

## PERSONAL DATA STORAGE AND DESTRUCTION POLICY

### OUR AIM:

As Yıldırım Holding A.Ş. and companies in our group;

The processing of personal data belonging to our employees, our suppliers, our customers and the real persons we are in a business relationship with, in accordance with the "Personal Data Protection Law" (KVKK) numbered 6698 and related legislation is among our priorities.

Based on the principle of "Honesty and Respect" to all parties, which is among corporate's values of establishment, Yıldırım Group Companies has the policy on this issue as follows:

All necessary administrative and technical measures for the processing, protection, transferring and destruction of personal data are taken by our group, and in this policy the details are explained. Data of legal entities are not included in this policy.

These policies and processes created by the senior management of the Group are periodically reviewed and updated as needed.

We are careful institutionally to make this policy clear and easily accessible to the public.

### DEFINITIONS:

**Personal Data:** Any information specific to an identified or identifiable natural person.

**Processing of personal data:** Any operations entirely or partially performed on personal data such as the recording, storage, archiving, alteration, rearrangement, disclosure, transfer, take over or use.

**Explicit consent:** Consent on a specific subject, based on information and taken with free will.

**Anonymization of personal data:** Making personal data unidentifiable or unrelated to a real person in any way, even by matching other data.

**Deletion of personal data:** Making personal data inaccessible and irrevocable for **the users concerned**.

**Destruction of personal data:** The process of making personal data inaccessible, irretrievable and irrevocable by **anyone**.

**Data controller:** A natural or legal person who is responsible for the establishment and management of the data record system which determines the processing purposes and means of personal data.

**Data processor:** Organizational unit responsible for the management of data that uses and stores personal data for its purpose.

**Periodic destruction:** The deletion, destruction or anonymization of the personal data which is carried out at intervals specified in the custody and destruction policy in the event that the processing conditions of the personal data are totally inadequate.

**TITLES, DUTIES AND RESPONSIBILITIES OF THOSE INVOLVED IN THE PROCESS OF STORAGE AND DESTRUCTION OF PERSONAL DATA:**

Unit or Administrator	Duty	Responsibility
Legal Directorate	Law Department-Personal data storage and destruction policy, legal compliance responsible	Evaluation of legislative appropriateness of processes and evaluation of legal aspects
Yıldırım Group KVK Committee Members (Company/department representatives and lawyers)	Member of the Committee on Protection of Personal Data	Establishment of the procedures of the company policy and rules in accordance with KVKK
Human Resources Managers	Human Resources Department - Personal data storage and destruction responsible	Proper storage of personal data on duty and proper management of the destruction process
Information Technology Management	Information Technology Department - Personal data storage and destruction responsible	Proper storage of personal data according to expiration date on duty and proper management of the destruction process
Department of Financial Affairs	Department of Financial Affairs - Personal data retention and destruction responsible	Proper storage of personal data according to expiration date on duty and proper management of the destruction process
Marketing and Sales Management	Marketing and Sales Department - Personal data storage and destruction responsible	Proper storage of personal data according to expiration date on duty and proper management of the destruction process
Administrative Affairs Department	Administrative Affairs Department - Personal data storage and destruction responsible	Proper storage of personal data according to expiration date on duty and proper management of the destruction process

## **PERSONAL DATA WE HAVE:**

The main personal data processed by our institutions and companies in the YILDIRIM Group can be described as follows:

- ID information; Name/Surname, T.R. Identification no., Passport no., place of birth/date, marital status, gender, insurance number, etc.
- Contact information; Address, Tel.no., E-mail address, voice call records saved by call center, Vehicle information (model, plate no., Etc.).
- Accounting information; Bank account number, IBAN no., Credit card information, Invoice information, Financial status information salary, etc.).
- Health information; Private health insurance data, Preventive medicine and related data.
- Use of biometric and fingerprints (for access).
- Customer complaints information, counter, subscriber consumption, etc. personal measurement assessment information.
- Past employment / life-related information included in the resume.
- Personal Background Documents; driving license, certificate, training records.

