POL.12 · KVKK

Special Categories of Personal Data Processing Policy

English translation for information. In case of discrepancy the Turkish text prevails (Türkçe metin esastır).

1 Purpose

This Policy sets out the processes for processing and securing special categories of personal data defined in Law No. 6698 on the Protection of Personal Data (the "Law").

2 Scope

Article 6 of the Law requires data controllers to also take the adequate measures determined by the Personal Data Protection Board when processing special categories of personal data.

This Policy covers the processing and security of special categories of personal data in line with the Board decision on "Adequate Measures to be Taken by Data Controllers in Processing Special Categories of Personal Data", published in the Official Gazette No. 30353 of 07.03.2018.

3 Processing of Special Categories of Data

Article 6 of the Law defines as "special categories of personal data" the data that may cause victimisation or discrimination if processed unlawfully: data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data.

Our Company strictly complies with the provisions of the Law when processing such data. Special categories of personal data are processed under the following conditions, provided that the adequate measures determined by the Board are taken:

Type of data	Processing condition	Example
Data on health and sexual life	Explicit consent of the data subject	Maternity leave and fit/unfit-for-work reports under the Labour Law
Special categories other than health and sexual life	Explicit consent of the data subject, or where provided by law (tax laws, Labour Law No. 4857, Turkish Commercial Code)	Criminal record certificate of an employee under Labour Law No. 4857

In our Company, special categories of personal data belonging to our employees are processed by the unit carrying out human resources activities; special categories of personal data contained in the

identity documents of persons with whom we have a contractual or commercial relationship, or of their employees/representatives, are processed within the relevant process. This data is processed and retained for the following purposes:

- carrying out processes related to obtaining health reports,
- making position changes according to an identified health condition and providing employees with positions suited to their health,
- intervening without delay where a situation may affect the health of other employees,
- complying with information retention, reporting and notification obligations imposed by legislation, regulators and other authorities,
- creating personnel files.

The data processed is: special categories of data contained in identity documents, laboratory test reports, maternity reports, sick-leave and incapacity reports, psychotechnical reports, disability reports, SGK (social security) reports and leave documents, blood group certificates, pre-employment health reports, civil society organisation membership certificates, additional health screening reports (laboratory findings, physical examination results, medical history, etc.), personal health information and criminal conviction data (criminal record). This data is kept by the unit carrying out human resources activities.

4 Security of Special Categories of Data

As data controller, our Company takes the following measures for special categories of personal data:

For employees

Regular training is provided on the Law, related regulations and the security of special categories of data; confidentiality agreements are signed; the scope and duration of access rights are defined; access rights are checked periodically; the rights of employees who change roles or leave are removed immediately.

Electronic environments

Data is stored using cryptographic methods; cryptographic keys are kept securely in separate environments; all actions on the data are logged securely; security updates are tracked continuously and security tests are carried out regularly and recorded; where data is accessed through software, user authorisations are defined; remote access requires at least two-factor authentication.

Physical environments

Adequate measures are taken, according to the nature of the environment, against electrical leakage, fire, flooding, theft and similar risks; physical security is ensured and unauthorised entry is prevented.

Transfers

Where e-mail transfer is necessary, it is made encrypted from a corporate e-mail address; media such as USB drives, CDs and DVDs are encrypted and the key is kept separately; transfers between servers in different physical locations use an encrypted connection (VPN or SFTP); for paper transfers, measures are taken against theft, loss or viewing by unauthorised persons and documents are sent marked “Confidential”.

In addition to these measures, the technical and administrative measures set out in our Personal Data Protection and Processing Policy (POL.13) also apply.

APPROVED BY
TURKEYSMS BİLİŞİM VE İLETİŞİM HİZMETLERİ TİCARET LİMİTED ŞİRKETİ
General Management

ISSUE DATE
06.01.2026
Revision No: 00