ED ZEMİN TEKNOLOJİLERİ A.Ş.

CRISIS RESPONSE PROCEDURE

TABLE OF CONTENTS

Purpose

Pursuant to Article 12(5) of the Personal Data Protection Law No. 6698 (Law), ED ZEMİN TEKNOLOJİLERİ A.Ş. (Company) is obliged to notify the relevant persons and the Personal Data Protection Board (Board) as soon as possible in the event that personal data being processed is obtained by others through unlawful means.

This Crisis Response Procedure (Procedure) has been prepared to inform employees about how to respond to a crisis and the steps to be taken in the event that personal data is obtained by others through unlawful means, i.e., in the event of a personal data breach.

Responsibility

All employees are responsible for the implementation of this Procedure. Employees acting contrary to this Procedure shall be subject to the provisions of the Disciplinary Regulation.

1. Personal Data Breach

A personal data breach occurs in situations such as unlawful acquisition of personal data, unlawful unauthorised access to personal data, accidental or intentional disclosure of personal data to unauthorised persons, and unlawful deletion, alteration or disruption of the integrity of personal data.

The following situations are generally considered to constitute a personal data breach:

- Theft or loss of physical documents or electronic devices containing personal data.
- Acquisition of individual usernames and passwords by unauthorised persons.
- Unlawful disclosure of confidential information.
- Accidental transmission or sending of emails containing personal data and/or confidential information to unrelated persons outside the company.
- Unlawful access to personal data through viruses or other attacks (e.g. cyberattacks) on IT equipment, systems and networks.

In the above-mentioned or similar situations, the procedure described in this Procedure must be followed.

2. Crisis Response Team

A Crisis Response Team (Team) shall be formed, consisting of participants designated from the following departments, to respond to crisis situations arising or potentially arising from a personal data breach and to fulfil the obligations stipulated under the Law:

- Data Controller Contact Person
- Senior Management of the Data Controller (General Manager)
- Manager of the Department Where the Breach Occurred

3. Crisis Response Process

Pursuant to Board Decision No. 2019/10 dated 24.01.2019 on "Procedures and Principles for Notification of Personal Data Breach", the Company is required to notify the Board without delay and within a maximum of 72 hours from the date it becomes aware of a personal data breach, and to notify the affected data subjects as soon as reasonably possible — directly if their contact address is available, or through the Company's own website or other appropriate methods if not.

To fulfil these obligations, certain steps must be followed within the Company in the event of a data breach:

- Preliminary assessment of the crisis.
- Conducting containment and recovery activities.
- Risk assessment.
- Notification.
- Evaluation and Improvement.

3.1. Preliminary Assessment of the Crisis

In the event of an actual or potential data breach within the Company, all relevant employees are obliged to notify the Data Controller Contact Person immediately and without delay. The relevant employee prepares and submits a report to the Data Controller Contact Person containing the following information:

- Date and time of the personal data breach.
- Date and time of detection of the personal data breach.
- Description of the personal data breach incident.
- Number of data subjects and records affected by the breach, if known.
- Description of steps taken and measures adopted at the time of detection of the breach, if any.
- Name, surname, contact information and date of the report of the employee(s) preparing the report.

The Data Controller Contact Person conducts a preliminary assessment taking into account the matters specified in the report. In conducting this assessment, considering whether a data breach has actually occurred, the scope and potential impacts of the breach, the Contact Person initiates a comprehensive investigation with the Team into the data breach.

3.2. Conducting Containment and Recovery Activities

Containment and recovery activities are conducted under the supervision of the Team to mitigate the effects of the data breach on the Company and the affected data subjects. Within this scope, the departments that need to be informed of the breach are first identified and these persons are provided guidance on the steps to be taken to control, prevent where possible, and minimise the damage from the breach.

Subsequently, an attempt is made to identify the data subjects and records that will be affected by the data breach and, where available, their contact information. Simultaneously, an assessment is made as to whether there are any other institutions or organisations that need to be notified of the data breach.

3.3. Risk Assessment

Personal data breaches may have many adverse effects on affected persons such as identity theft, restriction of rights, fraud, financial loss, reputational damage, loss of personal data security, and discrimination. Therefore, it is of utmost importance to carefully assess what kind of effects the potential consequences of the personal data breach may have on the Company and the affected persons, and to identify the risks.

When the Team assesses the risks, the nature, sensitivity and volume of the personal data affected, the number of individuals affected and the groups of data subjects, the impact of the breach on the Company's activities and reputation, the measures taken to mitigate the impact of the breach, and

the potential consequences of the breach should each be addressed separately. Based on the outcomes, the data breach is classified as "low level, medium level or high level risk":

- Low level risk: The breach does not cause any adverse effect on data subjects, or such effect is negligible.
- Medium level risk: The breach may cause adverse effects on data subjects but such effects are not significant.
- High level risk: The breach causes serious adverse effects on affected persons.

The Senior Management of the Data Controller is informed by the Team regarding data breaches classified as medium level and especially high level risk.

3.4. Notification

The data breach must be notified to third parties outside the Company both as a legal obligation and for purposes such as taking measures regarding the data breach and mitigating the potential effects of the breach.

3.4.1. Notification to the Board

The Data Controller Contact Person is obliged to notify the Board without delay and within a maximum of 72 hours from becoming aware of the personal data breach. Therefore, it is important for all employees within the Company to notify the Data Controller Contact Person of any data breach situation without delay, to prevent the Company from being subject to any sanction.

In the notification to the Board, the following information shall be included as a minimum:

- Nature of the personal data breach.
- Information on the categories and approximate number of data subjects affected by the breach.
- Information on the categories and approximate number of personal data records affected by the breach.
- Name and contact details of the Data Controller Contact Person.
- Likely consequences of the personal data breach.
- Measures taken or proposed to address the personal data breach.

3.4.2. Notification to Data Subjects

Following identification of the data subjects affected by the data breach, the Data Controller Contact Person notifies the affected data subjects through the most appropriate means (directly via their contact address if available, or through the Company's website or other means if not). The content of the notification shall include at minimum:

- Nature of the breach.
- Contact details of the Data Controller Contact Person.
- Likely consequences of the breach.
- Measures taken or proposed to address the breach.

3.5. Evaluation and Improvement

After the crisis response process is complete, the Team conducts a comprehensive review of the incident. This review aims to identify the root cause of the breach, assess the effectiveness of the response process, identify areas for improvement, and take measures to prevent recurrence. The findings of the review are documented and relevant updates are made to Company policies and procedures where necessary.

4. Related Policies and Procedures

- Policy on Protection and Processing of Personal Data
- Personal Data Retention and Disposal Policy
- Policy on Processing and Protection of Special Categories of Personal Data
- Information Systems General Standards and Security Policy

5. Update

This Procedure shall be reviewed and recorded once a year regardless of whether changes in its content are required due to corporate or legal reasons. The most current version shall be published on the Data Controller's website.