



DATA BREACH LINEE GUIDA

Allegato al Decreto Presidente ERSU n.5/2024



ENTE REGIONALE PRO SU DERETU A S'ISTUDIU UNIVERSITARIU DE CASTEDDU
ENTE REGIONALE PER IL DIRITTO ALLO STUDIO UNIVERSITARIO DI CAGLIARI



REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

Allegato A

PROCEDURA DATA BREACH LINEE GUIDA

PREMESSA

L'articolo 4 del Regolamento UE 2016/679 (d'ora in poi GDPR) definisce "data breach" (o, nella traduzione italiana, violazione dei dati personali) 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**¹ trasmessi, conservati o comunque trattati presso una Azienda o una Pubblica Amministrazione.

Gli articoli 33 e 34 del GDPR si occupano, rispettivamente, di disciplinare la notifica di una violazione dei dati personali all'autorità di controllo e la comunicazione di una violazione dei dati personali all'interessato.

Il presente documento illustra la procedura per lo svolgimento delle principali attività rivolte all'attuazione delle disposizioni del GDPR in caso di episodi di "data breach" che riguardino l'Ente conformemente a quanto disposto dall'art. 7 delle Direttive approvate con Decreto del Presidente 17 maggio 2018, n. 4 cui si rinvia.

1 TIPOLOGIE DI VIOLAZIONE DI DATI

La norma di chiusura delle Direttive approvate con Decreto del Presidente dell'ERSU 17 maggio 2018, n. 4, l'art. 7 rubricato "procedimento in caso di violazione dei dati personali (data breach)" introduce il concetto di violazione di dati personali (data breach) trasmessi, conservati o comunque trattati² dall'Ente stabilendo le regole di condotta da seguire e le attività da apprestare da parte dei soggetti coinvolti.

Dal tenore del comma 3 del medesimo articolo 7 si evince altresì che il Direttore Generale è preposto alla gestione del data breach è, pertanto, assume il ruolo di referente del data breach per il Titolare con compiti e funzioni previsti dagli artt. 33 e 34 del GDPR e quindi destinatario delle segnalazioni da parte dei dipendenti e collaboratori che agiscono sotto l'autorità del titolare o suo delegato.

¹ L'articolo 4 del GDPR definisce "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, i 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.

Sono categorie particolari di dati personali quei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici (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), i 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), i dati relativi alla salute (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), alla vita sessuale o all'orientamento sessuale della persona.

² Per "trattamento" si intende 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

Sul piano operativo, è pertanto necessario fornire agli attori coinvolti precise istruzioni procedurali in relazione all'applicazione e attuazione della disciplina dettata dall'art. 7 al fine di individuare e riparare tempestivamente all'eventuale data breach occorso nell'ambito dei trattamenti di propria competenza mappati ai sensi del Decreto del Presidente 23 maggio 2018, n. 5 come aggiornati con Decreto del Commissario Straordinario marzo 2021, n. 10 e Decreto del Presidente 28 marzo 2023, n.2 in ragione della nuova organizzazione della struttura dell'Ente con distribuzione delle funzioni e competenze all'interno dei Servizi ed Uffici titolari dei procedimenti indicati nell'apposito Registro dei Trattamenti ex art. 5 del GDPR.

Di seguito sono elencati possibili eventi che possono determinare violazioni di dati personali (in termini di confidenzialità, integrità, disponibilità). L'elencazione non è esaustiva e il verificarsi di uno degli eventi descritti non costituisce condizione sufficiente per stabilire l'effettiva sussistenza di un data breach.

Il verificarsi di un evento (anche non espressamente indicato nel presente documento) che prospetti il rischio di una violazione di dati personali costituisce sempre un fattore di allerta che richiede sempre un'analisi -anche a diversi livelli - per stabilire se si è verificato un data breach.

L'elenco è suddiviso in due parti: una riferita ai trattamenti informatici e una ai trattamenti cartacei.

1.1 EVENTI RELATIVI A TRATTAMENTI INFORMATICI

1.1.1 Eventi accidentali:

Eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali (confidenzialità, integrità o disponibilità) in caso di trattamenti informatici. Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in outsourcing) quali:

- Esecuzione erranea di comandi e/o procedure, ad esempio: pubblicazione erranea delle informazioni personali (non di dominio pubblico) su siti web dell'ERSU; erroneo invio di informazioni a enti/soggetti esterni all'ERSU, formattazione di dispositivi di memorizzazione, errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato, ecc.
- Rottura di componenti hardware, ad esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e/o di elettricità, umidità; corto circuito; caduta accidentale; eventi catastrofici; incendi, ecc.
- Malfunzionamento di software, ad esempio: esecuzione di uno script automatico non autorizzato; errori di programmazione del software che causano output errati, ecc.
- Visibilità errata di dati sui siti web dell'Amministrazione, ad esempio: visibilità da parte di utenti di dati di altri utenti anche per casi di omonimia, ecc.
- Fornitura di dati a persona diversa dall'interessato, ad esempio: comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato, ecc.
- Guasti alla rete, ad esempio: caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.

1.1.2 Eventi dolosi

Eventi dolosi causati da personale interno o soggetti esterni realizzati tramite:

1. Accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione.
2. Compromissione o rivelazione abusiva di credenziali di autenticazione.
3. Utilizzo di software malevolo.
4. Altro.

