GDPRLab PRO

Guida Operativa

Sezione: Registro Data Breach

Campo	Valore
Piattaforma	GDPRLab
Sezione	Registro Data Breach
Destinatari	Consulenti tecnici / DPO / Rivenditori
Versione guida	1.0

1. Cos’è la sezione Registro Data Breach

La sezione Registro Data Breach consente di registrare, gestire e tracciare gli incidenti di sicurezza che comportano – o che potrebbero comportare – una violazione dei dati personali (data breach), in adempimento agli obblighi previsti dagli artt. 33 e 34 del GDPR.

Il GDPR impone al Titolare del Trattamento di documentare internamente tutte le violazioni dei dati personali, indipendentemente dall’obbligo di notifica all’Autorità Garante.

La piattaforma supporta l’intero ciclo di gestione dell’incidente: dalla rilevazione alla notifica, fino alle azioni correttive.

Si accede cliccando su **Registro Data Breach** nel menu laterale sinistro.

2. Struttura della pagina principale

La pagina è composta da quattro aree:

→ Card KPI Totale Incidenti (rossa) – numero totale di incidenti registrati (con indicazione “Nella lista filtrata”)

→ Grafico Incidenti per Gravità (donut chart a sinistra)

→ Grafico Incidenti per Tipo (grafico a barre a destra)

→ Sezione Lista Incidenti con filtri di ricerca e lista degli incidenti registrati

3. Grafici di riepilogo

Grafico	Cosa mostra
Incidenti per Gravità (donut)	Distribuzione degli incidenti per livello di gravità (es. Bassa, Media, Alta, Critica). Si popola con i dati degli incidenti registrati.
Incidenti per Tipo (barre)	Distribuzione degli incidenti per categoria tipologica (es. accesso non autorizzato, perdita dati, ransomware, ecc.). Si popola con i dati degli incidenti registrati.

Quando non sono presenti incidenti entrambi i grafici mostrano “Nessun dato”.

4

4. Filtri della Lista Incidenti

Filtro	Opzioni / Descrizione
Cerca	Campo testo: ricerca per ID o descrizione dell’incidente
Stato	Menu a tendina: Tutti / Aperto / In gestione / Chiuso / ecc.
Gravità	Menu a tendina: Tutte / Bassa / Media / Alta / Critica
Tipo	Menu a tendina: Tutti / categorie di incidente disponibili

Quando non sono presenti incidenti la lista mostra “Nessun incidente registrato” con il pulsante **+ Apertura Incidente**.

5

5. Form “Apertura Incidente”

Cliccando su **+ Apertura Incidente** si apre il form di registrazione dell’incidente, strutturato in sei sezioni numerate.

Sezione 1 – Identificazione Incidente

Campo	Obbligatorio	Contenuto atteso / Note
Data e Ora di Rilevamento	Sì ★	Data e ora esatta in cui l’incidente è stato rilevato (precompilata con data/ora corrente, modificabile)
Rilevato da	Sì ★	Persona o sistema che ha rilevato l’incidente (es. nome dipendente, sistema di monitoraggio, antivirus)
Origine dell’Incidente	No	Menu a tendina – da dove proviene l’incidente. Può essere aggiunto successivamente durante l’investigazione
Tipo di Incidente	Sì ★	Menu a tendina – categoria dell’incidente (es. accesso non autorizzato, perdita dati, attacco ransomware, furto dispositivo, ecc.)
Gravità dell’Incidente	Sì ★	Menu a tendina – livello di gravità stimato (es. Bassa, Media, Alta, Critica)
Descrizione Sintetica dell’Incidente	Sì ★	Campo testo libero: descrizione sintetica e chiara di cosa è accaduto

> ***Nota operativa:*** *La Data e Ora di Rilevamento è precompilata con il momento corrente ma è modificabile: inserire l’ora effettiva in cui l’incidente è stato scoperto, non quella di apertura del form. Questa informazione è determinante per il calcolo dei termini di notifica al Garante (72 ore dalla conoscenza).*

Sezione 2 – Dettagli Incidente

Campo	Obbligatorio	Contenuto atteso / Note
Impatto dell'Incidente	No	Testo libero: numero di utenti/clienti coinvolti, servizi interrotti, eventuali danni economici o reputazionali
Asset o Sistemi Coinvolti	No	Elenco degli asset/sistemi interessati, uno per riga (es. SRV-EXCH-01, EP-F00F237B5339). Inserire server, endpoint, account utente, servizi o altri asset coinvolti
Probabile Causa	No	Menu a tendina – causa probabile dell'incidente (es. errore umano, attacco esterno, malfunzionamento tecnico, ecc.)
Tempo di Risoluzione (minuti)	No	Tempo totale dalla rilevazione alla risoluzione completa, espresso in minuti (es. 180)

> ***Nota operativa:*** *Il campo Asset o Sistemi Coinvolti accetta un asset per riga. Usare i codici identificativi degli asset così come sono stati censiti nella sezione Asset Management per garantire la tracciabilità incrociata.*

Sezione 3 – Azioni di Risposta Intraprese

Campo	Obbligatorio	Contenuto atteso / Note
Azioni di Risposta	No	Testo libero: descrizione dettagliata di tutte le azioni intraprese per contenere e gestire l'incidente (es. isolamento del sistema, reset credenziali, notifica agli interessati, coinvolgimento del team IT, ecc.)

