

TEMPLATE Content of the Notification of Cases of Personal Data Breach

A personal data breach refers to any type of incident which could result in a breach of confidentiality, integrity or accessibility of personal data. In more detail, a personal data breach can be described as unlawful destruction, loss, alteration, unauthorized provision or unauthorized access to personal data. Such cases also include **unintentional** as well as **intentional** personal data breaches. Common examples of personal data breach may include:

- Access to personal data provided to a non-authorized person
- Sending of personal data to a wrong addressee
- Loss or theft of equipment containing personal data
- Loss of accessibility of personal data
- Unauthorized alteration of personal data

Process of response to a breach

1. **Detection and filing** – A detected case of a personal data breach is, subsequently, included in the filing system of incidents led kept by the data protection officer.
 - a) Activities of the ITC – detection of attacks, results of penetration tests
 - b) Notification by an ordinary employee, student or any other natural person who detects a personal data breach (loss of equipment containing personal data), incorrect configuration of a system in use or a failure to protect paper documents containing personal data, etc.)
 - c) Notification based on a detection made by automated tools and aimed to detect such cases (automated network monitoring, automated monitoring of the personal data traffic in an all-cloud environment).
 - d) Notification received from the personal data processor – in addition to the aforementioned actions, legal actions arising from a contract concluded with the processor of personal data may be carried out.

Following the notification of a security incident to the central place (data protection officer), the said incident shall be included in the central filing system. Subsequently, an investigation of the incident should be conducted, which shall give answers to the following fundamental questions:

- What was the source of, the cause for a personal data breach?
 - Which personal data and natural persons were concerned by this breach?
2. **Categorization** – Assessment of a case of a personal data breach in order to identify the likely impact on the natural persons concerned.
 3. **Notification of cases of personal data breach** to the relevant entities – to the supervisory authority or to the natural persons concerned.
 - a) In the event that a personal data breach is unlikely to result in a risk to the rights and freedoms of particular natural persons, TBU is not obliged to notify this fact to anybody. The grounds for the failure to notify this fact must be recorded in the central place.
 - b) In the event that a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, TBU shall notify the personal data breach to the supervisory authority.
 - c) In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of concerned natural persons, TBU shall notify this fact to the natural persons concerned, and that also if the said natural person is likely to have been concerned. In the event that TBU has not the contact details of the above-mentioned natural persons, it may

issue a public announcement regarding the given case of a personal data breach.

- d) In the event of a notification of the incident to the supervisory authority or to the natural persons concerned, TBU shall provide the following data:
- Description of the type of the personal data breach – description of categories of data subjects concerned by the breach, estimated number of these natural persons and categories thereof and the number of concerned records on the minimum processing of personal data.
 - Name and contact details of the data protection officer.
 - Description of likely consequences of a personal data breach.
 - Description of planned or adopted measures including provisional measures aimed at minimizing the impact which would affect the person concerned adversely.
4. **Recovery** – An attempt to remedy the consequences arising from the given personal data breach.
5. **Guidance** – Adoption of appropriate measures aimed at preventing similar cases of a personal data breach. It is necessary to examine each occurrence of a personal data in order to reveal the source of such a breach. The goal is to enable the subsequent adoption of appropriate technological and organizational measures in such a manner as to eliminate the occurrence of such breaches. The result of the review and the subsequent proposed organizational measures shall be recorded in the central place. The data protection officer shall give his/her opinion on each case of this type and, in accordance with this opinion, further steps shall be taken such as the implementation of the measures proposed, the tightening or relaxing of the said measures.