In tale casistica sono compresi incidenti di sicurezza ICT che comportano la violazione di dati personali:

- Furto: furto di supporti di memorizzazione e/o elaborazione contenenti dati personali (es: furto laptop, hard disk, chiavette USB, smartphone, tablet, ecc.).
- Truffa informatica esterna: tutti i casi di frodi realizzate da un soggetto esterno all'amministrazione rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente o da suoi fornitori, ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi; appropriazione di dati bancari; appropriazione (e diffusione) delle credenziali di autenticazione ai servizi degli utenti.
- Truffa informatica interna: tutti i casi di frodi realizzate da personale interno all'Amministrazione che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

1.2 EVENTI RELATIVI A TRATTAMENTI CARTACEI

1.2.1 Eventi accidentali:

Eventi anomali, determinati da calamità o da fatti fortuiti, nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei contenenti dati personali in possesso dell'Ente quali:

- Distruzione accidentale di documenti, ad esempio in caso di incendio/allagamento dei locali dove sono presenti gli archivi cartacei presso le sedi dell'ERSU o di propri fornitori; distruzione per errore di documenti originali, senza eventuale copia; ecc.
- Smarrimento di documenti: ad esempio perdita di documenti contenenti dati personali; ecc.
- Fornitura involontaria di dati a persona diversa dall'interessato o a persona non autorizzata al trattamento.

1.2.2 Eventi dolosi:

Comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali dell'ERSU e/o strutture collegate quali:

- Distruzione dei documenti: ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati personali; accesso non autorizzato da parte di terzi ad archivi interni dell'ERSU e distruzione volontaria di documenti contenenti dati personali.

- **Accesso non autorizzato:** ad esempio accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi di questo Ente o propri fornitori. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.
- **Furto:** sottrazione da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati personali

2. GLI ATTORI DEL DATA BREACH

2.1 Soggetti attivi (o attori) sono tutti coloro che si occuperanno dell'episodio di "data breach" dalla fase di rilevazione dell'incidente alla fase di notifica di cui agli artt. 33 e 34 del GDPR, nel rispetto ed osservanza delle direttive di cui al Decreto del Presidente n.4/2018 e ss.mm.ii.; i ruoli coinvolti sono:

- **Titolare**, nella persona del suo delegato/soggetto designato (incaricato): è 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; l'Ente ha previsto nelle Direttive approvate con Decreto n. 4/2018 la delega (art.2, comma 2 e art. 3) di funzioni in capo ai Direttori di Servizio e dipendenti (art. 3, lettera o) e art.4). Il Titolare, pertanto, in caso di data breach, è il Direttore Generale e/o Direttore di Servizio che regge la struttura in cui si è rilevata la violazione o un episodio che possa determinarla.
- **RPD: Responsabile Protezione Dati o Data Protection Officer (DPO):** il soggetto nominato dall'Ente con riferimento agli articoli 37, 38, 39 del GDPR.
- **Referente data breach:** è il soggetto che svolge funzioni di referente per il supporto giuridico/procedurale per il data breach per il cui tramite il delegato del titolare trasmette le notifiche in esito alla procedura di data breach. Ai sensi dell'art. 7, comma 2 della Direttive, il referente data breach per l'Ente, è il Direttore Generale
- **Referente interno:** è il dipendente/collaboratore che ha rilevato o a cui è stato segnalato un evento anomalo di potenziale violazione di dati personali ed è tenuto alla comunicazione dell'incidente.

Processo di gestione del data breach

Qualsiasi dipendente o collaboratore dell'ERSU, a prescindere dal ruolo rivestito, nel momento in cui è a conoscenza di un episodio di potenziale data breach deve dare immediata comunicazione dello stesso al dirigente (Delegato del Titolare) responsabile della struttura presso la quale presta servizio secondo la procedura definita al paragrafo successivo. Se dalla prima analisi da parte del dirigente emergono elementi tali da escludere la possibile violazione dei dati personali, l'anomalia viene gestita all'interno della struttura interessata. Se, invece, dalla prima analisi emergono gli estremi per una probabile violazione, si procede ai necessari approfondimenti.

La seconda parte del processo è, pertanto, soltanto eventuale e si verifica qualora il Dirigente ravvisa un data breach o ritiene che un evento possa configurarsi come data breach:

in questo caso procede senza indugio (entro 24 ore dalla conoscenza della violazione da parte del dipendente o collaboratore), a segnalare l'episodio ad un gruppo di intervento costituito dallo stesso e dai seguenti soggetti:

- Il Direttore Generale quale il referente data breach per il supporto giuridico/procedurale;
- il/i Responsabile/i IT;
- il RPD;
- il referente in sede del RPD;
- il Responsabile della conservazione.

al fine di compiere le azioni necessarie per ridurre i rischi e comunque procedere alla raccolta delle informazioni necessarie per coadiuvare il Delegato del Titolare nell'effettuare le valutazioni in ordine alla sussistenza, dimensione e impatto della violazione e supportare lo stesso nella redazione della notifica all'autorità di controllo (Garante per la protezione dei dati personali), se dovuta.

Il gruppo degli attori sopra indicati si riunisce in tempi brevissimi e coinvolge all'occorrenza altri soggetti (anche fornitori esterni) che possano dare un contributo alle azioni di cui sopra.

In caso di constatazione di violazione dei dati personali, il Dirigente (Delegato dal Titolare), per il tramite del Direttore Generale (Referente data breach), notifica, ai sensi dell'art. 33 c. 1 del GDPR, la violazione 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.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. Il Direttore Generale (Delegato del Titolare), nel caso in cui ricorrano le condizioni previste dall'art. 34 del GDPR procede altresì alla comunicazione agli interessati valutando la modalità idonea a garantire le finalità della disposizione normativa. Qualora l'episodio riveli una matrice criminale o dolosa il Direttore Generale (Delegato del Titolare) procede al coinvolgimento dell'Autorità di Pubblica Sicurezza (con ogni probabilità la Polizia Postale) mettendola a conoscenza di tutti gli elementi in proprio possesso ed evidenziando l'obbligo di notifica entro 72 ore dalla conoscenza della violazione all'autorità Garante Nazionale e se sussistano i presupposti per la notifica anche agli interessati. Le azioni poste in essere devono risultare da atti formali. Pertanto, anche se per velocizzare gli interventi cisi avvarrà delle modalità più immediate, si dovranno formalizzare i passaggi salienti anche con la redazione di verbali.

