ED ZEMİN TEKNOLOJİLERİ A.Ş.

POLICY ON PROTECTION AND PROCESSING OF EMPLOYEE PERSONAL DATA

TABLE OF CONTENTS

I. Introduction

The Personal Data Protection Law No. 6698 (Law) introduces important regulations regarding the protection and lawful processing of personal data. The protection of personal data is among the priorities of ED ZEMİN TEKNOLOJİLERİ A.Ş. (Data Controller). Activities relating to the protection of personal data of the Data Controller's employees are managed under this "Policy on Protection and Processing of Personal Data" (Policy).

1. Purpose

This Policy sets out the rules that the Data Controller must comply with when processing the personal data of its employees. Therefore, the purpose of the Policy is to ensure that personal data is processed lawfully.

2. Scope

The primary addressee of this Policy is the Data Controller. The implementation of this Policy and the regulations set out herein concern the employees of the Data Controller. In addition to current employees whose employment relationship is ongoing, former employees whose personal data is still being processed and job applicants who have applied for a position with the Data Controller are also within the scope of this Policy. The term "employee" in this Policy shall encompass the Data Controller's employees, former employees and job applicants.

The units of the Data Controller responsible for the processing of employee personal data shall play the most significant role in implementing this Policy. Such units shall receive support from the Data Controller's senior management, the Data Controller Contact Person, or other responsible persons appointed for this purpose within the scope of implementing this Policy.

3. Relationship with Other Policies

This Policy governs the actions to be taken by the Data Controller regarding the processing of personal data of the Data Controller's employees. For matters not covered by this Policy, the provisions of the "Policy on Protection and Processing of Personal Data" regarding the processing of personal data shall apply.

4. Update

This Policy 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.

II. Collection of Personal Data During Recruitment

1. Steps to Be Followed in Job Advertisement and Application Processes

1.1. Specifying the Information of the Advertising Company

The Data Controller may initiate the recruitment process for open positions through job advertisements (via its website, employment or consultancy companies, or similar methods) or may evaluate CVs submitted to them.

The Data Controller takes care to process the personal data of candidates lawfully and to fulfil its obligation to inform.

Where the Data Controller initiates the recruitment process through an employment or consultancy company, measures are taken to ensure that how personal data collected by private employment platforms/agencies or consultancy companies will be used and shared is specified.

1.2. Consistency of Collected Personal Data with the Recruitment Process

The Data Controller informs candidates about the purpose for which the collected personal data is being collected, in order to fulfil its obligation to inform data subjects. Where the collected personal data is intended to be used or shared for a different position or purpose other than the position applied for by the candidate, such use and sharing purposes are clearly stated.

Questions asked and forms prepared to collect personal data during the recruitment process are evaluated for each type of open position, and measures are taken to prevent unnecessary collection of personal data (for example, questions may be asked about candidates' name, surname, address, date of birth, email address, work experience and education). Certain personal data collected from employees may not be requested before the candidate's employment is approved (for example, bank account details).

Depending on the nature of the position applied for, more extensive personal data processing may be required. However, such personal data must be appropriate to the nature of the job. Personal data required by the nature of the job must be valid only for the relevant position.

1.3. Processing of Special Categories of Personal Data

Data relating to job applicants' race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, physical appearance, membership of associations, foundations or trade unions, health, sexual life, criminal conviction, and biometric and genetic data constitute special categories of personal data.

The Data Controller may not discriminate on the basis of special categories of personal data in making recruitment decisions, nor process special categories of personal data during the recruitment process for such purposes, except where required by law or by the nature of the job.

Where processing of special categories of personal data is required due to the nature of the job or a legal requirement, only special categories of personal data that fall within this scope may be processed, as limitedly as possible. In such cases, the candidate is informed of the reason for requesting the special categories of personal data and the purpose of use, through the application form or a separate explanatory note.

Where the special categories of personal data to be requested can be collected from the candidate at a later stage, such data may not be requested at the first stage of the recruitment process.

1.4. Steps to Be Followed During Interviews

The Data Controller may conduct interviews with candidates via video conference, telephone or in person. The Data Controller informs the employees conducting the interview about how the personal data collected during the interview will be recorded and retained.

If the relevant candidate wishes to exercise their statutory rights regarding personal data recorded by the interviewers during the interview, such request is responded to by the Data Controller within a maximum of 30 days. The Data Controller informs employees who will conduct interviews about this matter and takes necessary measures for the exercise of statutory rights that may be asserted by candidates.

