Sensitive Personal Data Processing Policy

Purpose

This Policy was drafted by Çanakkale Otoyol ve Köprüsü İnşaat Yatırım ve İşletme A.Ş. **("Company")** as data controller in accordance with the Turkish Law No. 6698 on the Protection of Personal Data ("KVKK" or "Law") and Communiqué on the Procedures and Principles for Fulfillment of the Obligation to Inform, in order to determine in accordance with the legislation the procedures and principles for the processing of sensitive personal data of employees.

Scope

This Policy covers the processing of sensitive personal data of the Company's employees and its suppliers' employees.

This Policy may apply in full to all the aforementioned categories of data subjects while it could also be applied partially.

Foundations

This Policy is based on the Law No. 6698 on the Protection of Personal Data, the Regulation No. 30286 on the Data Controllers Registry and the Regulation No. 30224 on the Deletion, Destruction or Anonymization of Personal Data and the Board decision titled "Adequate Measures to be Taken by Data Controllers When Processing Sensitive Personal Data".

In the event of any inconsistencies between this Policy and the applicable legislation on the processing, protection and destruction of personal data, provisions of the Legislation shall prevail in application.

Sensitive Personal Data Storage Media

Sensitive personal data of data subjects are stored securely in the areas listed below by the Company in accordance with the relevant legislation, in particular the provisions of KVKK, and within the framework of international data security principles:

a) Electronical data storage areas:
   1. Computers,
   2. Shared / non-shared disk drives for storing data over the network,
   3. Cloud services.

b) Non-electronical data storage areas:

   1. Papers,
   2. Unit cabinets.

Technical and Administrative Measures Taken for Secure Storage of Sensitive Personal Data and to Prevent Unlawful Processing and Access

The Company takes all necessary technical and administrative measures to ensure compliant processing and destruction of sensitive personal data in accordance with the Law and good faith.

Additional technical and administrative measures taken for sensitive personal data are as follows:

- Protocols and procedures for ensuring the security of sensitive personal data have been determined and implemented.
- When sensitive personal data is transferred by e-mail, it is sent in encrypted form and via KEP (Registered Electronic Mail) or corporate e-mail account.
- Up-to-date encryption / cryptographic keys are utilized for sensitive personal data and are managed by different units.

Detailed information on technical and administrative measures taken for the processing of personal data is contained in the **"Personal Data Retention and Destruction Policy"** published by the Company.

Categories of Sensitive Personal Data Processed

The categories of sensitive personal data of employees and/or suppliers' employees as processed by the Company are:

PERSONAL DATA CATEGORY	**PROCESSED PERSONAL DATA IN THE CATEGORY**	**RETENTION PERIOD**	**DESTRUCTION PERIOD**
Health Data	Blood type information, disability status, personal health data, use of medical devices/prostheses	15 years after the conclusion of business relations	Within 6 Months After Expiration of Storage Period
Criminal Conviction and Security Measures	Criminal records	10 years after the conclusion of business relations	

Purposes of Processing Sensitive Personal Data

Sensitive personal data of employees and suppliers' employees can be processed for the following purposes, in accordance with Article 20 of the Constitution and Article 4 of the KVKK:

- Audit / Ethics Activities
- Compliance with the Legislation
- Internal Audit / Investigation / Intelligence Activities
- Human Resources Process Planning
- Conducting Workplace Health / Safety Activities
- Execution of Assignment Processes
- Retention and Archiving Activities
- Conducting of Contract Processes

Transfer of Sensitive Personal Data to Third Parties

Sensitive personal data can be transferred to the following groups of natural or legal persons, provided that they are limited to the purposes of processing:

- Business Partners
- Suppliers
- Authorized Public Institutions and Organizations

Destruction of Sensitive Personal Data

All information and procedures regarding the destruction of sensitive personal data can be found in the "Personal Data Retention and Destruction Policy" published by the Company.

Table of Updates

Changes to this Policy up to this date are listed in the table below.

UPDATE DATE	**SCOPE OF UPDATES**
20.01.2020	Policy publication date