3.1 Fasi del processo

3.1.1 Rilevazione dell'incidente e segnalazione

In questa fase si acquisisce la notizia di una possibile violazione di dati personali. La segnalazione di un possibile data breach può provenire dall'esterno (cittadini, fornitori esterni, enti istituzionali ecc.) o dall'interno, da parte di qualsiasi dipendente o collaboratore dell'ERSU durante il normale svolgimento dell'attività lavorativa. Il dipendente/collaboratore che riceve la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di potenziale violazione di dati personali deve segnalarlo immediatamente, anche per le vie brevi, al Delegato del Titolare (Direttore generale di riferimento o suo sostituto) e al Dirigente della struttura organizzativa presso la quale presta servizio che potranno avvalersi del supporto del Responsabile IT di dominio della stessa struttura organizzativa e/o di altri soggetti responsabili di attività da cui possono derivare ulteriori elementi conoscitivi, al fine di effettuare insieme una prima valutazione (rapida e di massima) ed assicurarsi con certezza che l'evento segnalato non costituisca un data breach.

Qualora venga ravvisato un pericolo di violazione di dati personali (data breach) e, comunque, nei casi dubbi, al fine di porre in essere le eventuali successive azioni da attivare tempestivamente per mitigare o eliminare i rischi, il Dirigente titolare dell'articolazione organizzativa gravata dalla violazione dovrà avvisare gli altri soggetti attivi, ossia:

- il Referente data breach;
- il RPD;
- il/i Responsabile/i IT;
- il Responsabile della Conservazione.

La fase di rilevazione dell'incidente e segnalazione deve concludersi entro 24 ore dalla conoscenza della violazione da parte del dipendente o collaboratore.

3.1.2 Raccolta delle informazioni inerenti all'evento

Qualora sia stato ravvisato un potenziale data breach e il Delegato del Titolare abbia proceduto a coinvolgere gli altri soggetti attivi, dovranno essere acquisiti gli elementi necessari per condurre la fase successiva di ulteriore valutazione al fine di escludere o confermare la sussistenza del data breach. A tal fine è attivata senza indugio da parte del Direttore Generale (Referente data breach) la riunione con i restanti soggetti attivi (il Dirigente (Delegato del Titolare), il Responsabile/i IT, Responsabile della Conservazione, RPD e, se necessario, Referente interno).

Gli stessi procedono alla raccolta delle informazioni necessarie per la successiva fase di valutazione e a una prima analisi di identificazione della tipologia di violazione. Il Direttore Generale quale Referente data breach, anche su richiesta degli altri soggetti attivi, al fine di integrare l'analisi, coinvolge altri soggetti responsabili di attività da cui possono derivare ulteriori elementi conoscitivi, i quali devono garantire tempestivamente il supporto richiesto. Se dalla prima analisi del gruppo di intervento emergono elementi tali da escludere la possibile violazione dei dati personali, la gestione dell'anomalia viene rimandata all'interno della struttura interessata.

Se, invece, emergono gli estremi per una probabile violazione, si procede ai necessari approfondimenti. Nella pratica, rilevazione e valutazione dell'evento sono spesso interconnesse e già nell'immediato può essere riscontrato un rischio ragionevole di violazione e, anche se non sono disponibili subito maggiori informazioni di dettaglio, si rende necessaria una preventiva comunicazione al Garante da parte del Dirigente del Titolare, per il tramite del Referente data breach.

Nella pratica, rilevazione e valutazione dell'evento sono spesso interconnesse e già nell'immediato può essere riscontrato un rischio ragionevole di violazione e, anche se non sono disponibili subito maggiori informazioni di dettaglio, si rende necessaria una preventiva comunicazione al Garante da parte del Dirigente (Delegato del Titolare), per il tramite del Referente data breach.

Vi sono casi in cui è possibile definire se l'evento costituisca una violazione ai sensi del GDPR solo al termine della fase di valutazione a cui partecipano tutti i soggetti attivi. In quest'ultimo caso la decorrenza delle tempistiche per la comunicazione al Garante (72 ore) è dal momento della constatazione. La notifica deve essere redatta dal Delegato del Titolare ai sensi dell'art. 33 del GDPR e inviata all'Autorità di controllo a cura del Referente data breach.

Il WP29 ha chiarito che, nell'ipotesi in cui i titolari del trattamento (o loro delegati) non siano in possesso di tutte le informazioni relative alla violazione nelle 72 ore successive al suo verificarsi, con *Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP250, versione emendata e adottata il 6 febbraio 2018* (<https://www.garanteprivacy.it/regolamentoue/databreach>), essi hanno la possibilità di comunicare entro il termine di legge all'Autorità di controllo la sola violazione subita, per poi fornire in un successivo momento tutte le informazioni richieste dal suddetto art. 33, corredandole con i motivi del ritardo.

3.1.3 Valutazione dell'evento

Scopo di questa fase è quello di confermare o meno l'avvenuta violazione, di circostanziare in modo completo l'evento e fornire una valutazione del possibile pregiudizio per gli interessati. I soggetti attivi effettuano un'analisi di dettaglio, esaminano le informazioni aggiuntive e valutano il livello di rischio dell'evento e il livello di pregiudizio per gli eventuali interessati impattati dalla violazione.

Nel caso in cui, dall'analisi, si constati che l'evento costituisce una violazione dei dati personali, da questo momento decorrono le tempistiche (dal momento della conoscenza 72 ore¹¹) previste dalla normativa in tema di comunicazioni al Garante.