2. Steps to Be Followed in Pre-Employment Checks or Controls

2.1. Verification of Personal Data Provided by Candidates and Conducting Additional Research

During the recruitment process, the accuracy of personal data submitted by candidates may be verified from other sources by the Data Controller. Such verification is carried out only for the purpose of confirming the accuracy of personal data submitted by the candidate.

Where the Data Controller verifies the accuracy of personal data submitted by the candidate, the candidate is informed about this matter (regarding the personal data to be verified, the verification method and sources to be used) and explicit consent is obtained where required. Furthermore, where there is a discrepancy between the information obtained from verification and the personal data submitted, the candidate is given an opportunity to explain the situation.

In certain special circumstances, the Data Controller may also actively conduct research to obtain additional information about a candidate. It is preferred to obtain the desired information from the candidate directly, to the extent possible, rather than conducting research.

In research conducted about a candidate, lawful methods are chosen. Where the personal data to be investigated cannot be obtained, a more reasonable alternative is sought to achieve the same objective (for example, verifying the authenticity of a candidate's educational diploma).

III. Processing of Employee Data

The Data Controller may process employee personal data for the following types of processes:

- During the establishment, performance and termination of the employment contract.
- For compliance with statutory obligations.
- For performance evaluation and career development activities.
- For benefit and compensation management.
- For communication, training and development activities.
- For occupational health and safety compliance.
- For use of third-party service provider services.

Personal data shall not be collected in excess of the processing purpose. The lawful basis for processing must be identified before any processing takes place. Where explicit consent is required, it must be obtained before processing commences.

IV. Data Relating to Employee Health

The Data Controller may collect employee health data through medical examinations and tests under an occupational health and safety programme. The purposes of such examinations and tests are determined in advance. Less intrusive methods are preferred where possible (for example, health surveys rather than reviewing examination results). The Data Controller may not collect biometric or genetic samples from employees covertly. Activities based on legal grounds constitute an exception.

V. Purposes of Processing Employee Data

The Data Controller collects and processes employee personal data for the following purposes:

- Supporting the processes of determining and monitoring performance evaluation criteria for employees.
- Supporting the processes of planning and monitoring benefits and perquisites provided to employees.
- Supporting the Data Controller in the planning and execution of payroll management and bonus processes.
- Supporting strategic human resources planning, succession planning and organisational development activities.
- Implementing appointment, promotion and departure decisions of senior managers and making related announcements.
- Supporting the determination of remuneration and bonus packages for senior managers.
- Supporting the planning and execution of employee engagement measurement processes.
- Supporting the planning and execution of career development, training and talent management activities for employees.
- Supporting recruitment processes.
- Performing corporate and partnership law transactions.
- Supporting compliance with applicable legislation.
- Conducting activities for protecting Group reputation, sustainability and social responsibility.
- Organising events across the Data Controller.
- Conducting audit activities to ensure the Data Controller's activities are carried out in accordance with other Data Controller policies and applicable legislation.
- Conducting communication and correspondence activities for employees; managing employee satisfaction and engagement processes.

The Data Controller shall make the required notifications under the Law and applicable legislation for the processing of employee personal data for the above-mentioned purposes, and shall obtain the relevant explicit consents where necessary.

VI. Special Circumstances in Which Employee Personal Data Is Processed

1. Processing of Employee Personal Data in the Context of Benefits and Perquisites

Private health insurance, life insurance, personal accident insurance, company vehicle, private pension, flexible benefit programme or similar benefits are referred to as benefits and perquisites under this heading.

When sharing employees' personal data with third-party service providers for the purpose of providing benefits and perquisites to employees, the Data Controller takes care to share a minimum amount of data. Only the personal data necessary for providing the relevant benefit or perquisite is shared with such third parties. Additionally, measures are taken to ensure that personal data collected in this context is not used for any other purpose. Whether personal data to be shared with third-party service providers constitutes special categories of personal data is assessed prior to sharing. Employees are informed about personal data sharing with third-party service providers. Within this scope, employees are informed of which personal data is shared and for what purpose it will be used.

