Procedura di gestione delle violazioni di dati personali (Data Breach)

REV E DATA	CREATION	REVIEW	APPROVAL	Changes from the previous edition
Rev. 01 del 13/10/2025	Unità Prevenzione della Corruzione, Trasparenza e Privacy	Joint Lab per la Cybersecurity, DPO	Unità Prevenzione della Corruzione, Trasparenza e Privacy con determina n. 13./25 del 13 ottobre 2025	Allineamento con la Procedura di gestione degli incidenti di sicurezza e ai Provvedimenti del Garante Privacy; integrazione dell'Introduzione; inserimento delle "Definizioni" e degli "Attori principali"; aggiornamento dei riferimenti normativi.
Rev. 00 del 13/02/2019	Unità Prevenzione della Corruzione, Trasparenza e Privacy	Servizio IT	Unità Prevenzione della Corruzione, Trasparenza e Privacy con determina n. 04/19 del 13 febbraio 2019	Adozione.

1. PREMESSA

La Fondazione Bruno Kessler (di seguito anche “FBK” o “la Fondazione”) riconosce l'importanza fondamentale di gestire con efficacia gli imprevisti che possono minacciare la sicurezza delle informazioni. Questo impegno è essenziale per salvaguardare la confidenzialità e l'integrità delle risorse informative, oltre a garantire la disponibilità e la continuità operativa dei sistemi e servizi. Inoltre, si pone l'obiettivo di proteggere la reputazione aziendale e conformarsi agli obblighi legali e normativi.

Una Procedura di Gestione degli Incidenti relativi alla Sicurezza delle Informazioni (documento riservato) è stata adottata per affrontare in modo mirato gli eventi che comportano la compromissione della sicurezza delle informazioni, stabilendo chiaramente ruoli, responsabilità e azioni da intraprendere. Tale procedura si estende a individui, sistemi informatici e dati aziendali, coinvolgendo tutti coloro che hanno accesso a tali sistemi o dati in qualsiasi contesto, deve essere seguita internamente ed è direttamente collegata alla presente procedura.

2. DEFINIZIONI

Principio di Riservatezza delle Informazioni: garantisce che le informazioni siano accessibili solo a coloro che hanno il diritto di conoscerle. Le informazioni riservate non dovrebbero essere divulgate o rese disponibili a entità o individui non autorizzati.

Principio di Integrità delle Informazioni: assicura che le informazioni siano accurate, complete e non siano soggette a manipolazioni. Le informazioni devono essere protette da modifiche non autorizzate che potrebbero compromettere la loro affidabilità e precisione.

Principio di Disponibilità delle Informazioni: garantisce che le informazioni siano accessibili e utilizzabili quando necessario da parte di persone autorizzate. Le informazioni devono essere protette da eventi che potrebbero causare interruzioni indesiderate o impedire l'accesso, quando richiesto.

Incidente di Sicurezza delle Informazioni: evento che potenzialmente minaccia la sicurezza delle informazioni, compromettendo uno o più tra i principi di riservatezza, integrità e disponibilità. Questa definizione include situazioni in cui l'evento impedisce il rispetto degli obblighi legali, esponendo l'organizzazione al rischio di sanzioni o richieste di risarcimento.

Violazione di dati personali: ogni infrazione alla sicurezza degli stessi che comporti - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dalla Fondazione. Esistono tre tipologie di violazioni di dati personali:

- **Violazione della Riservatezza**: in caso di divulgazione o di accesso non autorizzato o accidentale ai dati personali. Per esempio, l’accesso non autorizzato ai sistemi informatici che contengono banche dati con informazioni di pazienti/dipendenti.
- **Violazione dell’Integrità**: in caso di modifica non autorizzata o accidentale di dati personali. Per esempio, l’alterazione di banche dati senza autorizzazione rilasciata dal relativo “owner”.
- **Violazione della Disponibilità**: in caso di perdita accidentale o non autorizzata dell’accesso ai dati personali, o loro distruzione. Per esempio, perdita o furto di documenti cartacei contenenti dati del personale dipendente.