La notifica all'Autorità di controllo deve essere redatta dal Delegato del Titolare ai sensi dell'art. 33 del GDPR e trasmessa a cura del Referente data breach. Il gruppo di intervento accerta anche se la violazione di dati comporti un elevato pregiudizio per i diritti e le libertà degli interessati (cittadini, dipendenti, soggetti terzi, ecc.) a fini della comunicazione agli stessi. Nel caso in cui ricorrano le condizioni previste dall'art. 34 del GDPR, il Delegato del Titolare procede alla comunicazione agli interessati valutando la modalità idonea a garantire le finalità della disposizione normativa. Qualora l'episodio riveli una matrice criminale o dolosa il Delegato del Titolare procede al coinvolgimento dell'Autorità di Pubblica Sicurezza (con ogni probabilità la Polizia Postale) mettendola a conoscenza di tutti gli elementi in proprio possesso. Nella comunicazione dovranno essere evidenziati l'obbligo di notifica entro 72 ore dalla conoscenza della violazione all'autorità Garante Nazionale e l'eventuale sussistenza dei presupposti per la notifica anche agli interessati. Per la valutazione dell'evento e relativa graduazione della gravità si rinvia al paragrafo 4: "Metodologia valutazione data breach" a seguire predisposta dall'Unità

3.1.4 Comunicazione

In caso di violazione dei dati che comporti un elevato pregiudizio per i diritti e le libertà degli interessati (cittadini, dipendenti, soggetti terzi, ecc.), ai sensi dell'art. 34 del GDPR, il Delegato del Titolare comunica la violazione agli stessi senza ingiustificato ritardo. Il gruppo di intervento supporta il Delegato del Titolare nel verificare che siano o meno soddisfatte le condizioni di cui al c. 3 dell'art. 34 del GDPR per le quali non è previsto l'obbligo di comunicazione agli interessati. Qualora non ricorra nessuna tali condizioni, il gruppo di intervento supporta il Delegato del Titolare nella predisposizione del testo della comunicazione e nella individuazione della modalità di diffusione. La comunicazione agli interessati dovrà descrivere con un linguaggio semplice e chiaro la natura della violazione e contenere almeno le informazioni e le misure di cui all'art. 33 par. 3, lett. b), c) e d) del GDPR. Nel caso in cui l'Autorità di Pubblica Sicurezza, interessata all'evento data breach, dovesse richiedere di ritardare la comunicazione agli interessati per non pregiudicare lo svolgimento delle indagini, il Referente data breach - su disposizione della Autorità di P.S. -

può chiedere al Garante l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento delle stesse.

3.1.5 Processo di gestione del data breach in caso di segnalazione da parte di fornitori

Nel caso in cui un fornitore dell'ERSU, in qualità di responsabile del trattamento, venga a conoscenza di una violazione (o presunta tale) di dati personali trattati nell'ambito dell'erogazione di un servizio, effettua una prima analisi dell'accaduto e, ove accerti che si tratti di un data breach, invia la segnalazione al Delegato del Titolare (Direttore generale della struttura per la quale eroga il servizio), al RPD, al/ai Responsabile/i IT, al Referente data breach e al Responsabile della conservazione senza ingiustificato ritardo. La segnalazione deve contenere tutti gli elementi utili alla comprensione/identificazione dell'evento. Il fornitore garantisce, inoltre, assistenza al Delegato del Titolare fornendo eventuali informazioni aggiuntive per la corretta valutazione e gestione dell'evento.

Il Delegato del Titolare che riceve la segnalazione procede secondo quanto previsto ai paragrafi 3.1.2, 3.1.3, 3.1.4.

3.2 Aspetti sanzionatori

Secondo quanto disposto dall'art. 83 c. 4 del GDPR, la violazione degli obblighi del titolare del trattamento e del responsabile del trattamento previsti dagli artt. 8, 11, da 25 a 39, 42 e 43 è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 euro; rientrano, pertanto, anche le violazioni alle procedure in materia di data breach, previste dagli artt. 33-34 del GDPR. Inoltre, l'art. 82 prevede che chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).

Lo stesso GDPR, all'art. 83 c. 2, indica dei fattori che possono mitigare o aggravare la violazione; un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del titolare che può dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione. L'atteggiamento reattivo e cooperativo comporta sicuramente un'attenuazione delle sanzioni applicabili.

Dalla lettura dei punti indicati in nota e, in particolare dei punti c, e, f, h, k, appare evidente come una corretta gestione della procedura sia importante per limitare, in caso di violazione di una disposizione, l'applicazione delle sanzioni connesse. In tal senso, fermo restando la necessità di una continua formazione del personale, si raccomanda di scoraggiare atteggiamenti reticenti o non pienamente collaborativi in quanto la segnalazione del possibile data breach e un pronto intervento di gestione rappresentano sicuramente comportamenti valutabili in senso positivo secondo quanto detto sopra.

3.3 Registro violazioni

L'art. 33 c. 5 del GDPR dispone: *"Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio."* L'ERSU si è dotato di un apposito registro dei trattamenti in cui è presente una sezione per la registrazione delle violazioni dei dati personali.

In detta sezione sono annotate a cura del RPD tutte le informazioni richieste dalla normativa vigente, quali, ad es.: (a) le circostanze relative alla violazione; (b) le conseguenze; (c) i provvedimenti adottati per contrastarla e limitarne gli effetti; (d) i dati personali coinvolti, ecc. A tal fine al RPD è trasmessa, a cura del Referente data breach, tutta la documentazione necessaria allo stesso per procedere alle registrazioni compresi i verbali delle riunioni dei soggetti attivi.

Le comunicazioni inviate al CERT-PA ai sensi dell'art. 4 della Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia digitale devono essere altresì trasmesse al RPD anche ai fini delle eventuali segnalazioni nel registro. I dati presenti nel registro sono trattati nel rispetto del principio di minimizzazione e secondo le misure per mitigare i rischi di violazione dei dati personali.

4. METODOLOGIA VALUTAZIONE DATA BREACH

Nell'ipotesi in cui, nonostante le misure di sicurezza adottate al fine di prevenire il rischio di perdita di dati si verifichi un potenziale data breach, qui di seguito la metodologia per **la valutazione della gravità delle violazioni dei dati personali** adottata dalla Regione Sardegna. Tale metodologia è stata definita sulla base delle indicazioni fornite dall'**ENISA** (European Union Agency for Network and Information Security) all'interno del documento "*Recommendations for a methodology of the assessment of severity of personal data breaches*".

