FONDAZIONE
BRUNO KESSLER

Data Breach Management Procedure

Adopted with resolution. No. 04 / 2019 dated February 13th, 2019
by the Corruption Prevention, Transparency and Privacy Unit

FONDAZIONE
BRUNO KESSLER

1. INTRODUCTION

By "personal data breach" it is meant any security violation that involves - accidentally or unlawfully – the destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed by the Foundation.

Data breaches may occur, by way of example, in the following cases:

- unauthorized access to ICT systems with disclosure of the information obtained;
- hacking;
- alteration or destruction of databases without authorization issued by the owner concerned;
- presence of viruses or other attacks on the computer system or company network;
- disclosure of confidential data to unauthorized individuals;
- corporate infidelity (for example: data breach caused by an internal person who, having access to the data, produces a copy that is distributed in a public environment);
- sending e-mails containing personal and/or particular data to unintended recipients;
- breach of physical security measures (for example: forcing doors or windows of security rooms or archives, containing confidential information);
- loss or theft of data or tools in which the data are stored;
- loss or theft of paper documents.

2. REGULATORY FRAMEWORK

- EU Regulation 2016/679 on the protection of personal data (GDPR);
- Guidelines on Personal data breach notification under Regulation 2016/679 (Guideline WP250);
- Privacy Regulations of the Bruno Kessler Foundation.

3. PURPOSE AND ADDRESSEES

This procedure defines the methods for handling security breaches of personal data and the consequent actions that the Foundation must implement and complete.

The procedure applies to all Users - as classified in the Privacy Regulations (Section I, Article 3) - who, in any capacity, process personal data on behalf of the Foundation.

4. DATA BREACH MANAGEMENT PROCEDURE

This procedure for addressing personal data breaches consists of five steps:

1. identification;
2. investigation;
3. mitigation;
4. communication;
5. reporting and monitoring.

FONDAZIONE
BRUNO KESSLER

4.1 Identification

Any security event or incident that might constitute a personal data breach must be promptly reported to the Data Protection Officer (DPO) via one of the following channels:

- notification form (for Internal Users only);
- e-mail to privacy@fbk.eu;
- call to +39.0461.314.370.

The User who becomes aware of the breach must notify, without delay, his/her immediate supervisor (Internal Data Processor).

The DPO shall then alert the System Administrator of reference and/or the Head of the IT, Infrastructure and Corporate Assets Service in order to promptly address the logical or physical security breach, minimizing its impact and blocking its effects.

4.2 Investigation

The DPO, the System Administrator and the Internal Data Processor shall proceed with an initial investigation on the incident reported.

If it is determined that a Data Breach has occurred, the above mentioned Users shall assess its impact on the rights of the data subjects affected, basing their assessment on the Record of Processing Activities and the Guidelines of the WP250.

4.3. Mitigation

The DPO and the System Administrator, after checking the measures taken to minimize the effects of the Data Breach, shall plan further measures to prevent the recurrence of the incident.

4.4. Communication

Once the impact of the Data Breach has been assessed, the DPO shall determine:

a. whether the Data Protection Authority should be notified of the breach;

b. whether the Data Subjects affected should be informed of the breach.

The Data Protection Authority must be notified whenever the incident is classified as other than Low Risk, while the obligation to communicate to the individuals affected arises when it has been determined that the risk is high.

For the purpose of notifying the Data Protection Authority, the DPO shall use the form attached to this procedure (Annex 1).

When informing the affected Data Subjects, the DPO shall receive the support of the Internal Data Processor.

In cases where the Foundation is not the Data Controller of the personal data on which the breach has occurred, the DPO shall promptly send the Data Controller concerned the internal investigation report referred to in point 4.2.

4.5. Reporting and monitoring

Regardless of the need to proceed with the notifications referred to in point 4.4, whenever a personal data breach has occurred, the DPO shall record the incident in the dedicated Record of Personal Data Breaches.

The DPO shall monitor the evolution of breach resolution actions over time.

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:

_____

_____

_____

_____