INFORMATION ON DATA CONTROLL AND DATA PROTECTION

CREDITFORTE KFT.

Dr Gábor Saly
Managing Director

INTRODUCTION

This Notification Guide on Personal Data Breach ("Guide") enters into force on the effective date of the General Data Protection Regulation (GDPR) of the European Union. The Regulation mandates the notification of the supervisory authority in the event of a personal data breach (or the lead supervisory authority in the case of cross-border breaches), and in certain cases, also the notification of data subjects affected by the breach.

The general purpose of this Guide is to enable Creditforte Kft. (the Company) to identify personal data breaches and assess whether the breach falls within the scope of mandatory notification, and whether it is necessary to report it to the authorities and to inform the data subjects.

For further information on data breaches affecting IT systems and infrastructures, please refer to the Information Security Policy.

Scope of the Guide

This Guide applies in the event of a personal data breach. Questions related to the identification of incidents are addressed in the Information Security Policy (see the chapter titled "Incident Management").

What Constitutes a Personal Data Breach

Under the GDPR, a personal data breach is a breach of security leading to the unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that is transmitted, stored, or otherwise processed.

The following description categorizes the general types of data breaches:

Category	Typical Activity	Note
Breach of Confidentiality	Accidental, unlawful, or unauthorized disclosure of or access to personal data	Personal data is received or accessed by individuals who are not authorized to receive or access it.
Breach of Integrity	Accidental or unlawful alteration of personal data (e.g., modification)	"Alteration" refers to the modification of personal data.
Breach of Availability	Accidental or unlawful loss or destruction of personal data	"Destruction" means that the personal data no longer exists or is incomplete. "Loss" means that the personal data can no longer be processed or accessed, although it still exists.

A personal data breach can only be discussed after a security incident has occurred. However, not all security incidents constitute a personal data breach. It is only considered a personal data breach if the incident affects personal data. A data breach subject to the notification obligation under the GDPR may also affect individuals who are not the direct subjects of the breach.

Examples:

- Unauthorized access by a third party (e.g., an IT service provider who was not authorized by the Company to process personal data gains access to the debtor/employee database)
- Loss or theft of devices containing personal data (e.g., an employee loses a USB drive containing personal data)
- Loss of availability of personal data (e.g., in the event of a cyberattack, the personal data of employees is stolen)

Notification in the Event of a Data Breach

Supervisory Authority: This may include the lead supervisory authority, such as the data protection authority competent for each processor in the respective EU member state, as well as the data subjects. The supervisory authority must be notified if the data breach poses a risk to the rights and freedoms of natural persons. Data subjects must be notified if the breach poses a high risk to their rights and freedoms. The specific form and method of notification to the supervisory authority are determined by national legislation.

The supervisory authority must be notified properly and without undue delay, and no later than 72 hours after the Company becomes aware of the data breach. Data subjects must be notified without undue delay.

Security Incident
Did the security incident result in the destruction, loss, alteration, unauthorized disclosure of, or access to personal data?

Data Breach
Does the data breach pose a risk to the rights and freedoms of natural persons?

Notification of the Supervisory Authority
Does the data breach pose a high risk to the rights and freedoms of natural persons?

Notification of the Data Subject
The notification to be sent to the data subject is included as Annex 2 of this Guide.

Notification Obligation in the Event of a Personal Data Breach

Both the data controller and the data processor are subject to notification obligations in the event of a personal data breach. However, the GDPR distinguishes between the scope of their respective responsibilities. If a personal data breach occurs, the data controller is responsible for notifying the supervisory authority and, in certain cases, the data subjects, while the data processor is only required to notify the data controller. The data controller may, however, enter into an agreement with the data processor, authorizing the latter to fulfill the notification obligation on behalf of the controller.

To determine the nature of the notification obligation, each data breach must be assessed to establish:

- Whether the Company is acting as a **data controller** or **data processor** with respect to the affected data.
- Whether any additional steps have been taken in relation to the data breach notification.

To assess whether a personal data breach identified by the Company falls under the scope of mandatory notification, the risk posed by the breach must be evaluated.

The assessment process is similar to a **Data Protection Impact Assessment (DPIA)**. However, while a DPIA is conducted before a data breach occurs, the assessment described in this Guide is carried out **after** the breach has taken place.
When assessing whether the data breach poses a **risk or a high risk** to the rights and freedoms of individuals, the following factors must be considered:

- The type of data breach
- The sensitivity of the personal data involved
- The purpose of the data and the number of data subjects affected
- The degree of identifiability of individuals
- The severity of the potential consequences for individuals
- Any specific characteristics of the individuals involved

The Company designates a responsible party to ensure compliance with the data breach notification obligation: the **Data Protection Officer (DPO)**. Any employees who become aware of a potential breach must report it to the DPO if they suspect a security incident has occurred.

Exceptions to the Notification Obligation
The GDPR provides certain exceptions: notification is not required if the breach is **unlikely** to pose a risk to the rights and freedoms of natural persons.

The Company as Data Controller
When acting as a data controller and engaging a processor for data processing, the agreements between the Company and the processor must ensure that the processor adequately guarantees compliance with the data breach notification requirements. Since in practice, processors often become aware of breaches first, such agreements must ensure that the Company can fulfill its own notification obligations. Specifically, the processor must be required to inform the Company **promptly** of any data breach and any developments. The Company may agree that the processor will notify the **supervisory authority** and/or **data subjects** on its behalf. However, in such cases, the processor must notify the Company of every notification it sends to the authority/data subjects, and also inform the Company whenever it decides **not** to notify based on its risk assessment.