Gli elementi chiave da tenere in considerazione in sede di valutazione della gravità risultano essere i seguenti:

- **La natura e contesto dei dati violati (VALUTAZIONE 1)**
- **Facilità di identificazione** dell'individuo in base ai dati violati (**VALUTAZIONE 2**)
- **Circostanze della violazione** (violazione di riservatezza, integrità e disponibilità dei dati), che hanno un'influenza aggiuntiva sulla gravità di una violazione (**VALUTAZIONE 3**)

La valutazione della gravità della violazione può essere effettuata secondo le seguenti sotto fasi:

- **Valutazione 1** analizzare la criticità dell'insieme di dati violati in un contesto di elaborazione specifico;
- **Valutazione 2:** si tratta del fattore di correzione della Valutazione 1. La criticità complessiva di un trattamento dei dati può essere ridotta in base al valore identificato.
- **Valutazione 3:** quantifica le circostanze specifiche della violazione che possono essere presenti o meno in una particolare situazione. Pertanto il fattore, laddove presente, può solo incrementare la gravità di una specifica violazione. Per questo motivo il punteggio iniziale può essere ulteriormente regolato da quest'ultima valutazione
- **Valutazione 4 - Calcolo della gravità:** calcolo della gravità della violazione sulla base dei 3 precedenti elementi.

Definizione del punteggio per la natura e contesto dei dati violati (VALUTAZIONE 1)

Il punteggio della valutazione 1 (*di seguito anche "pt.1"*) è al centro della metodologia e valuta la criticità dell'insieme di dati violati in un contesto di elaborazione specifico.

Nella tabella seguente sono riassunte le attività inerenti a questa fase di valutazione:

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
1	RPD /Cyber Security	Definire e Classificare i tipi di dati personali	Definisce e classifica la tipologia di dato trattato che ha subito una violazione sulla base delle seguenti quattro categorie: <ul style="list-style-type: none"> • dati identificativi/personali; • dati comportamentali; • dati finanziari; • dati sensibili/particolari. Inoltre, aggiorna il Registro dei Data Breach nella sessione "Tipologia di dato trattato" (fare riferimento all'allegato B)	Registro dei Data Breach (allegato B)
2	RPD / Cyber Security	Attribuire il punteggio base	Attribuisce il punteggio base secondo la tabella 1 definita dalla metodologia per le categorie di natura di dato (dati identificativi/personali, dati comportamentali, dati finanziari, dati sensibili).	Tabella 1 Contesto Elaborazione Dati
3	RPD / Cyber Security	Aumentare o Ridurre il punteggio base secondo il contesto specifico	Aumenta o riduce il punteggio base in funzione della presenza di fattori contestuali relativi all'elaborazione dei dati (ad es. volume di dati, caratteristiche speciali dei Titolari o degli individui, inesattezza dei dati, disponibilità del dato al pubblico prima della violazione, natura del dato). Il punteggio che emerge dalla tabella 1 può variare da 1 a 4.	Tabella 1 Contesto Elaborazione Dati

Di seguito riportiamo le tabelle da utilizzare per la determinazione del punteggio della valutazione 1:

Tabella 1 – Natura e contesto dei dati		Punteggio
Dati Identificativi/ Personali	Esempio Dati Identificativi: Data di nascita, Stato di famiglia, Studi, Lavoro, Stipendio, Inquadramento Esempio Dati Personali: Nome del cittadino, Numero di Telefono, Indirizzo, email, ID card, Fotografia	
	Punteggio Base: quando la violazione riguarda "dati identificativi/personali" e il Titolare non è a conoscenza di alcun fattore aggravante.	1
	Il punteggio potrebbe essere umentato di 1 , ad esempio quando il volume di "dati identificativi/personali" e/o le caratteristiche del Titolare sono tali da consentire l'abilitazione di determinati profili o possono essere formulate assunzioni sullo stato sociale/finanziario dell'individuo.	2
	Il punteggio potrebbe essere umentato di 2 , ad esempio quando i "dati identificativi/personali" e/o le caratteristiche del Titolare possono portare a supposizioni sullo stato di salute dell'individuo, sulle preferenze sessuali, sulle convinzioni politiche o religiose.	3

Tabella 1 – Natura e contesto dei dati		Punteggio
	Il punteggio potrebbe essere umentato di 3 , ad esempio quando a causa di determinate caratteristiche dell'individuo (ad es. gruppi vulnerabili, minori), l'informazione può essere critica per la sicurezza personale o per le condizioni fisiche / psicologiche.	4
Dati Comportamentali	Esempio: Abitudini, preferenze personali e interessi, vita sociale e contatti	
	Punteggio Base: quando la violazione comporta "dati comportamentali" e il controllore non è a conoscenza di fattori aggravanti o di diminuzione.	2
	Il punteggio potrebbe essere diminuito di 1 , ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni comportamentali dell'individuo o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	1
	Il punteggio può essere umentato di 1 , ad esempio quando il volume di "dati comportamentali" e / o le caratteristiche del controllore sono tali da consentire la creazione di un profilo dell'individuo, esponendo informazioni dettagliate sulla sua vita quotidiana e sulle sue abitudini.	3
	Il punteggio può essere umentato di 2 , ad esempio se è possibile creare un profilo basato sui dati di una persona (es. cittadini).	4
Dati Finanziari	Esempio: IBAN, Numero di conto, Saldo conto, Transaction History, Informazione di base sulla carta di credito (senza CVC), Complete informazioni sulla carta di credito (con CVC), Dati sui mutui/prestiti	
	Punteggio Base: quando la violazione riguarda "dati finanziari" e il responsabile del trattamento non è a conoscenza di fattori aggravanti o di diminuzione.	3
	Il punteggio potrebbe essere diminuito di 2 , ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni finanziarie dell'individuo (ad esempio, il fatto che una persona sia il cliente di una determinata banca senza ulteriori dettagli).	1
	Il punteggio potrebbe essere diminuito di 1 , ad esempio quando il set di dati specifici include alcune informazioni finanziarie ma non fornisce ancora informazioni significative sullo stato / sulla situazione finanziaria dell'individuo (ad esempio: i numeri di conti bancari semplici senza ulteriori dettagli).	2
	Il punteggio potrebbe essere umentato di 1 , ad esempio quando a causa della natura e / o del volume dell'insieme di dati specifici, vengono divulgate informazioni complete finanziarie (ad esempio: informazioni complete sulla carta di credito con il codice cvc)	4
Dati Sensibili/Particolari	Esempio: Dati Sanitari, origine etnica, Orientamento politico e religioso, Orientamenti sessuali, Procedimento penale / condanna, Dati biometrici, Dati genetici	
	Punteggio Base: quando la violazione riguarda "dati sensibili" e il controllore non è a conoscenza di alcun fattore di diminuzione.	4

