Data Breach Management Procedure

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	Information Security Incident Management Procedure alignment, “Introduction” integration, “Definitions” and “Main Actors” sessions inclusion, “Regulatory framework” update.
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	Adoption

1. INTRODUCTION

The Bruno Kessler Foundation (hereinafter also called “FBK” o “la Fondazione”) recognizes the critical importance of effectively managing contingencies that can threaten information security. This commitment is essential to safeguarding the confidentiality and integrity of information resources, as well as ensuring the availability and business continuity of systems and services. It also aims to protect corporate reputation and comply with legal and regulatory obligations.

An “Information Security Incident Management Procedure” (confidential document) has been adopted to purposefully address events involving information security compromise by clearly establishing roles, responsibilities and actions to be taken. It extends to individuals, information systems, and corporate data, involving everyone who has access to those systems or data in any context, must be followed internally and is directly connected to the present procedure.

2. DEFINITIONS

Principle of Confidentiality of Information: ensures that information is accessible only to those who have the right to know it. Confidential information should not be disclosed or made available to unauthorized individuals or entities.

Principle of Integrity of Information: ensures that information is accurate, complete, and not subject to manipulation. Information must be protected from unauthorized modification that could compromise its reliability and accuracy.

Principle of Availability of Information: ensures that information is accessible and usable when needed by authorized persons. Information must be protected from events that could cause unwanted interruptions or prevent access when required.

Information Security Incident: event that potentially threatens information security by compromising one or more of the principles of confidentiality, integrity and availability. This definition includes situations where the event prevents compliance with legal obligations, exposing the organization to the risk of penalties or claims.

Personal Data Breach: 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. There are three types of Personal Data Breaches:

- **Confidentiality breach**: where there is an unauthorised or accidental disclosure of, or access to personal data. For example: unauthorized access to ICT systems which include datasets with information about patients/employees.
- **Integrity breach**: where there is an unauthorised or accidental alteration of personal data. For example: the alteration of databases without authorization issued by the owner concerned.
- **Availability breach**: where there is an accidental or unauthorised loss of access to, or destruction of, personal data. For example the loss or theft of paper documents containing Human Resources files of employees.

3. REGULATORY FRAMEWORK

- EU Regulation 2016/679 on the protection of personal data (GDPR)[1];
- EDPB Guidelines on Personal data breach notification under Regulation 2016/679 (Guideline WP250)[2];
- Italian Data Protection Authority Provision 157/2019 on the data breach notifications[3];

[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
[3] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126951

- EDPB Guidelines 01/2021 on Examples regarding Personal Data Breach Notification[4];
- Italian Data Protection Authority Provision 209/2021 on the online procedure for data breach notifications[5];
- EDPB Guidelines 09/2022 on personal data breach notification under GDPR[6];
- FBK Privacy Regulations[7];
- FBK Information Security Incident Management Procedure (confidential).

4. PURPOSE AND ADDRESSEES

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

The procedure applies to all internal and external Users[8] - as classified in the Privacy Regulations - who, in any capacity, process personal data on behalf of the Foundation.

5. MAIN ACTORS AND DUTIES REGARDING THIS PROCEDURE

Internal Users: has the responsibility to promptly report any anomaly or malfunction concerning computer devices, systems, network or any loss, theft or damage of information handled in the activities. In particular, in case of loss or unauthorized processing/disclosure of personal data, users are obliged to report the incident immediately by following the present procedure.

External Users: must promptly report any incident that has an impact on the processing of FBK personal data; cooperates with and shall follow FBK instructions with regard to such incidents in order to enable FBK to perform a thorough investigation into the incident, to formulate a correct response, and to take suitable further steps in respect of the incident. In case of a Personal Data Breach, the External User promptly reports any violation (real or potential) that could reasonably involve personal data processed on behalf of FBK as Data Controller.

Incident Management Team: collects and evaluates all relevant information for incident analysis; investigates together with the DPO the reported incident; advices on possible measures to be taken to minimize the effects of the Data Breach and to prevent the recurrence of the incident; collects notifications and monitors security events from the IT infrastructure and shares the reports with the Privacy Unit in order to discuss together potential future measurements to be adopted.

Corruption Prevention, Transparency and Privacy Unit (also referred to in this procedure as **"Privacy Unit"**): collects reports about incidents and Personal Data Breaches; evaluates and manages data protection issues and connected legal obligations; helps preserving the confidentiality, availability and integrity of personal data while ensuring clarity and full adherence to established privacy standards.