2. Processing of Employee Personal Data for the Purpose of Ensuring Equal Opportunities

The Data Controller may process personal data to the extent necessary to ensure equal opportunities among employees. Within this scope, the Data Controller aims to identify inequalities in processes such as recruitment, promotion, working conditions, and in-company career planning and development, and to ensure equal opportunities among employees by identifying equitable practices. Personal data may be processed for the purposes of ensuring gender equality in the workplace, implementing practices required by law (such as establishing breastfeeding rooms and nurseries) as well as practices identified by the Data Controller.

Personal data processed for equal opportunity purposes is checked at regular intervals. Personal data processed for this purpose is used in anonymised form to the greatest possible extent.

3. Processing of Employee Personal Data in the Context of Fighting Irregularities

The Data Controller may compare personal data sets in various units to prevent irregular transactions by employees. Rules for the comparison of personal data sets in the context of fighting irregularities are determined by the Data Controller. The Data Controller shares employees' personal data for the purpose of detecting irregular transactions only where one of the following or similar conditions exists:

- Where it is legally mandatory to share the relevant employee's personal data.
- Where there is strong suspicion that if the employee's personal data is not shared, a crime cannot be prevented or detected.
- Where data sharing is necessary for the proper implementation of Data Controller Policies and Procedures.

4. Processing of Employee Personal Data in Company Mergers, Acquisitions and Other Transactions Changing Company Structure

All transactions that change the company structure, including mergers and acquisitions, are assessed under this section.

When the Data Controller needs to share employees' personal data for the purpose of a change in company structure, it first ensures that such personal data is shared in anonymised form to the greatest extent possible. For employee personal data that cannot be shared in anonymised form, an undertaking is obtained from the counterparty that such data will be used only for transactions related to the change in company structure, that personal data will be protected in accordance with the data security provisions of the Law, processed in accordance with the relevant provisions of the Law, not transferred to third parties, and deleted or destroyed after the relevant transactions are completed.

5. Processing of Employee Personal Data in Disciplinary Investigations

The Data Controller is obliged to comply with its obligations regarding the protection of employees' personal data during disciplinary investigations as well. In this context, the following actions are taken in particular:

- Ensuring that policies and procedures relating to disciplinary investigations are aligned with obligations regarding the protection of personal data.
- Informing persons authorised to conduct disciplinary investigations that personal data within the scope of disciplinary investigations may also be accessed within the scope of employees' right of access to their personal data.
- Taking measures to ensure that personal data is not obtained through unlawful methods during disciplinary investigations.
- Ensuring that personal data to be used during disciplinary investigations is accurate and up to date.
- Retaining personal data and records relating to disciplinary investigations securely.
- Ensuring that unsubstantiated allegations about employees are deleted from employees' files if there is no legal reason for not deleting them.

The Data Controller prevents arbitrary access to employees' personal data solely on the grounds of a disciplinary investigation. In this context, personal data of employees may not be accessed solely for the purpose of a disciplinary investigation if such access is inconsistent with the purposes for which the personal data was obtained, or if accessing the personal data is considered a disproportionate measure given the seriousness of the subject of the investigation.

6. Processing of Personal Data Relating to Employees' Electronic Communications in Connection with Work Activities

The principles relating to the processing of personal data in connection with employees' electronic communications carried out in relation to work activities are specified in the Data Controller's "Information Systems General Standards and Security Policy".

7. CCTV Use at the Workplace

The Data Controller may install security cameras at various points to ensure the security of workplaces. Care is taken to ensure that the field of view of these security cameras covers only areas with particular risk, entry-exit points and similar areas, rather than the entire workplace. The Data Controller takes care to inform employees about the areas where filming and monitoring with security cameras takes place, and the purposes of monitoring.

8. Tracking of Company Vehicles

Where vehicles are assigned to employees by the Data Controller, the assigned vehicles may be tracked for purposes such as determining the distance covered, measuring fuel consumption and obtaining location data. Employees are informed in advance of such tracking.

VII. Statutory Rights of Employees Regarding Personal Data Collected About Them

1. Statutory Rights of Employees

Employees have the following rights:

- To learn whether personal data has been processed.
- To request information if personal data has been processed.
- To learn the purpose of processing personal data and whether it is used in accordance with its purpose.
- To know the third parties to whom personal data has been transferred domestically or abroad.
- To request correction of personal data that is incomplete or inaccurate, and to request that the operations performed in this scope be notified to third parties to whom personal data has been transferred.
- To request deletion or destruction of personal data where the reasons requiring processing cease to exist, notwithstanding lawful processing, and to request that the operations performed in this scope be notified to third parties to whom personal data has been transferred.
- To object to the emergence of a result against the person themselves by analysing the processed data exclusively through automated systems.
- To claim compensation for the damage incurred in case of damage due to unlawful processing of personal data.