Tabella 1 – Natura e contesto dei dati		Punteggio
	Il punteggio potrebbe essere diminuito di 3 , ad esempio quando la natura del set di dati non fornisce alcuna comprensione sostanziale delle informazioni sui dati sensibili o i dati possono essere raccolti facilmente (indipendentemente dalla violazione) attraverso fonti disponibili pubblicamente (ad esempio la combinazione di informazioni da ricerche web).	1
	Il punteggio potrebbe essere diminuito di 2 , ad esempio quando la natura dei dati può portare a ipotesi generali.	2
	Il punteggio potrebbe essere diminuito di 1 , ad esempio quando la natura dei dati può portare a supposizioni su informazioni sensibili.	3

Si specifica che l'elenco dei tipi di dati descritti nelle quattro categorie non è esaustivo; tuttavia, la maggior parte dei dati coinvolti in casi reali può essere abbinata ad almeno una delle categorie.

La definizione dell'indicatore per la natura e contesto dei dati violati è il punteggio più alto raggiunto. Se i dati corrispondono a più di una categoria, è necessario seguire i passaggi sopra indicati per ogni categoria applicabile e in questi casi il valore da prendere in considerazione è il punteggio della categoria a cui è stato attribuito il valore più alto. Esempio:

- se la violazione riguarda "dati identificativi/personali" e il Titolare non è a conoscenza di alcun fattore aggravante, il punteggio da attribuire è 1;
- se la violazione riguarda anche dati comportamentali" e il Titolare non è a conoscenza di fattori aggravanti o di diminuzione, il punteggio è 2;

Pertanto, ai fini del calcolo del punteggio per la natura e contesto dei dati violati (VALUTAZIONE 1), occorre prendere in considerazione il valore 2.

Definizione del punteggio per la facilità di identificazione (Valutazione 2)

Il punteggio della 2^a valutazione (*di seguito anche "pt.2"*) è il fattore di correzione della Valutazione 1 che tiene in considerazione la facilità di identificazione dell'individuo in base ai dati violati.

Nella tabella seguente sono riassunte le attività inerenti alla **valutazione 2**:

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
4	RPD	Valutare la facilità di identificazione dell'individuo e determinare il pt.2	Valuta la facilità di identificazione dell'individuo ed attribuisce un punteggio secondo la tabella 2 definita dalla metodologia secondo i seguenti quattro livelli: <ul style="list-style-type: none"> • trascurabile (0,25); • limitato (0,5); • significativo (0,75); • massimo (1). Il fattore di correzione pt.2 può essere 0,25 / 0,5/ 0,75 o 1.	Tabella 2 Facilità di identificazione

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
			<p>Il punteggio più basso viene attribuito quando la possibilità di identificare l'individuo è trascurabile, il che significa che è estremamente difficile abbinare i dati a una determinata persona, ma comunque potrebbe essere possibile con determinate condizioni.</p> <p>Al contrario, il punteggio più alto viene attribuito quando l'identificazione è possibile direttamente dai dati violati, senza alcuna ricerca specifica per determinare l'identità dell'individuo.</p>	
5	RPD	Correggere il valore identificato in fase 1 moltiplicando con il fattore di valutazione 2	Una volta individuato il fattore di correzione, esso viene moltiplicato per il valore 1, al fine di determinare il punteggio iniziale della gravità della violazione dei dati.	Tabella 2 Facilità di identificazione

Di seguito riportiamo le tabelle da utilizzare per la valutazione del secondo valore (valutazione 2):

Tabella 2 - Facilità di identificazione		Punteggio	Livello
Descrizioni (a titolo esemplificativo)	Definizione: Facilità con cui possono essere identificati gli interessati (FI)		
	L'aggressione riguarda dati identificativi o dati personali non direttamente identificabili (ad esempio: nome/cognome molto diffuso in un paese)	0,25	Trascurabile
	L'aggressione riguarda i dati identificativi di un individuo ma non facilmente identificabile (ad esempio: nome/cognome condiviso da poche persone in un intero paese)	0,5	Limitata
	L'aggressione riguarda dati identificativi e rivela ulteriori informazioni di identificazione dell'individuazione (ad esempio: nome completo con l'indicazione dell'indirizzo email di questa persona)	0,75	Significativo
	L'aggressione riguarda dati identificativi o dati personali direttamente identificativi (ad esempio: nome completo con l'indicazione della data di nascita e l'indirizzo email di questa persona)	1	Massimo

La definizione del punteggio per la facilità di identificazione (Valutazione 2) è il punteggio più alto raggiunto. Se i dati corrispondono a più di una categoria, è necessario prendere in considerazione il punteggio della categoria a cui è stato attribuito il valore più alto.

Definizione del punteggio per le Circostanze della violazione (Valutazione 3)

Il punteggio della valutazione 3 quantifica le **circostanze specifiche della violazione** che possono essere presenti o meno in una particolare situazione.