3. RIFERIMENTI NORMATIVI

- Regolamento UE 2016/679 in materia di protezione dei dati personali (GDPR)[1];
- Linee guida WP250 sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679[2];

[1] https://eur-lex.europa.eu/legal-content/IT-EN/TXT/?uri=CELEX:32016R0679&from=IT
[2] https://ec.europa.eu/newsroom/article29/items/612052

- Provvedimento dell'Autorità Garante n. 157 del 30 luglio 2019 - sulla notifica di violazioni di dati personali (data breach)[3]
- Linee guida EDPB 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali[4];
- Provvedimento dell'Autorità Garante n. 209 del 27 maggio 2021 - Procedura telematica per la notifica di violazioni di dati personali (data breach)[5]
- Linee guida EDPB 9/2022 sulla notifica di Data Breach[6];
- Regolamento Privacy FBK[7]
- Procedura di Gestione degli Incidenti relativi alla Sicurezza delle Informazioni (riservato).

4. SCOPO E DESTINATARI

La presente procedura definisce gli attori, i compiti e le modalità di gestione delle violazioni di sicurezza delle informazioni di carattere personale (Data Breach) e delle conseguenti azioni che la Fondazione deve avviare e completare.

La procedura è rivolta a tutti i soggetti[8] interni ed esterni - come classificati nel Regolamento Privacy - che a qualsiasi titolo trattano dati personali per conto della Fondazione.

5. PRINCIPALI ATTORI E COMPITI RELATIVI ALLA PRESENTE PROCEDURA

Soggetti interni: hanno la responsabilità di segnalare tempestivamente qualsiasi anomalia o malfunzionamento riguardante dispositivi informatici, sistemi, rete o qualsiasi perdita, furto o danneggiamento delle informazioni trattate nell'ambito delle attività. In particolare, in caso di perdita o trattamento/divulgazione non autorizzati di dati personali, gli utenti sono tenuti a segnalare immediatamente l'incidente seguendo la presente procedura.

Soggetti esterni: devono segnalare tempestivamente qualsiasi incidente che abbia un impatto sul trattamento dei dati personali di FBK; collaborano con FBK e seguono le sue istruzioni in merito a tali incidenti, al fine di consentire a FBK di svolgere un'indagine approfondita sull'incidente, formulare una risposta corretta e adottare ulteriori misure adeguate in relazione all'incidente. In caso di violazione dei dati personali, l'utente esterno segnala tempestivamente qualsiasi violazione (reale o potenziale) che potrebbe ragionevolmente coinvolgere i dati personali trattati per conto di FBK in qualità di titolare del trattamento.

Team di Gestione degli Incidenti: raccoglie e valuta tutte le informazioni utili all'analisi dell'incidente; valuta, insieme al/la DPO l'incidente segnalato; fornisce consulenza sulle possibili misure da adottare per ridurre al minimo gli effetti della violazione dei dati e per prevenire il ripetersi dell'incidente; raccoglie le segnalazioni degli utenti e monitora gli eventi di sicurezza

---

[3] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126951
[4]https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012021-examples-regarding-personal-data-breach_en
[5] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9667201
[6]https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en
[7]https://trasparenza.fbk.eu/Disposizioni-generali/Atti-generali/Atti-amministrativi-generali/Linee-Guida-e-Regolamenti/Regolamento-Privacy
[8] **Soggetti interni**: componenti degli Organi statutari e degli altri organismi; personale dipendente, personale collaboratore coordinato e continuativo, personale in somministrazione, personale presente in FBK a fronte di accordi di distacco o di un comando, personale dipendente provinciale messo a disposizione di FBK, consulenti e lavoratori/trici autonomi/e occasionali, risorse affiliate (Alti profili, Affiliated fellows, Visiting fellows, PhD students, Scholars, High School fellows).
Soggetti esterni/Responsabili del Trattamento nominati da FBK ai sensi dell'art. 28 del GDPR: imprese fornitrici di beni, servizi o lavori che operino con la Fondazione, indipendentemente dal rapporto giuridico sottostante, ed il loro personale dipendente e collaboratore, personale di altre entità presente in FBK in forza di convenzioni o accordi inter-istituzionali, visitatori/trici e ospiti di vario genere.

dall'infrastruttura IT e ne condivide i report con l'Unità Privacy per discutere insieme le potenziali misure da adottare in futuro.

