FONDAZIONE
BRUNO KESSLER

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

Adottata con determina n. 04/2019 di data 13 febbraio 2019
del Responsabile dell'Unità Prevenzione della Corruzione, Trasparenza e Privacy

FONDAZIONE
BRUNO KESSLER

1. PREMESSA

Per “violazione di dati personali” si intende 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.

Le violazioni di dati personali possono darsi, a titolo esemplificativo, nei seguenti casi:

- accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite;
- pirateria informatica;
- alterazione o distruzione di banche dati senza autorizzazione rilasciata dal relativo “owner”;
- presenza di virus o altri attacchi al sistema informatico o alla rete aziendale;
- divulgazione di dati confidenziali a persone non autorizzate;
- infedeltà aziendale (ad esempio: data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico);
- invio di e-mail contenenti dati personali e/o particolari a erroneo destinatario;
- violazione delle misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- perdita o furto di dati o di strumenti nei quali i dati sono memorizzati;
- perdita o furto di documenti cartacei.

2. RIFERIMENTI NORMATIVI

- Regolamento UE 2016/679 in materia di protezione dei dati personali (GDPR);
- Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/679 (Linea Guida WP250);
- Regolamento Privacy della Fondazione Bruno Kessler.

3. SCOPO E DESTINATARI

La presente procedura definisce 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 - come classificati nel Regolamento Privacy (Capo I, art. 3) - che a qualsiasi titolo trattano dati personali per conto della Fondazione.

4. PROCEDURA DI GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

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

1. rilevazione;
2. valutazione;
3. mitigazione;
4. comunicazioni;
5. registrazione e monitoraggio.

FONDAZIONE
BRUNO KESSLER

4.1 Rilevazione

Ogni rilevazione di un evento o incidente di sicurezza che possa configurare una violazione di dati personali (Data Breach) deve essere tempestivamente notificata al Data Protection Officer (DPO) attraverso uno dei seguenti canali:

- modulo di segnalazione (esclusivamente per soggetti interni);
- e-mail a privacy@fbk.eu;
- telefonata a +39.0461.314.370;

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

Il DPO attiva quindi l'Amministratore di Sistema di riferimento e/o il Responsabile del Servizio IT, Infrastrutture e Patrimonio al fine di gestire con urgenza la violazione di sicurezza logica o fisica, minimizzandone l'impatto e bloccandone gli effetti.

4.2 Valutazione

Il DPO, l'Amministratore di Sistema ed il Responsabile Interno del Trattamento procedono con una prima valutazione del fatto segnalato.

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 sul Registro dei trattamenti e sulle Linee guida WP250.

4.3. Mitigazione

Il DPO e l'Amministratore di Sistema, verificate le misure adottate per la minimizzazione degli effetti del Data Breach, programmano ulteriori nuove misure necessarie a prevenire il ripetersi dell'evento.

4.4. Comunicazioni

Una volta valutato l'impatto del Data Breach il 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 DPO utilizzerà il modulo allegato alla presente procedura (Allegato 1).

Per la comunicazione agli Interessati il DPO verrà supportato dal Responsabile Interno del Trattamento.

Nei casi in cui la Fondazione non sia il Titolare del trattamento dei dati personali oggetto della violazione, il DPO invierà tempestivamente al Titolare interessato la valutazione interna di cui al punto 4.2.

4.5. Registrazione e monitoraggio

Indipendentemente dalla valutazione circa la necessità di procedere con le comunicazioni di cui al punto 4.4, ogni qualvolta si verifichi una violazione di dati personali, il DPO registra l'evento nell'apposito registro delle violazioni di dati personali.

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

FONDAZIONE BRUNO KESSLER

VIOLAZIONE DI DATI PERSONALI (DATA BREACH)

MODULO DI COMUNICAZIONE

ex art. 33 Reg. UE n. 2016/679

Titolare del trattamento

Denominazione o ragione sociale _____

Provincia _____ Comune _____

CAP _____ Indirizzo _____

Responsabile della struttura organizzative che ha subito la violazione _____

Persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Recapito telefonico per eventuali comunicazioni _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Responsabile della Protezione dei Dati Personali - DPO

Nominativo _____

Recapito telefonico per eventuali comunicazioni _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Responsabile del trattamento ex art. 28 Reg. UE n. 2016/679 (ove nominato)

Denominazione o ragione sociale _____

Provincia _____ Comune _____

CAP _____ Indirizzo _____

Responsabile della struttura organizzative che ha subito la violazione _____

Persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Recapito telefonico per eventuali comunicazioni _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

FONDAZIONE BRUNO KESSLER

DESCRIZIONE DELLA VIOLAZIONE

Quando si è verificata la violazione dei dati personali trattati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare, ad esempio, se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili, etc…)

_____

_____

Modalità di esposizione al rischio (Rischi che derivano dalla perdita di riservatezza, integrità o disponibilità)

1. Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del Titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi, ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del Titolare e non li detiene neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del Titolare e li detiene l'autore della violazione)
- ☐ Diffusione
- ☐ Comunicazione non autorizzata
- ☐ Attacco Hacker
- ☐ Altro (specificare) _____

2. Dispositivo oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ Archivio fisico
- ☐ Altro (specificare) _____

FONDAZIONE BRUNO KESSLER

3. Natura della violazione

☐ Accidentale

☐ Deliberata

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

_____

_____

_____

Quante persone fisiche (interessati) sono state colpite dalla violazione dei dati personali trattati?

☐ n. _____ persone fisiche

☐ Circa _____ persone fisiche

☐ Un numero (ancora) sconosciuto di persone fisiche

Che tipo di dati sono oggetto di violazione?

☐ Dati comuni (dati anagrafici, codice fiscale, altro)

☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)

☐ Dati relativi a minori

☐ Dati relativi all'ubicazione di persone fisiche

☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale

☐ Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale

☐ Dati relativi a condanne penali e reati

☐ Dati pseudo-anonimizzati

☐ Ancora sconosciuto

☐ Altro (specificare) _____

Livello di gravità della violazione dei dati personali per i diritti e le libertà dell'interessato

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

FONDAZIONE BRUNO KESSLER

PROBABILI CONSEGUENZE DELLA VIOLAZIONE DEI DATI PERSONALI

(es: furto d'identità, perdite finanziarie, danni all'immagine, danni alla reputazione, etc…)

_____

_____

MISURE TECNICHE E ORGANIZZATIVE

Misure tecniche e organizzative applicate ai dati oggetto di violazione:

_____

_____

_____

_____

Misure tecniche e organizzative adottate – successivamente al data breach – per contenere la violazione dei dati, attenuare i possibili effetti negativi e prevenire simili violazioni future:

_____

_____

COMUNICAZIONE AGLI INTERESSATI

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il _____

☐ No, perché _____

Contenuto della comunicazione resa agli interessati:

_____

_____

_____

_____