Nella tabella seguente sono riassunte le attività inerenti alla **Valutazione 3**:

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
6	RPD	Quantificare le circostanze specifiche della violazione	<p>Attribuisce il punteggio relativo alle circostanze della violazione classificate secondo le seguenti macro categorie:</p> <ul style="list-style-type: none"> • violazione di riservatezza; • violazione di disponibilità; • violazione di integrità dei dati; • eventuali intenzioni malevole. <p>Le circostanze possono avere solo un'influenza aggiuntiva sulla gravità di una violazione.</p> <p>Il pt.3 può incrementare il punteggio iniziale delle gravità di 0,25 o 0,5 a seconda dei casi.</p>	Tabella 3

Di seguito riportiamo la tabella da utilizzare per la valutazione del terzo punteggio (di seguito "pt.3"):

Tabella 3 - Circostanze della violazione		Punteggio
Violazione di riservatezza	<p>Definizione: La perdita di riservatezza si verifica quando le informazioni sono accessibili da parti che non sono autorizzate o che non hanno uno scopo legittimo di accedervi. L'entità della perdita di riservatezza varia a seconda della portata della divulgazione, ovvero il numero potenziale e il tipo di parti che possono avere accesso illecito all'informazione.</p>	
	<p>Esempi di dati esposti a rischi di riservatezza senza prove che l'elaborazione illegale si è verificata:</p> <ul style="list-style-type: none"> - Un file cartaceo o un laptop si perde durante il transito; - L'attrezzatura è stata smaltita senza distruzione dei dati personali. 	0
	<p>Esempi di dati trasmessi verso un certo numero di destinatari conosciuti:</p> <ul style="list-style-type: none"> - Un'e-mail con dati personali è stata inviata erroneamente a un certo numero di destinatari conosciuti; - Alcuni soggetti esterni (es. cittadini, rappresentanti legali di un ente) possono accedere agli account di altri in un servizio online. 	0,25

Tabella 3 - Circostanze della violazione		Punteggio
	<p>Esempi di dati trasmessi verso un certo numero di destinatari sconosciuti:</p> <ul style="list-style-type: none"> - I dati sono pubblicati su una bacheca internet; - I dati vengono caricati su un sito P2P; - Un dipendente vende un CD ROM con i dati del cittadino; - Un sito Web configurato in modo errato rende accessibili pubblicamente i dati Internet dagli utenti interni. 	0,5
Violazione di integrità	<p>Definizione: La perdita di integrità si verifica quando le informazioni originali vengono alterate e la sostituzione dei dati può essere pregiudizievole per l'individuo. La situazione più grave si verifica quando esistono gravi possibilità che i dati modificati siano stati utilizzati in un modo che potrebbe danneggiare l'individuo.</p>	
	<p>Esempi di dati modificati ma senza alcun uso errato o illegale identificato:</p> <ul style="list-style-type: none"> - Le registrazioni di un database con dati personali sono state erroneamente aggiornate ma è stata effettuata una copia dell'originale prima del verificarsi della modifica. 	0
	<p>Esempi di dati modificati ed eventualmente usati in modo errato o illegale ma con possibilità di recupero:</p> <ul style="list-style-type: none"> - Un dato necessario per la fornitura di un servizio online è stato modificato e l'individuo deve richiedere il servizio in modalità offline. - È stato modificato un dato importante per l'accuratezza del file di un individuo in un servizio medico online. 	0,25
	<p>Esempi di dati modificati ed eventualmente usati in modo errato o illegale senza possibilità di recupero:</p> <ul style="list-style-type: none"> - Valgono gli esempi precedenti con l'aggravante che i dati originali non possono essere recuperati. 	0,5
Violazione di disponibilità	<p>Definizione: La perdita di disponibilità si verifica quando non è possibile accedere ai dati originali quando ce n'è bisogno. Può essere temporaneo (i dati sono recuperabili ma richiederà un periodo di tempo e questo può essere dannoso per l'individuo) o permanente (i dati non possono essere recuperati).</p>	
	<p>Esempi di dati che possono essere recuperati senza difficoltà:</p> <ul style="list-style-type: none"> - Una copia del file è persa ma sono disponibili altre copie. - Un database è danneggiato ma può essere facilmente ricostruito da altri database. 	0
	<p>Esempi di indisponibilità temporale:</p> <ul style="list-style-type: none"> - Un database è corrotto ma può essere ricostruito da altri database, sebbene sia richiesta qualche elaborazione. - Un file è perso ma l'informazione può essere fornita di nuovo dall'individuo 	0,25
	<p>Esempi di indisponibilità totale (i dati non possono essere recuperati dal controllore o dai singoli):</p> <ul style="list-style-type: none"> - Un file è perso / database danneggiato, non c'è il backup di queste informazioni e non può essere fornito dall'individuo. 	0,5
Intenzioni malevole	<p>Definizione: La violazione è dovuta a un'azione intenzionale malevola, ad esempio al fine di causare problemi al Titolare o danneggiare gli interessati.</p>	

Tabella 3 - Circostanze della violazione		Punteggio
	Esempi di violazione dovuta a un'azione intenzionale: - Un dipendente condivide intenzionalmente dati privati dai cittadini in un sito pubblico di social media. - Un dipendente vende dati privati dei cittadini a una società. - Un membro di un social network invia intenzionalmente delle informazioni sugli altri membri ai propri familiari al fine di danneggiarli.	0,5

La definizione del punteggio per le Circostanze della violazione (Valutazione 3) è data dalla somma dei punteggi ottenuti per ciascuna tipologia di circostanza.

Esempio: se è stato quantificato un punteggio di 0,5 per la violazione di riservatezza, di 0,5 per la violazione di integrità, di 0,5 per la violazione di disponibilità, di 0,5 per la violazione di intenzioni malevole, il punteggio da tenere in conto per le Circostanza della violazione (Valutazione 3) è 2.

Calcolo della gravità (Valutazione 4)

Il punteggio finale mostra il livello di gravità di una determinata violazione, tenendo conto dell'impatto sui diritti e libertà delle persone fisiche.

