi della Direttiva UE 2022/2555 (cosiddetta Direttiva NIS 2), come recepita nel D.Lgs 138/2024, gli incidenti aventi un impatto rilevante sulla continuità dei servizi essenziali prestati, anche se non coinvolgono dati personali, devono comunque essere notificati senza indebito ritardo anche al CSIRT (Computer Security Incident Response Team - Gruppo di intervento per la sicurezza informatica in caso di incidente) e all'autorità NIS competente, cioè ACN. Per la Direttiva, si definisce incidente "*ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi*".

In questo caso, quindi, si sovrappongono le due normative e l'Azienda, che eroga il servizio interessato dall'incidente (e dalla contestuale violazione dei dati personali), deve adempiere agli obblighi di notifica previsti da entrambe le normative, ossia deve effettuare sia la notifica per gli incidenti di cui alla Direttiva NIS, sia la notifica per la violazione dei dati personali prevista dal GDPR.

Va evidenziato che non tutte le violazioni di sicurezza determinano necessariamente una violazione di dati personali, potendo riguardare informazioni non connesse a persone fisiche o identificabili: non tutti i *data breach* sono anche *personal data breach*.

E' inoltre da rilevarsi che la sicurezza dei trattamenti di dati personali non è esclusivamente di tipo informatico o fisico, ma anche organizzativo, dovuto a inefficienze quali il mancato censimento dei flussi di dati (ad esempio, la non completezza del Registro dei trattamenti), la carenza di policy necessarie, l'omessa individuazione di profili di autorizzazione di chi può accedere e a che cosa, la concessione di autorizzazioni a soggetti che non devono averla, deficienze nell'allocazione dei ruoli di trattamento.

7.2 La gestione dell'evento

7.2.1 L'accertamento della violazione

I termini della notifica decorrono dal momento in cui il Titolare acquisisce consapevolezza dell'avvenuta violazione.

Incidente di sicurezza endo-aziendale

In questo caso l'incidente di sicurezza deve essere comunicato dal singolo dipendente, che ne accerta il verificarsi al livello gerarchico superiore in modo che poi la notizia sia acquisita dal Titolare.

Tale soggetto che viene a conoscenza della violazione della sicurezza dei dati personali effettiva,

potenziale o sospetta deve darne quindi immediata comunicazione a:

- Responsabile Privacy
- Responsabile Informatica, Telecomunicazioni e Sistema Informatico
- Punto di Contatto NIS2

La definizione di incidente di sicurezza è molto ampia, pertanto, quando si verifica un evento di violazione, è opportuno innanzitutto partire dall'ipotesi che riguardi dati personali, avviare le successive indagini e poi eventualmente pervenire ad una diversa conclusione, in modo che tutte le misure di sicurezza e di rischio siano state correttamente e tempestivamente attivate.

Si ribadisce che:

- se l'incidente di sicurezza non ha coinvolto dati personali, non è identificabile come *data breach;*

- se la violazione di sicurezza riguarda dati personali, configura un'ipotesi di *data breach*.

Per comprendere cosa si intende per "dato personale", si deve tenere conto che sono dati personali tutte quelle informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute la sua situazione economica.

Come sottolinea il Garante nelle istruzioni in merito, l'identificazione richiede elementi che permettano di distinguere una persona dalle altre: ad esempio, il nome e il cognome è evidente che identificano direttamente una persona; ma anche il numero di telefono, il codice fiscale, l'indirizzo IP, la targa di un veicolo consentono di identificare una persona, in modo indiretto. Sono pertanto dati personali, i dati anagrafici (nome, cognome, data di nascita, luogo di nascita), i dati di contatto (indirizzo postale, indirizzo di posta elettronica, numero di telefono fisso o mobile), dati di accesso e di identificazione (username e password), dati di geolocalizzazione, dati di pagamento.

Vanno considerati con massima cautela e delicatezza i dati appartenenti a categorie particolari (cfr, art. 9 del GDPR), quali quelli idonei a rivelare le condizioni di salute o la vita sessuale o l'orientamento sessuale, i dati genetici e i dati biometrici, insieme ai dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati relativi a condanne penali o reati (art. 10 GDPR).