2. Principles Regarding Exercise of Employees' Statutory Rights

The Data Controller takes all necessary administrative, legal and technical measures and designs the relevant processes to enable employees to exercise their statutory rights, to make necessary applications, and to respond to such applications within a maximum of 30 days.

All due care is taken to ensure that personal data of third parties is not disclosed in responses to employees exercising their statutory rights.

VIII. Sharing of Employee Personal Data with Third Parties

1. General Rules on Personal Data Sharing

The Data Controller establishes internal procedures for the sharing of employees' personal data. Data sharing requests are ensured to be answered by competent employees.

Necessary measures are taken to verify the authenticity and accuracy of data sharing requests from outside the Company (such as requests from judicial authorities, administrative authorities, insurance companies). Data sharing requests from outside the Company are required to be made in writing.

Where employees' personal data is sent abroad upon request, all necessary administrative, legal and technical measures regarding transfer of personal data abroad are taken.

Where sharing of employees' personal data constitutes a legal obligation, only the data sharing consistent with the scope of such legal obligation may be carried out. Subject to the statutory requirements regarding international data transfer and transfer of special categories of personal data, employees' personal data may only be transferred to third parties where one of the conditions set out in the Law exists.

2. Notification and Record-Keeping Regarding Personal Data Sharing

Prior to sharing employees' personal data with third parties, the sharing must be based on one of the conditions set out in the Law. Employees are informed of such sharing at the latest at the time of sharing, if they have not previously been informed. However, where such notification would constitute a legal violation or would amount to a prior warning regarding an investigation to be conducted by authorised authorities, the relevant employee is not informed of the matter.

Non-routine external data sharing requests regarding employees' personal data and sharing conducted within this scope may be recorded by the Data Controller. At a minimum, the following information is recorded: the person who approves the sharing, the person requesting the sharing, the reason for sharing, the date and time of sharing, and the types of data shared. These records are ensured to be regularly checked and reviewed.

3. Publication of Personal Data

The Data Controller may publish employees' personal data only while observing the following conditions:

- There must be a legal right or obligation for publishing the personal data, or the employee must have given explicit consent for publication.
- The personal data must not be clearly unsuitable for publication. The Data Controller acts with an approach that balances the benefits to be obtained from publication against employees' expectations of privacy.

Where the names and other personal data of certain employees are published in annual reports, publications or websites, such cases are specifically evaluated and whether explicit consent is required is determined. Where it is concluded that explicit consent is required, the relevant employees' explicit consent is obtained before the publication of personal data.

IX. Retention Period of Employee Personal Data

The Data Controller retains employees' personal data in accordance with the period necessary for the purposes for which they are processed and the minimum periods stipulated by the legislation applicable to the relevant activity.

In this context, the Data Controller first determines whether a retention period is stipulated in the relevant legislation for personal data. If a period is specified, it acts accordingly. If no statutory period exists, personal data is retained for as long as necessary for the processing purpose. Personal data is disposed of at the end of the determined retention periods in accordance with periodic disposal periods or upon the data subject's application, using the determined disposal methods (deletion and/or destruction and/or anonymisation).

X. Use of External Service Providers for Personal Data Processing

The Data Controller may use external service providers for the processing of employees' personal data. However, the Data Controller is required to take the following measures regarding external service providers:

- Verifying that the external service provider has taken the technical and administrative security measures required by the applicable legislation and industry practices.
- Auditing at regular intervals that the external service provider has taken the technical and administrative security measures required by the applicable legislation and industry practices.
- Concluding a contract with the external service provider containing conditions aimed at taking the necessary technical and administrative security measures.
- Taking necessary legal, administrative and technical measures where personal data is sent to external service providers abroad.

XI. Security of Personal Data

The Data Controller takes all reasonable measures to ensure the security of employee data. The measures taken are designed to prevent risks of unauthorised access, accidental data loss, intentional deletion or damage to data.