Accountability Principle and Documentation
The data controller is required to maintain **internal records** of all personal data breaches. These records must include:

- The date the breach was discovered
- A detailed description of the breach and its effects
- Remedial actions taken by the Company

The Company appoints a **Data Protection Officer** responsible for maintaining and updating these records.

Actions in the Event of a Personal Data Breach

1. Appoint a data breach response team
2. Launch an investigation
3. Assess the risk
4. Determine the notification obligation: whether notification is required, and if so, to whom
5. Notify the supervisory authority and, if necessary, the data subject(s)
6. Implement remedial measures
7. Notify the supervisory authority and data subjects of any updates (if applicable)
8. Record the data breach

Penalties for Failure to Notify

Failure to comply with the personal data breach notification obligation may result in **administrative fines** imposed by the supervisory authority. These may reach up to **EUR 10,000,000** or **2% of the total worldwide annual turnover** of the preceding financial year, whichever is higher.
Additionally, if the authority identifies a **lack of appropriate security measures**, or the **inadequacy** of existing measures, it may impose further sanctions for **failing to notify** and for **insufficient security**, as these represent separate violations.

DATA BREACH FLOWCHARTS

Notification by the Data Processor (without delay)

1. The processor determines that a personal data breach has occurred
2. The processor notifies the data controller

Notification by the Data Controller

1. A security incident is identified, and it is assessed whether a personal data breach occurred
2. Does the breach pose a **risk** to the rights and freedoms of natural persons?
   a. No
   b. Yes → Notify within 72 hours, if possible
3. If yes: notify the **supervisory authority**, or the **lead supervisory authority** if the breach affects individuals in multiple member states
4. Does the breach pose a **high risk** to the rights and freedoms of natural persons?
   a. No
   b. Yes
5. If yes: notify the **data subjects**

NOTIFICATION OF THE SUPERVISORY AUTHORITY BY THE DATA CONTROLLER

Aspect	Requirement	Note
Category of Data Breach	- Personal data breach likely to pose a risk to the rights and freedoms of natural persons	- e.g.,loss of a security element involving personal data - No notification is required if the data breach is *"unlikely to result in a risk"*, e.g., the personal data is already publicly available and its disclosure does not pose a risk to the individual.
Notification Timeframe	- Without undue delay - Where feasible, no later than 72 hours after becoming aware of the data breach. If notification within 72 hours is not possible, the reasons for the delay must be provided along with the notification. If all information cannot be provided at the same time, it may be supplied in phases, without further undue delay	- "Becoming aware" means that the Company is certain a security incident has occurred that compromises personal data. - Justification for delay: for example, if the data controller must handle multiple similar breaches affecting a large number of data subjects in a short period of time. - Agreements with data processors must include a provision requiring the processor to notify the

		Company in the event of a data breach. These agreements may also authorize the processor to send the notification on behalf of the controller. - Agreements with other controllers (e.g., in joint controllership arrangements) must specify whether the Company or another controller is responsible for complying with the notification obligation—or for any failure to comply.
Form of Notification	- In accordance with legal requirements	- According to legal requirements - To comply with the accountability principle, the notification must be provided in written or electronic form, ensuring that compliance with the notification obligation can be demonstrated.
Content of Notification	- Description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected - Name and contact details of the Data Protection Officer - Description of the likely consequences of the personal data breach - Description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects	- The GDPR specifies the minimum content required for a notification - It is recommended to assess which additional information about the data breach may be relevant from the supervisory authority's perspective - After a follow-up investigation, the Company must inform the supervisory authority; it is the Company's responsibility to determine whether the security incident has been contained and whether or not a personal data breach actually occurred
Other Requirements	- The controller must document any personal data breach, summarizing the facts relating to the breach, its effects, and the remedial actions taken.	- The controller must enable the supervisory authority to verify compliance with the GDPR requirements (in line with the accountability principle).

NOTIFICATION TO THE DATA CONTROLLER BY THE DATA PROCESSOR

Aspect	Requirement	Note
Category of Data Breach	-Personal data breach	-All personal data breaches must be reported to the data controller – it is the controller's responsibility to assess whether the breach is likely to pose a risk to the rights and freedoms of natural persons.
Notification Timeframe	-Without undue delay after identifying the data breach - -If it is not possible to provide all information at the same time, it may be provided in phases, without further undue delay	-The timeframe for this obligation must be defined in the agreement with the data controller (e.g., in a data processing agreement or a personal data protection clause) -It must be acknowledged that the data controller has 72 hours to notify the supervisory authority of the breach -The processor must immediately inform the controller of any additional information about the data breach as it becomes available in subsequent phases
Form of Notification	-Not specified by the GDPR	-To comply with the accountability principle, the notification should be made in written or electronic form so that compliance with the notification obligation can be demonstrated.
Content of Notification	-Description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects affected, as well as the categories and approximate number of personal data records concerned -Description of the likely consequences of the personal data breach -Description of the measures taken or proposed to be taken to address the personal data breach	-Based on the notification, the data controller must be able to fulfill its obligations related to the data breach.

CREDITFORTE Kft.
VAT No.: 14656257-2-43
Company No.: 01-09-345193
Seat: 1118 Budapest
Pannonhalmi Street 36-38.

CONTACT DATA:
Mailing address: 1506 Budapest Pf.74.
E-mail: info@creditforte.hu
Web: http://www.creditforte.hu
Data control identifier: 02807-0001

NOTIFICATION OF DATA SUBJECTS

Aspect	Requirement	Note