The personal data we have and, which are summarized above, are formatted in the inventory.

## **OUR LIABILITIES:**

### ➤ **Our Disclosure Obligation:**

While collecting personal data as a data controller, we have the obligation to inform the relevant person about the purpose of data processing, transferring of data to whom and for what purpose, and the deletion and destruction of the data after the completion of their function.

We educate and inform our employees about the storage, protection, deletion, destruction and transfer of personal data in accordance with the Personal Data Processing Law and company rules.

### ➤ **Our obligation to ensure data security:**

As we stated before, the administrative and technical measures required to ensure the safety of data are by us. Accordingly, our liability is to prevent the processing and access of personal data in violation of the law and company policy/rules, to ensure proper storage and safekeeping, and to carry out the destruction of data in accordance with the law and company policies/rules.

In the case of discrepancies with the rules, the required statutory and internal disciplinary actions are applied. In case of cooperation with third parties for the processing of personal data process personal data provisions regarding the necessary security measures are included.

To prevent unauthorized access to personal data, our human resources with technical expertise are utilized.

Physical and electronic access to personal data is restricted to authorized personnel. The authorization procedure is applied for data access within the company. During the internal audit processes, compliance with the relevant procedures and rules is controlled.

In case of unauthorized disclosure of personal data, the necessary procedure is established to inform the relevant person and the KVKK Board.

### **PROCESSING PERSONAL DATA:**

Our personal data processing purposes can be defined as;

- To maintain our corporate activities,
- To ensure the fulfilment of our legal obligations, as required or obliged by statutory regulations,
- To carry out our commercial activities with customers, dealers and suppliers in the supply chain,
- To evaluate job applications,
- To ensure compliance management,
- To carry out call center activities,
- To provide corporate communication,
- To provide information about individual, proper job announcement and employment,
- To protect employee rights,
- To send newsletters or notifications by SMS and E-mail.

We process personal data for the purposes stated above, and we do not process personal data that is not needed.

It is the responsibility of the data processor to ensure that personal data is up-to-date. Depending on the need, the relevant department contacts the data owner and ensures the data are up-to-date.

The data are deleted and destroyed at the end of the defined period according to the process.

### **PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA**

The special categories of personal data are processed with the explicit consent of data subject or required by legislation, and the details are given in the Security Policy of Special Categories of Personal Data.

### **PERSONAL DATA PROCESSING FOR HUMAN RESOURCES AND EMPLOYMENT PURPOSES:**

The personal data contained in the documents such as resumes etc., issued at the application of an employee candidate are processed, stored and transferred to Group companies for the purpose of evaluating the application.

The personal data of the employee are processed by the Human Resources department and are kept in the personal data files in the closed and protected areas.

### **WIRELESS NETWORK CONNECTION DATA:**

Data that includes time, location, continuity, downloading or loading content information of the connection that an electronic device used and/or uses to connect to any Internet or network. It is compulsorily collected and processed in order for the applications, internet etc., to be used. If the visitor does not allow this information, he/she cannot access the internet.

### **WHERE EXPLICIT CONSENT IS NOT MANDATORY IN THE PROCESSING OF PERSONAL DATA:**

The explicit consent is not required if the processing of personal data is

- clearly stipulated by the law
- necessary under the condition of actual impossibility
- necessary, provided that it is directly related to the establishment or performance of the contract.
- necessary for compliance with a legal obligation to which the data controller is subjected.
- made public by the data subject himself/herself
- necessary for the establishment, exercise or protection of any right.
- necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

### **SECURE TRANSFER OF PERSONAL DATA:**

Personal data for sharing with group companies, authorized representatives (lawyers, consultants and audit services, etc.) and our business partners (domestic and foreign) are transferred within the scope of the relevant legislation.

No data shall be transmitted to any other person without the consent of the data subject except for the cases stated above.

In case of transferring personal data abroad, the international protection situations defined by the KVKK Board shall be taken into consideration.

In addition, the technical and administrative measures necessary for the protection of data shall be taken by us.

E-mail is preferred for transferring personal data. The data transferred by encrypted files where the password and attachments are in separate e-mails.