The Data Controller appoints responsible employees within the Company for personal data processing activities to be carried out specifically for employees' work activities. The number of employees who will be responsible for and have access to personal data obtained through such processing is kept as limited as possible. In this context, the Data Controller revokes or limits the access authorisations of employees who currently have unnecessary access to such data. Necessary physical security measures are taken to ensure that only authorised persons access employees' personal data. Additionally, authorised persons are prevented from having unnecessarily broad authorisation.

Measures such as audit trails are implemented on information systems pursuant to Law No. 5651, to enable identification of who accesses employees' personal data. Access logs created within this scope are regularly checked and investigation mechanisms for unauthorised access are established.

Employees with access to employees' personal data must undergo the necessary security checks. Such persons must also sign confidentiality agreements/undertakings or have relevant provisions included in their employment contracts, and must be continuously trained on their responsibilities.

Where employee personal data is taken outside the workplace via laptops or other devices, necessary security measures are taken and relevant employees are informed of these measures.

XII. Processing of Personal Data Relating to Employees' Activities at the Workplace

This section details the types of personal data (such as communication, vehicle use, etc.) that may be processed in relation to specific activities performed by employees in the course of the Data Controller's operations, and the principles to be observed by the Data Controller in this regard.

1. Determining for Which Work Activities and for Which Purposes Employee Personal Data Will Be Processed

The Data Controller identifies for which work activities and for which purposes it processes employees' personal data (such as email checks, use of vehicle tracking devices, CCTV monitoring) and determines personal data processing methods appropriate to the processing purposes and the intended outcome.

Following an internal evaluation, the Data Controller ensures that the purposes or methods of personal data processing in relation to employees' work activities comply with personal data protection rules. The Data Controller informs the employees assigned to personal data processing activities in relation to employees' work activities about data protection and related legislation, matters to be observed under applicable legislation, and the Data Controller's obligations under applicable legislation. Additional confidentiality and security obligations are added to contracts with employees who have access to personal data obtained through these activities, or such persons are required to sign confidentiality policies/undertakings.

2. Informing Employees About Personal Data Processing Activities of the Data Controller Relating to Employees' Work Activities

The Data Controller informs employees about how personal data processing is carried out in the context of work-related activities (such as email checks, use of vehicle tracking devices, CCTV monitoring), the purposes of processing such personal data and the procedures.

Where the Data Controller processes employees' personal data for purposes such as monitoring compliance with business and workplace rules during working hours, whether employees are fulfilling their duties properly, and tracking whether conduct disturbing workplace peace and order is occurring, the relevant employees must be clearly and specifically informed.

3. Use of Personal Data Obtained as a Result of Processing Employee Personal Data Relating to Work Activities for Other Purposes

Personal data processed in connection with employees' work activities may also be processed for other lawful purposes in accordance with the conditions specified in Article 5 of the Law and the personal data processing principles stipulated in Article 4 of the Law. Employees are informed of such purposes by the Data Controller through appropriate means.

4. Right of Defence for Employees Against Information Obtained as a Result of Processing Personal Data Relating to Work Activities

Before initiating a complaint procedure or disciplinary process against an employee on the basis of data obtained from the processing of personal data relating to their work activities, employees are given the right to view the data obtained, to make statements about such data, and to exercise their right of defence.

XIII. Categorisation of Personal Data

Within the scope of this Policy, in addition to the categorisation of personal data specified in the "Policy on Protection and Processing of Personal Data", the following categories of personal data of employees are processed:

- Employee Information: Personal data processed in the context of activities carried out to ensure the commercial and legal security of the Company and employees during their employment (including vehicle information, educational information, marital status information and reference information).
- Job Applicant Information: All types of personal data processed for the purpose of obtaining information to assess job applicants for the relevant position during the recruitment process (including military service status, educational information and reference information).
- Performance and Career Development Information: Personal data processed for the purposes of measuring the performance of the Data Controller's employees and planning and executing their career development within the Company's human resources policy, and for auditing such activities.
- Benefit and Compensation Information: Personal data processed in the context of determining and managing benefits and remuneration provided to employees (including salary information, bank account details and private health insurance information).
- Workplace Safety Information: Personal data processed for the purpose of ensuring occupational health and safety in the workplace (including information regarding occupational accidents, occupational diseases, health reports and emergency contacts).
- Legal Compliance Information: Personal data processed for the purpose of ensuring the Data Controller's compliance with applicable legislation (including information regarding work permits, social security registrations, tax registrations and judicial records where legally required).