Sezione 4 – Notifica alle Autorità Competenti

Campo	Obbligatorio	Contenuto atteso / Note
Data Notifica	No	Data e ora in cui è stata inviata la notifica all'Autorità Garante (da compilare solo se è stato necessario notificare)
Tipo Notifica	No	Menu a tendina – tipologia di notifica effettuata. Valore predefinito: Nessuna

> **Scadenza critica: Il GDPR (art. 33) impone la notifica al Garante entro 72 ore dalla conoscenza del data breach, quando quest'ultimo può presentare un rischio per i diritti e le libertà delle persone fisiche. Se la notifica non viene effettuata entro il termine, è necessario documentare i motivi del ritardo. Aprire l'incidente il prima possibile per avviare il conteggio delle 72 ore.**

Sezione 5 – Valutazione Post-Incidente

Campo	Obbligatorio	Contenuto atteso / Note
Valutazione Post-Incidente	No	Testo libero: valutazione completa dell'incidente dopo la risoluzione. Includere: cause radice identificate, impatto effettivo, lezioni apprese, valutazione dell'adeguatezza delle misure di sicurezza esistenti

Sezione 6 – Azioni Correttive e Preventive

Campo	Obbligatorio	Contenuto atteso / Note
Azioni Correttive e Preventive	No	Testo libero: azioni adottate o pianificate per evitare il ripetersi dell'incidente (es. aggiornamento software, formazione del personale, revisione delle policy di accesso, implementazione di nuovi controlli di sicurezza)
Stato	No	Menu a tendina – stato corrente dell'incidente. Valore predefinito: Aperto. Opzioni tipiche: Aperto / In gestione / Chiuso

> ***Nota operativa:*** *Il campo Stato permette di tracciare il ciclo di vita dell'incidente. Aggiornarlo man mano che l'incidente viene gestito: Aperto (appena rilevato) → In gestione (in corso di risoluzione) → Chiuso (risolto e documentato). Un incidente non deve mai rimanere nello stato Aperto dopo la risoluzione.*

6

6. Salvataggio

In fondo al form sono presenti due pulsanti:

→ **Salva** – salva l'incidente con tutti i dati inseriti e lo aggiunge alla Lista Incidenti

→ **Annulla** – chiude il form senza salvare

> ***Nota operativa:*** *Non è necessario compilare tutti i campi per salvare un incidente: in fase di apertura urgente è sufficiente compilare i campi obbligatori (Data/Ora, Rilevato da, Tipo, Gravità, Descrizione sintetica) e salvare. I dettagli possono essere integrati in seguito modificando l'incidente.*

7

7. Riferimento normativo: artt. 33 e 34 GDPR

Obbligo	Articolo	Termine	Destinatario
Notifica all'Autorità Garante	Art. 33 GDPR	Entro 72 ore dalla conoscenza del breach (se rischio per diritti e libertà)	Garante per la protezione dei dati personali (Italia: Garante Privacy)
Comunicazione agli Interessati	Art. 34 GDPR	Senza ingiustificato ritardo (se rischio elevato per diritti e libertà)	Persone fisiche i cui dati sono stati compromessi
Documentazione interna	Art. 33, par. 5	Sempre – indipendentemente dall'obbligo di notifica	Registro interno del Titolare

> **Attenzione: La documentazione interna è obbligatoria per TUTTI i data breach, anche quelli che non richiedono notifica al Garante (es. perché il rischio è improbabile). Il Registro Data Breach di GDPRLab assolve a questo obbligo. Non limitarsi a registrare solo gli incidenti gravi.**

8. Workflow consigliato in caso di incidente

→ Appena rilevato l'incidente: aprire immediatamente il form (+ Apertura Incidente) e salvare con i dati minimi obbligatori

→ Avviare il conteggio delle 72 ore dalla data/ora di rilevamento inserita

→ Completare la Sezione 2 (Dettagli) man mano che l'investigazione procede

→ Compilare la Sezione 3 (Azioni di risposta) con tutte le misure adottate

→ Valutare se il breach richiede notifica al Garante (art. 33) e/o comunicazione agli interessati (art. 34)

→ Se richiesta, effettuare la notifica al Garante e compilare la Sezione 4 con data e tipo di notifica

→ A risoluzione completata: compilare Sezione 5 (Valutazione post-incidente) e Sezione 6 (Azioni correttive)

→ Aggiornare lo Stato a Chiuso

Scadenza critica: Le 72 ore si contano dalla "conoscenza" del breach, non dal momento in cui viene aperto il form. In caso di incidente rilevato in un momento non lavorativo, il termine decorre comunque. Aprire il form appena possibile e documentare la data/ora effettiva di rilevamento.

9. Relazioni con altre sezioni

Sezione	Relazione con il Registro Data Breach
Asset Management	I codici degli asset coinvolti nell'incidente corrispondono agli asset censiti in Asset Management
Sicurezza informatica	Le misure di sicurezza configurate (firewall, backup, logging) sono il riferimento per valutare l'adeguatezza delle protezioni al momento del breach
Trattamenti	I trattamenti coinvolti nel breach devono essere identificati per valutare l'impatto sugli interessati
DPIA	Un data breach grave su un trattamento ad alto rischio può richiedere o influenzare la DPIA correlata
Repository	I report degli incidenti possono essere salvati nel repository per conservazione certificata