With the exception of mandatory cases, data cannot be transferred with memory sticks. When required, this transfer is made in the company by the responsible persons. Encryption is applied for these data files.

Sealed envelopes are used for the security of the data transferred in paper environment. It is the responsibility of the data processor to take the necessary precautions in this regard.

## **PERSONAL DATA STORAGE:**

Laws and regulations oblige the storage of relevant personal data for a certain period of time. Therefore, it is our responsibility to keep such personal data in accordance with the legislation and for the required period of time. These retention periods are defined in the prepared inventory tables on the basis of data.

Personal data are kept for the period stipulated by the legislation or as required by its purpose. Data are stored in physical (unit cabinets, archives) or electronic (server, cloud, etc.) environment. Security measures have been taken for storage and protecting the data by providing the environment. In this environment, care is taken for not losing data integrity.

Personal data whose storage period has expired are destroyed (deletion, destruction) in 6-month periods. The necessary infrastructure and specific mechanisms have been established.

## **DELETION, DESTRUCTION OF PERSONAL DATA:**

In the following cases, the deletion, destruction and/or anonymization process are applied for personal data:

- If there is a change in the provisions of the legislation that constitute the basis for the processing of personal data,
- If the conditions that require the processing and storage of personal data are not valid anymore
- If the data subject concerned does not give consent or take back his/her consent and this decision is approved by the data collector
- If the maximum data storage period is expired
- If the request for the destruction of the personal data is approved as a result of application made to the KVKK Board

## **METHODS USED IN DELETION AND DESTRUCTION OF PERSONAL DATA:**

- The secure deletion and destruction of data stored in the physical environment (in cabinets and/or archives) is the responsibility of the unit managers that process the data. Such documents are destroyed by cutting, burning or shredding or other methods in such a way that they cannot be restored or read. Support may also be obtained from an expert organization for the destruction/disposal of these data as described.
- In the electronic environment, it is the responsibility of the Information Technology department to reliably delete and destroy it. The data stored in the digital environment is deleted in such a way that it cannot be accessed by relevant parties and is subjected to the destruction process in a way that cannot be reused. In the cloud system, the deletion of the relevant data is carried out by the same department.
- Transactions applied to data stored and destroyed in both physical or electronic media are recorded in specially prepared log-books or records by the data processor and information technology group. The records of deletion and destruction process performed in 6-month periods are kept for 3 years by the same groups unless otherwise specified.

### **ANONYMIZATION OF PERSONAL DATA:**

Anonymization is not implemented within our Group.

However, in the case of the use of some personal data for the purpose of statistical analysis and evaluation, in response to requests made from outside our group, these data are anonymized in a way that they cannot be matched with the persons they belong to (identity, position, etc.) and can be used by transferring them outside the organization.

In this case the responsibility lies in the data processing department, and compliance with rules is examined in internal audits.

### **RIGHTS OF DATA SUBJECT:**

The data subject has the following rights;

- To learn whether personal data is processed or not, and to request information about it,
- To learn the purpose of processing personal data and whether they are used appropriately for their purpose,
- To learn the recipients of the data both locally and internationally
- To request deletion and destruction of personal data in case the reasons for requiring the processing of personal data disappear,
- To request correction or updating of personal data if they are incomplete, incorrect or out of date,
- To claim compensation for the damage arising from the unlawful processing of personal data

### **USE OF COMMUNICATION AND RIGHTS:**

In the case of claims within the clauses above, according to the nature of the claim, the request shall be concluded as soon as possible within thirty days (30) at the latest, free of charge or in accordance with the terms of the tariff to be determined by the KVKK Board.

Requests in this regard may be made by written and signed document to the Department of the Legal Directorate located at the following address: Yıldırım Holding, Maslak Mah., Söğütözü Sok., No:1C, Maslak 1453 Sitesi, B2 Blok, Sarıyer, İstanbul.

The application is justified and rejected in cases where it is not based on a just cause, involves a transaction contrary to the relevant legislation, or if the application procedure is not followed.