Incidente di sicurezza presso il Responsabile esterno

Qualora la violazione sia avvenuta presso un Responsabile esterno ex-art.28 GDPR, a cui è stato affidato il trattamento, il Responsabile esterno deve comunicare senza ingiustificato ritardo, e comunque entro le 24 ore, all'Azienda sanitaria l'avvenuta violazione (è ammesso, se giustificato, un posticipo entro le 48 solo in casi eccezionali); dal momento dell'avvenuta comunicazione da parte del Responsabile esterno, decorrono i termini di 72 ore a carico del Titolare per la notifica al Garante. È importante sottolineare che nei contratti/atti/convenzioni che affidano servizi a Responsabili ex-art. 28 deve essere specificato il tempo entro il quale l'avvenuta violazione viene comunicata all'Azienda sanitaria.

Le "*Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679*" del EDPB sottolineano che il Responsabile del trattamento non è il soggetto che deve valutare la probabilità che la violazione presenti un rischio per gli interessati: infatti, il responsabile deve accertare solo se si è verificata una violazione e in caso positivo deve notificarla al Titolare del trattamento senza indugio.

Nel caso in cui informazioni di dettaglio circa le cause e circostanze della violazione non siano tempestivamente disponibili, il responsabile informa comunque immediatamente il Titolare dell'avvenuta violazione, comunicando in un momento successivo, non appena disponibili, le informazioni di dettaglio.

L'obbligo di comunicazione consente al Titolare del trattamento di venire a conoscenza della violazione, di fronteggiarla in maniera tempestiva ed efficace e di stabilire, anche sulla base delle informazioni fornite dal Responsabile, se la violazione deve essere notificata al Garante e comunicata agli interessati coinvolti.

Successivamente, il Responsabile esterno deve supportare e fornire al Titolare tutta la collaborazione e tutto il supporto necessari a ricostruire l'avvenuto e a ripristinare la situazione, così come stabilito contrattualmente.

Il soggetto all'interno dell'Azienda che riceve una comunicazione di un Data Breach da parte di un Responsabile deve comunicare l'evento a:

- Responsabile Privacy
- Responsabile Informatica, Telecomunicazioni e Sistema Informatico
- Punto di Contatto NIS2

Unità di gestione Data Breach

L'"unità di gestione *data breach*" è costituita da:

- Responsabile Privacy
- Responsabile Informatica, Telecomunicazioni e Sistema Informatico
- Punto di Contatto NIS2

Il Gruppo è coordinato dal Responsabile Privacy ed è integrato, laddove necessario, da strutture e soggetti specifici in relazione alla natura ed oggetto del *data breach*. Le riunioni possono svolgersi anche in modalità remota, mediante l'impiego di strumenti per la videoconferenza.

L'"unità di gestione *data breach*" è competente a gestire l'evento dall'inizio alla sua conclusione e sarà di riferimento per tutte le problematiche. All'"unità di gestione *data breach*" collabora anche il Responsabile esterno qualora la violazione si sia verificata presso tale soggetto.

Il Titolare, con il supporto delle figure sopra individuate, verifica se l'incidente di sicurezza sia tale da far scattare l'obbligo di notifica al Garante ed eventualmente di comunicazione agli interessati.

7.2.2 Individuazione e valutazione del tipo di violazione

Secondo quanto indicato dalla norma, come illustrato nelle premesse cui si rinvia, i tipi di violazione che necessitano di notifica sono:

- Violazione di riservatezza del dato;
- Violazione di integrità del dato;

- Violazione di disponibilità del dato.

Il Titolare, ricevuta la segnalazione della gravità dell'incidente, con l'assistenza del Gruppo di lavoro, effettua un'ulteriore analisi del rischio dell'incidente al fine di valutare la necessità di procedere alla notifica all'Autorità Garante per la protezione dei dati personali ed eventualmente alle comunicazioni agli interessati ai sensi dell'art. 33 GDPR.

Come previsto dal GDPR, tale valutazione viene condotta con modalità oggettive, in base ai seguenti criteri.

a. GRAVITÀ DELL'IMPATTO

Il requisito della gravità è valutato attraverso 3 indicatori, secondo la presente formula: Gravità (GR)= T + C + G.

- tipologia dei dati oggetto della violazione (T);
- tipologia di Interessati coinvolti e caratteristiche del Titolare (C);
- gravità delle conseguenze per l'Interessato (G).