Data Protection Officer (also referred to in this procedure as **"DPO"**): collects and evaluates all relevant information for incident analysis and data breaches identification; investigates together with the Incident Management Team the reported incident to assess whether personal data is involved; advices on possible measures to be taken to prevent the recurrence of the incident and

---

[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] **Internal Users:** members of the statutory bodies and other bodies; employees; in-house consultants; leased employees; Staff assigned to FBK premises; Province employees assigned to work at FBK premises; Occasional consultants; Affiliates (High profiles, Affiliated fellows, Visiting fellows, PhD students, Scholars, High School interns). **External Users/Data Processors appointed by FBK pursuant to art. 28 of the GDPR:** Staff, in any capacity, of contractors providing supplies, services, or works for FBK and their employees or collaborators; Staff of other organizations present at FBK due to MoUs or inter-institutional agreements; Various visitors and guests.

to minimize the effects of the Data Breach; collects reports and monitors occurred Personal Data Breaches and shares them with the Privacy Unit in order to discuss together potential future measurements to be adopted; coordinates the drafting of the notification to the Data Protection Authority; contributes to the communication to be sent to the Data Subjects; acts as a point of contact between FBK as Data Controller, Data Subjects, and the Data Protection Authority facilitating communication and compliance with the GDPR.

System Administrator: provides all the necessary information about the incident; ensures the confidentiality, availability and integrity of the information involved in the incident; in close collaboration with the Incident Management Team, the Privacy Unit and the DPO addresses the logical or physical security breach, minimizing its impact and blocking its effects.

Internal Data Processor: has the responsibility for the processing of personal data attributable to his/her relevant area of concern, therefore also for any Personal Data Breach involving his/her organizational articulation; provides all the necessary information about the incident; contributes to the drafting of the notification to the Data Protection Authority; contributes to the communication to be sent to the Data Subjects.

6. DATA BREACH MANAGEMENT PROCEDURE

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

1. collection of the incident notification;
2. assessment;
3. mitigation;
4. communication;
5. reporting and monitoring.

6.1 Collection of the incident notification

As part of the *FBK Security Incident Management Procedure*, **all Internal Users** are given the responsibility to promptly report any anomaly or malfunction concerning computer devices, systems, network or any loss, theft or damage of information handled in work activities. The detailed reporting arrangements shall include:

- for anomalies, operations or malfunctions of computer devices, systems and network, contact the Digital Solutions and IT Infrastructure Service via designated channels, such as the Ticket system of the Support (help-it@fbk.eu) or the internal number (111);
- for theft and damage of information contact the Joint Lab for the Cybersecurity (help-cyber@fbk.eu), with copy DPO (privacy@fbk.eu) and ODV (odv@fbk.eu);
- for device theft contact the the Digital Solutions and IT Infrastructure Service, with copy DPO (privacy@fbk.eu) and Corporate Assets Department (logistica@fbk.eu);
- for dangerous conditions and safety devices to contact the RSPP (sicurezza@fbk.eu) and the Corporate Assets Department (logistica@fbk.eu);
- **for security events or incidents that might constitute a personal data breach**, to promptly report them to the DPO and to the Incident Management Team providing a short description of the event/incident reported, via one of the following channels:
  - notification form;
  - e-mail to privacy@fbk.eu with copy help-cyber@fbk.eu;
  - call to +39.0461.314.370.

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

The External User (i.e. Data Processors) who becomes aware of the incident must promptly notify FBK via email privacy@fbk.eu providing a description of the nature of the incident, including where possible the categories and approximate number of data subjects concerned; the name and contact details of its data protection offices or another contact point where more information can be obtained; a description of the likely consequences of the incident; and a description of the measures taken or proposed to be taken to address the incident including, where appropriate, measures to mitigate its possible adverse effects. The notification should be done as soon as the External User becomes aware of the Personal Data Breach, and not later than 48 hours after the occurrence of the Personal Data Breach.

The DPO, in collaboration with the Incident Management Team, shall then alert the System Administrator of reference in order to promptly address the logical or physical security breach, minimizing its impact and blocking its effects.

6.2 Assessment

The DPO and the Incident Management Team shall proceed with an initial investigation on the incident reported to analyse whether personal data is involved. During this investigation, the Internal Data Processor and/or the System Administrator must cooperate by providing all the necessary information about the incident.

If it is determined that a Data Breach has occurred, the above mentioned actors shall assess its impact on the rights of the data subjects affected, basing their assessment also on the Data Registry registrations and (if available) on the Data Protection Impact Assessments.

6.3 Mitigation

The DPO and the Incident Management Team, after checking the measures taken to minimize the effects of the Data Breach, shall plan further measures to prevent the recurrence of the incident/Data Breach. The System Administrator and the Privacy Unit must be informed and directly involved in the implementation of the planned measures.

6.4 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 follow the Data Protection Authority procedure[9] and shall use the templates therein provided, whereas the Internal Data Processor shall provide any information and support needed. The official notification must be sent by FBK as Data Controller without undue delay and, where feasible, not later than 72 hours after having become aware of the Personal Data Breach.

When advising on how and when to inform the affected Data Subjects, the DPO shall receive the support of the Internal Data Processor. It is the responsibility of FBK as Data Controller to actually inform the affected Data Subjects without undue delay.

In cases where FBK 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 6.2.

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

6.5 Reporting and monitoring

Regardless of the need to proceed with the notifications referred to in point 6.4, 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.