Nella tabella seguente sono riassunte le attività inerenti alla **fase di Calcolo della gravità (CG)**:

ID	Ruolo/Incaricato	Attività	Descrizione Attività	Strumenti
7	Privacy Team / RPD	Procedere al Calcolo della Gravità = pt.1* pt.2 + pt.3	Calcola la gravità della violazione applicando la formula definita dalla metodologia	Formula
8	RPD	Definire il livello di gravità della violazione	Definisce il livello di gravità (basso, medio, alto e molto alto) secondo il risultato finale della valutazione. Il risultato viene classificato secondo quattro livelli di gravità: <ul style="list-style-type: none"> • Basso (punteggio finale è inferiore a 2) • Medio (punteggio finale è tra 2 e 3) • Alto (punteggio finale è tra 3 e 4) • Molto alto (punteggio finale è superiore a 4) 	Tabella livello gravità della violazione

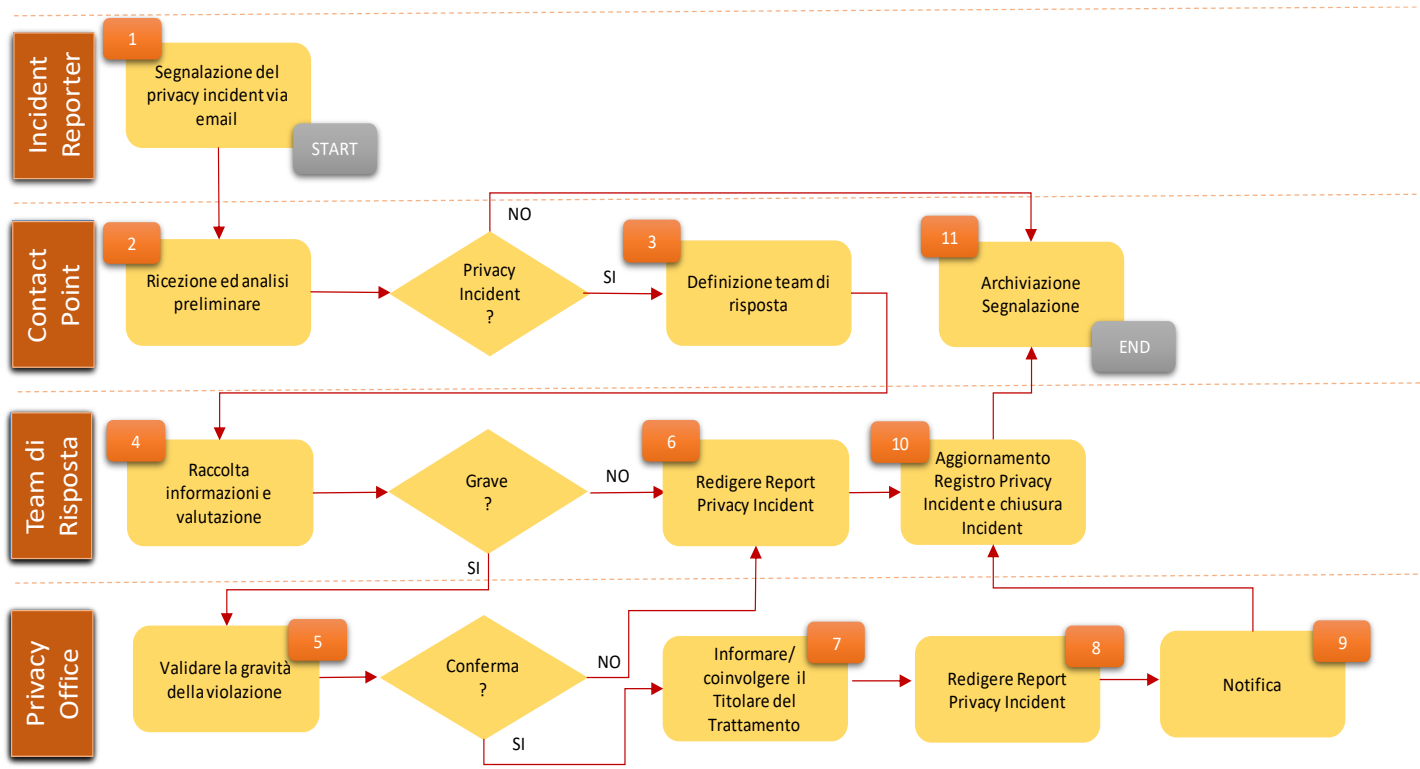
Di seguito riportiamo le tabelle da utilizzare **per la valutazione del livello di gravità**:

Punteggio	Livello	Descrizione	Esito valutazione
Gravità < 2	Basso	Gli individui non saranno interessati dalla violazione o potrebbero incontrare alcuni inconvenienti, che supereranno senza alcun problema (tempo trascorso a reinserire informazioni, fastidi, etc.).	Non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma l'incidente deve essere annotato all'interno del registro delle violazioni.

$2 \leq \text{Gravità} < 3$	Medio	Gli individui possono incontrare notevoli disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi dell'ente, paura, mancanza di comprensione, stress, disturbi fisici minori, etc.).	Non è necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, ma devono essere adottate ulteriori misure organizzative e tecniche al fine di migliorare la sicurezza dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni.
$3 \leq \text{Gravità} < 4$	Alto	Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, lista nera da parte delle banche, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, etc.).	È necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali e deve essere annotato l'incidente all'interno del registro delle violazioni.
$\text{Gravità} \geq 4$	Molto Alto	Gli individui possono incontrare conseguenze significative, o addirittura irreversibili, che non possono superare (difficoltà finanziarie come debito sostanziale o incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, etc.).	È necessario notificare il data breach all'Autorità Garante per la protezione dei dati personali, darne comunicazione ai soggetti interessati e annotare l'incidente all'interno del registro delle violazioni.

ISTRUZIONI OPERATIVE PER IL DATA BREACH MANAGEMENT

Il processo di data breach management avviene secondo il seguente flusso di attività:



LEGENDA