Tipologia dei dati oggetto della violazione (T)

	Valore	*Tipologia di dati oggetto della violazione*
Tipologia di dati oggetto della violazione (T)	1	Dati personali comuni
	2	Altre tipologie di dati rilevanti nel caso concreto (es. economici, di posizione, ecc)
	3	Dati Particolari e Dati relativi a condanne e reati
	4	Combinazione di più categorie

Tipologia di Interessati coinvolti e caratteristiche del Titolare (C)

Nel caso in cui la violazione coinvolga categorie di Interessati particolarmente vulnerabili (es. dipendenti con patologie) e nei casi in cui il trattamento presenti caratteristiche che ne determinino una particolare capacità lesiva, è applicato un correttivo di valore compreso tra 1 e 4, in base alle peculiarità del singolo caso concreto.

Gravità delle conseguenze per l'Interessato (G)

L'impatto che la violazione può produrre sull'Interessato è misurato in termini di disponibilità, integrità e riservatezza dei dati.

Tali valori si declinano in:

- danno per la reputazione;
- discriminazione;
- furto di identità (nome e cognome);
- perdite finanziarie;
- dati fisici o psicologici;
- perdita di controllo dei dati;
- altri svantaggi economici e sociali;
- impossibilità di esercitare diritti, servizi o opportunità.

In relazione alle caratteristiche del caso specifico, l'impatto è valutato con valore compreso tra 1 e 4.

Entità/Gravità delle conseguenze	**Valore attribuito**
Trascurabile	1
Basso	2
Medio	3
Elevato	4

Livello Gravità	**Riservatezza (divulgazione e accesso illegittimo)**	**Integrità (alterazione illegittima)**	**Disponibilità (distruzione illegittima, indisponibilità, perdita dei dati)**
1 - <u>Trascurabile</u>	La mancanza di riservatezza, di integrità o di disponibilità ha impatti lievi (es. fastidio) sulla vita sociale o personale degli Interessati. Ad esempio, perdita di tempo nel dover ripetere le procedure o di aspettarle, riutilizzo dei dati da parte di terzi per scopi pubblicitari, senso di violazione della *privacy* senza danno reale.		
2 - <u>Basso</u>	La mancanza di riservatezza, integrità e disponibilità ha impatti, non critici e che creano piccole difficoltà (es. costi, paura, incomprensioni, stress, malanni minori) a causa degli effetti sulla vita sociale o personale degli Interessati.		
3 - <u>Medio</u>	La mancanza di riservatezza, integrità e disponibilità ha un elevato impatto che può essere superato con difficoltà sulla vita sociale o personale degli Interessati. Ad esempio fondi non disponibili, blocco da parte di enti economici, danni alla proprietà, perdita del posto di lavoro, denunce, peggioramento della salute, appropriazione indebita di denaro, guadagni persi, perdita di lavoro, vittima di ricatti, cyberbullismo, molestie morali.		

4 - <u>Elevato</u>	La mancanza di riservatezza, integrità e disponibilità ha impatti irreversibili sulla vita sociale o personale e comporta: - perdita di autonomia; - esclusione (p.e. inabilità a lavorare); - sanzioni penali e perdita di libertà; - danni fisici (p.e. danni fisici o mentali a lungo termine o morte); - impossibilità di azione legale; - squilibrio di potere; - perdita di fiducia; - perdita economica.

Applicando quanto sopra riportato, la gravità dell'evento è misurata secondo la seguente formula: Gravità (GR)= T + C + G.

Gravità	Valore attribuito
Trascurabile	I = un valore pari o inferiore a 3
Basso	I = un valore pari o inferiore a 6
Medio	I= un valore pari o inferiore a 9
Elevato	I = un valore pari o inferiore a 12

b. LA PROBABILITÀ DELL'IMPATTO

Il requisito della probabilità è, invece, misurato attraverso 3 fattori, secondo la seguente formula: N + F + V:

- numero di individui impattati dalla violazione (N);
- facilità di identificazione per i casi di perdita di riservatezza o facilità di ripristino per i casi di perdita di disponibilità e integrità (F);
- tipologia di violazione (V).