Unità Prevenzione della Corruzione, Trasparenza e Privacy (nel documento anche **"Unità Privacy"**): raccoglie i report degli incidenti e delle violazioni di dati personali; analizza e gestisce le questioni legate alla protezione dei dati personali ed i conseguenti adempimenti legali; contribuisce a preservare la riservatezza, la disponibilità e l'integrità dei dati personali, garantendo al contempo chiarezza e totale aderenza agli standard di privacy stabiliti.

Data Protection Officer (nel documento anche **"DPO"**): raccoglie e valuta tutte le informazioni rilevanti per l'analisi degli incidenti e l'identificazione delle violazioni dei dati; indaga insieme al Team di Gestione degli Incidenti sull'incidente segnalato per valutare se sono coinvolti dati personali; fornisce consulenza sulle possibili misure da adottare per prevenire il ripetersi dell'incidente e ridurre al minimo gli effetti della violazione dei dati; raccoglie le segnalazioni e monitora le violazioni dei dati personali verificatesi e le condivide con l'Unità Privacy al fine di discutere insieme le potenziali misure future da adottare; coordina la predisposizione della notifica all'Autorità Garante; contribuisce alla comunicazione da inviare agli interessati; funge da punto di contatto tra FBK in qualità di Titolare del trattamento, gli interessati e l'Autorità Garante, facilitando la comunicazione e la conformità al GDPR.

Amministratore di Sistema: fornisce tutte le informazioni necessarie sull'incidente; garantisce la riservatezza, la disponibilità e l'integrità delle informazioni coinvolte nell'incidente; in stretta collaborazione con il Team di Gestione degli Incidenti, l'Unità Privacy e il/la DPO, affronta la violazione della sicurezza logica o fisica, riducendone al minimo l'impatto e bloccandone gli effetti.

Responsabile Interno/a del Trattamento: è responsabile del trattamento dei dati personali riconducibili al relativo ambito di competenza, quindi anche di eventuali violazioni dei dati personali che coinvolgono la sua articolazione organizzativa; fornisce tutte le informazioni necessarie relative all'incidente; contribuisce alla preparazione della notifica all'Autorità Garante; contribuisce alla comunicazione da inviare agli interessati.

6. PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

La presente procedura di gestione delle violazioni di dati personali si compone di cinque fasi:

1. raccolta della notifica dell'incidente;
2. valutazione;
3. mitigazione;
4. comunicazioni;
5. registrazione e monitoraggio.

6.1 Raccolta della notifica dell'incidente

Ai sensi della *Procedura FBK di gestione degli incidenti di sicurezza*, **tutti i soggetti interni** hanno la responsabilità di segnalare tempestivamente qualsiasi anomalia o malfunzionamento riguardante dispositivi informatici, sistemi, rete o eventuali perdite, furti o danneggiamenti di informazioni trattate nelle attività lavorative. La modalità per effettuare tali segnalazioni nel dettaglio prevede:

- per anomalie, funzionamenti o malfunzionamenti di dispositivi informatici, sistemi e rete di contattare il Servizio Soluzioni Digitali e Infrastrutture IT tramite i canali designati, quali il sistema di ticketing del Supporto IT (help-it@fbk.eu) o il numero interno (111);
- per furti e danneggiamenti di informazioni di contattare il Joint Lab per la Cybersecurity (help-cyber@fbk.eu), con in copia il /la DPO (privacy@fbk.eu) ed l'Organismo di Vigilanza (odv@fbk.eu);

- per furti di dispositivi di contattare il Servizio Soluzioni Digitali e Infrastrutture IT (help-it@fbk.eu), con in copia il /la DPO (privacy@fbk.eu) e il Servizio Patrimonio (logistica@fbk.eu);
- per condizioni di pericolo e dispositivi di sicurezza di contattare il/la RSPP (sicurezza@fbk.eu), e il Servizio Patrimonio (logistica@fbk.eu);
- **per eventi o incidenti che possa configurare una violazione di dati personali (Data Breach)** di segnalarli tempestivamente alla DPO e al Team di Gestione degli Incidenti fornendo una breve descrizione dell'evento/incidente segnalato attraverso uno dei seguenti canali:
  - modulo di segnalazione;
  - e-mail a privacy@fbk.eu, con in copia help-cyber@fbk.eu;
  - telefonata a +39.0461.314.370;

Il soggetto interno che rileva la violazione deve altresì informare, per le vie brevi, il/la suo/a diretto Responsabile (Responsabile Interno/a del Trattamento).