Numero di persone fisiche coinvolte

	Valore	*Numero dei soggetti Interessati*
Numero di Interessati coinvolti dal Data Breach (N)	1	Meno di 100
	2	Più di 100
	3	Più di 1.000
	4	Più di 5.000

Facilità di identificazione (in caso di perdita di riservatezza)

Facilità di	*Valore*	*Facilità di identificazione*

identificazione (F)	4	L'identificazione dei soggetti interessati è possibile attraverso la semplice conoscenza del dato oggetto della violazione.
	3	L'identificazione dei soggetti interessati attraverso la semplice conoscenza del dato oggetto della violazione è possibile attraverso ulteriori dati facilmente accessibili.
	2	L'identificazione dei soggetti interessati attraverso la semplice conoscenza del dato oggetto della violazione è difficile, ma possibile con grandi sforzi.
	1	L'identificazione dei soggetti interessati attraverso la semplice conoscenza del dato oggetto della violazione è assolutamente impossibile.

Facilità di recupero dei dati (per perdita di integrità e disponibilità)

	Valore	*Facilità di recupero dati*
Facilità di recupero dati (F)	4	La società non ha implementato un sistema di *back up* e non è possibile ripristinare i dati.
	3	La società ha implementato un sistema di *back up* che permette il ripristino dei dati in tempi lunghi e con difficoltà.
	2	La società ha implementato un sistema di *back up* che permette il ripristino dei dati in tempi brevi (c.a. 3 giorni).
	1	La società ha adottato un sistema di *disaster recovery* che permette il ripristino dei dati nell'immediatezza della violazione.

Tipologia di violazione

	Valore	*Tipologia di violazione*
Tipologia di violazione (V)	1	Perdita di disponibilità temporanea
	2	Perdita di disponibilità definitiva o Perdita di riservatezza o Perdita di integrità
	3	Due tipologie di violazione insieme
	4	Tre tipologie di violazione insieme

Pertanto, la probabilità dell'impatto sarà pari a: N + F + V

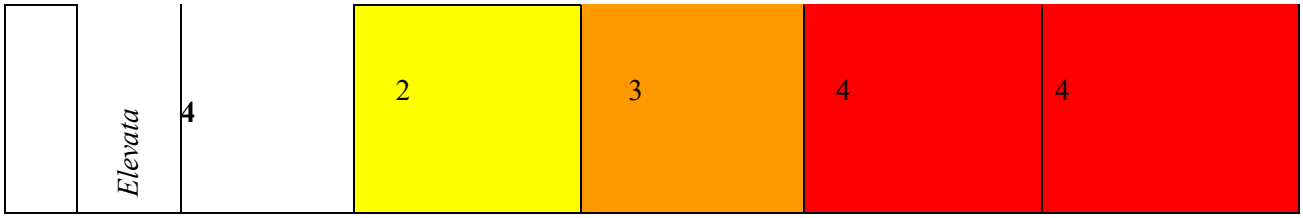
Sulla base del valore ottenuto si provvederà a definire il livello di probabilità, secondo le seguenti proporzioni:

Probabilità	Valore attribuito
Trascurabile	P = un valore pari o inferiore a 3
Basso	P = un valore pari o inferiore a 6
Medio	P = un valore pari o inferiore a 9
Elevato	P = un valore pari o inferiore a 12

c. IL LIVELLO DI RISCHIO PER I DIRITTI E LE LIBERTÀ DEGLI INTERESSATI

Il livello del rischio per i diritti e le libertà degli Interessati sarà definito sulla base della formula **R= GxP** attraverso la seguente tabella:

			Probabilità			
			Trascurabile	*Bassa*	*Media*	*Elevata*
			1	**2**	**3**	**4**
Gravità	*Trascurabile*	**1**	1	1	2	2
	Bassa	**2**	1	2	3	3
	Media	**3**	2	3	3	4



- Improbabile **R = un valore pari o inferiore a 1**
- Poco Probabile **R = un valore pari o inferiore a 2**
- Probabile **R = un valore pari o inferiore a 3**
- Altamente probabile **R = un valore pari o inferiore a 4**

Laddove il rischio per gli interessati risulti improbabile, non sarà necessario procedere con la notifica al Garante; laddove invece risulti poco probabile, sarà discrezione del Titolare valutare la necessità di notifica tenendo conto del caso concreto. Infine, laddove il rischio risulti probabile o altamente probabile, sarà necessario procedere immediatamente con la notifica.
Sulla base della valutazione dei rischi eseguita, il Titolare, con il supporto del Gruppo di lavoro Operativo, determina se sia necessario o meno notificare la violazione al Garante per la Protezione dei Dati e se sia necessario o meno effettuare la comunicazione agli Interessati.

Laddove non sia possibile, in considerazione dei termini per la notifica del Data Breach, convocare il Gruppo di lavoro, il Titolare del trattamento ha comunque l'obbligo di procedere alla notifica in via cautelativa.

In ragione dell'attività svolta, dei presidi di controllo adottati e delle procedure già in essere, la società rileva il seguente livello di rischio di data breach:
Gravità: Bassa (2)
Probabilità: Media (3)

7.2.3 Contenuto della notifica

La violazione non sarà oggetto di comunicazione esclusivamente nel caso in cui la valutazione condotta dia atto dell'elevata improbabilità che la violazione produca effetti sui diritti e le libertà degli Interessati. Se, al contrario, la valutazione non attesta tale elevata improbabilità e rileva una concreta possibilità che la violazione possa determinare effetti negativi, si procederà con l'analisi del livello di rischio e, ove tale analisi evidenzi un probabile rischio per i diritti e le libertà degli Interessati, la violazione verrà notificata al Garante, non oltre le 72 ore decorrenti dal momento in cui il Titolare abbia avuto conoscenza della stessa.
Il termine per la notifica all'Autorità di controllo competente decorre dal momento in cui il Titolare percepisce, con un ragionevole grado di certezza, che un incidente di sicurezza – informatico o materiale – abbia compromesso dei dati personali.
Ove non sia possibile rispettare tale termine il Titolare del trattamento dà evidenza delle ragioni del ritardo nella notifica successivamente effettuata.

La notifica all'Autorità Garante deve contenere le seguenti informazioni:

a. la 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;
b. gli eventuali dati anagrafici e di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere maggiori informazioni;
c. le probabili conseguenze della violazione dei dati personali;
d. le misure adottate o di cui si propone l'adozione da parte del Titolare del Trattamento al fine di porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora (e nella misura in cui) non sia possibile indicare tutte le informazioni contestualmente, queste potranno essere fornite anche in fasi successive senza ulteriore ingiustificato ritardo.

La notifica della violazione è effettuata attraverso apposito form disponibile sul sito web del Garante Privacy (***www.garanteprivacy.it***).

La notifica è inviata dal rappresentante legale della società.

Inoltre, il Legale rappresentante ha la facoltà di individuare un soggetto a cui delegare la notifica relativa a un singolo *data breach* o, in alternativa, l'intera gestione delle notifiche relative a tutti i *data breach*.

Comunicazione agli interessati

La violazione sarà oggetto di comunicazione esclusivamente nel caso in cui la valutazione condotta dia atto dell'elevata gravità per i diritti e le libertà degli Interessati.

La comunicazione deve descrivere in un linguaggio semplice e chiaro:

- la natura della violazione dei dati personali;
- il nome e i dati del punto di contatto NIS 2 presso cui ottenere informazioni;
- le probabili conseguenze della violazione dei dati personali;
- le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e attenuarne gli eventuali effetti negativi.

La violazione dei dati personali deve essere comunicata direttamente agli Interessati attraverso uno dei seguenti mezzi: e-mail, lettere, sms ed altre forme di messaggistica diretta.

Nelle ipotesi in cui l'esecuzione della comunicazione con tali modalità comporti uno sforzo sproporzionato, la società può procedere con una comunicazione pubblica, attraverso pubblicazione di specifico annuncio sul proprio sito internet o tramite una misura analoga ma altrettanto efficace.

Qualora, pur avendo appurato con ragionevole certezza l'esistenza di una violazione, il Titolare non sia in possesso di tutti gli elementi utili per effettuare la descrizione completa ed esaustiva della violazione, si può bilanciare le esigenze di celerità del messaggio con quelle di una sua sostanziale accuratezza e completezza, procedendo per gradi, attraverso una notifica preliminare che contenga, in prima battuta, il numero approssimativo di persone e dati interessati dalla violazione ed una notifica integrativa successiva, che ne definisca il numero esatto, in seguito agli approfondimenti condotti.