Il soggetto esterno (es: Responsabile del Trattamento) che venga a conoscenza di un incidente deve notificare FBK via email privacy@fbk.eu fornendo una descrizione della natura dell'incidente, indicando, ove possibile, le categorie e il numero approssimativo degli interessati coinvolti; il nominativo e i dati di contatto della struttura competente in materia di protezione dei dati personali o di un altro punto di contatto al quale fare riferimento per ottenere ulteriori informazioni; una descrizione delle probabili conseguenze dell'incidente e una descrizione delle misure adottate o che si propone di adottare per affrontare l'incidente, comprese, se del caso, le misure per mitigarne i possibili effetti negativi. La notifica deve essere effettuata non appena l'utente esterno viene a conoscenza della violazione dei dati personali e comunque entro 48 ore dal verificarsi della violazione stessa.

Il/la DPO, in collaborazione con il Team di Gestione degli Incidenti, attiva quindi l'Amministratore di Sistema di riferimento al fine di gestire con urgenza la violazione di sicurezza logica o fisica, minimizzandone l'impatto e bloccandone gli effetti.

6.2 Valutazione

Il/la DPO e il Team di Gestione degli Incidenti procedono con una prima valutazione del fatto segnalato per definire se siano coinvolti dati personali. Durante l'analisi, il/la Responsabile Interno/a del Trattamento e/o l'Amministratore di Sistema devono collaborare e fornire tutte le necessarie informazioni sull'incidente.

Qualora l'ipotesi di Data Breach fosse confermata, i soggetti di cui sopra ne valutano l'impatto sui diritti degli interessati, basando la loro valutazione anche sulle informazioni presenti nel Registro dei trattamenti e (qualora disponibile) sulla Valutazione d'Impatto sulla Protezione dei Dati.

6.3 Mitigazione

Il/la DPO e il Team di Gestione degli Incidenti, verificate le misure adottate per la minimizzazione degli effetti del Data Breach, programmano ulteriori nuove misure necessarie a prevenire il ripetersi dell'incidente/della violazione di dati personali. L'Amministratore di Sistema e l'Unità Privacy devono essere informati e direttamente coinvolti nell'implementazione delle misure programmate.

6.4 Comunicazioni

Una volta valutato l'impatto del Data Breach il/la DPO stabilisce:

a. se sia necessario notificare la violazione all'Autorità Garante;

b. se sia necessario comunicare la violazione agli Interessati.

Gli obblighi di notifica all'Autorità Garante scaturiscono dal superamento di una soglia di rischio basso, mentre l'obbligo di comunicazione agli Interessati scaturisce a partire da un rischio alto.

Per la notifica all'Autorità Garante, il/la DPO seguirà la procedura[9] stabilita dall'Autorità Garante e utilizzerà i modelli in essa presenti, mentre il/la Responsabile Interno/a del Trattamento fornirà tutte le informazioni ed il supporto necessario. La notifica formale dovrà essere inviata da FBK, quale Titolare del Trattamento, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza della violazione di dati personali.

Nel fornire consulenza sulla comunicazione agli Interessati, il/la DPO verrà supportato/a dal/la Responsabile Interno/a del Trattamento. E' responsabilità di FBK, quale Titolare del Trattamento, informare gli interessati senza ingiustificato ritardo.

Nei casi in cui la Fondazione non sia il Titolare del trattamento dei dati personali oggetto della violazione, il/la DPO invierà tempestivamente al Titolare interessato la valutazione interna di cui al punto 6.2.

6.5 Registrazione e monitoraggio

Indipendentemente dalla valutazione circa la necessità di procedere con le comunicazioni di cui al punto 6.4, ogni qualvolta si verifichi una violazione di dati personali, il/la DPO registra l'evento nell'apposito registro delle violazioni di dati personali.

Il/la DPO controllerà nel tempo l'evoluzione delle attività di risoluzione delle violazioni.

[9] https://servizi.gpdp.it/databreach/s/