7.3 Notificazione di incidente rilevante al CSIRT

Ai sensi del D.Lgs. 138/2024, che recepisce la Direttiva UE 2022/2555, qualora un incidente rientri nella categoria prevista e comporti un impatto rilevante sulla continuità dei servizi essenziali prestati – anche in assenza di coinvolgimento di dati personali – esso dovrà essere notificato al **Computer Security Incident Response Team** (sin d'ora per brevità, CSIRT) entro 24 ore dal momento in cui il Titolare ne abbia avuto conoscenza.

Ai sensi dell'art. 25 del D.Lgs. 138/2024, la società Prestige Group S.r.l. deve trasmettere al CSIRT:

a) senza ingiustificato ritardo, e comunque **entro 24 ore** da quando si è venuti a conoscenza dell'incidente significativo, una **pre-notifica** che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b) senza ingiustificato ritardo, e comunque **entro 72 ore** da quando sono venuti a conoscenza dell'incidente significativo, **una notifica dell'incidente** che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;

d) **una relazione finale entro un mese** dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:

- una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
- il tipo di minaccia o la causa originale (*root cause*) che ha probabilmente innescato l'incidente;
- le misure di attenuazione adottate e in corso;
- ove noto, l'impatto transfrontaliero dell'incidente;

Laddove, al momento della trasmissione della relazione finale, l'incidente sia in corso, la società dovrà trasmettere una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

La comunicazione al CSIRT è a cura del Punto di Contatto NIS della azienda registrato presso il portale ACN, in quanto tale soggetto – secondo le disposizioni dell'articolo 25 del d.lgs. n. 138/2024 - ha il compito di curare l'attuazione delle disposizioni del decreto NIS per conto del soggetto stesso, a partire dalla registrazione, e interloquisce, per conto del soggetto NIS, con l'Autorità nazionale competente NIS.

7.4 Registro dei *data breach*

Il Titolare del trattamento deve documentare tutte le violazioni dei dati personali che si verificano, indipendentemente dal fatto che una violazione debba o meno essere notificata al Garante.

Ai sensi dell'art. 33, par. 5 del Reg. UE 2016/679, è istituito il "*Registro dei casi di data breach*", comprendente qualsiasi violazione dei dati personali e la descrizione dell'evento. Si stabilisce di tenere documentazione nel Registro dei casi di violazione notificati al Garante ed eventualmente comunicati agli interessati; a parte, si tiene inoltre traccia anche dei casi occorsi che non hanno richiesto la notifica e/o la comunicazione.

Il tracciamento dei casi di violazione dei dati personali viene effettuato allo scopo di:

- Individuare e tenere sotto controllo i fattori di rischio
- Misurare l'efficacia delle *policy* aziendali e delle procedure adottate
- Ispezioni ed indagini, anche per dimostrare di essere "*compliant*" rispetto a leggi e *best practices*: infatti le Linee Guida raccomandano di documentare il ragionamento alla base delle decisioni prese in risposta a una violazione, come, ad esempio, il perché una determinata violazione non è stata notificata al Garante.

8 Riferimenti normativi

- Regolamento Generale sulla Protezione dei Dati Regolamento Europeo 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("GDPR").
- Decreto legislativo 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali e s.m.i., in particolare Decreto Legislativo n.101/2018.
- Provvedimento dell'Autorità Garante per la Protezione Dati Personali sulla notifica delle violazioni dei dati personali (data breach) – 30 luglio 2019
- Prescrizioni del EDPB "Guidelines on Personal data breach notification under Regulation 2016/679, adottate il 03/10/2017 (ultima revisione 28/03/2023)
- Linee Guida EDPB sugli esempi di data breach (01/2021)
- Decreto Legislativo 04/09/2024 n. 138 Attuazione della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione
- Circolare 18 aprile 2017, n. 2/2017, recante «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», pubblicata in Gazzetta Ufficiale (Serie Generale n.103 del 5-5-2017)

9 Verifica/ Indicatori di verifica/ Parametri di controllo

Criterio	Indicatore	Standard
Tempestività	N° ore da accertamento violazione a notifica	Entro 72 ore
Sicurezza	N° di violazioni annue	meno di 10 violazioni annue in media
Sicurezza	N° di notifiche al garante /n° violazioni soggette a notifiche	100%
Sicurezza	N° di comunicazioni agli interessati/n° violazioni rischio elevato	100%

10 Diffusione della procedura per il *data breach*

La presente Procedura viene pubblicata sul sito aziendale al seguente link: *https://www.prestigegroupsrl.it.*