Cengiz Holding A.Ş.

Information Confidentiality Policy

Revision No. : 01
Revision Date : 15.09.2025

Table of Contents

1. Purpose and Scope

The Information Confidentiality Policy ("Policy") aims to protect personal data, trade secrets, technical information, and all other confidential information belonging to existing and potential customers, third parties, business partners, employees and job candidates, shareholders, visitors, and employees of institutions in cooperation with Cengiz Holding Inc. and its Group Companies ("Cengiz Holding", "Holding" or "Group").

The Policy is intended to ensure Cengiz Holding's compliance with applicable legislation, the Law on the Protection of Personal Data No. 6698 ("KVKK"), and the national and international data protection standards in force in the countries of operation (e.g., GDPR, ISO 27001).

This Policy covers all individuals and institutions whose personal or confidential information is obtained by the Holding in the course of its activities.

2. Definitions

Unless otherwise defined under this section, the terms, words, and expressions used in the Policy shall take their meaning from applicable laws, regulations, and sectoral usage.

Explicit Consent: Refers to consent that is related to a specific subject, based on information, and declared with free will.

Anonymisation: Refers to making personal data impossible to associate with an identified or identifiable natural person under any circumstances, even by matching with other data.

Personal Data: Refers to any information relating to an identified or identifiable natural person.

Processing of Personal Data: Refers to any operation performed on personal data, whether fully or partially automated, or non-automated provided that it forms part of a data recording system, such as collection, recording, storage, retention, alteration, reorganisation, disclosure, transfer, acquisition, making available, classification, or prevention of use.

Legislation: Refers to the Law on the Protection of Personal Data No. 6698 and all applicable laws in Türkiye and in the countries and regions where operations are carried out, concerning the protection of personal data.

Phishing: Refers to a fraud method aiming to obtain user data by sending fake messages via e-mail.

Data Controller: Refers to the natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

Data Processor: Refers to the natural or legal person who processes personal data on behalf of the data controller based on the authority granted.

3. General Principles

Cengiz Holding acts in accordance with the Law on the Protection of Personal Data No. 6698 (KVKK) in particular, as well as all relevant national and international data protection

regulations and the principles of lawfulness in the processing of personal data. In this context:

Compliance with the Law and the Principle of Good Faith

Personal data must be processed within the framework defined by legislation, taking into account the interests and expectations of the data subject, and only to the extent required by the activities and limited thereto.

Accuracy and Keeping Data Up to Date When Necessary

Both the data subject and the business processing the data may suffer harm from outdated or inaccurate personal data. Accordingly, the sources from which personal data are obtained must be identifiable, and the accuracy of the source from which the data is collected must be verified.

Processing for Specific, Explicit and Legitimate Purposes

Personal data may only be used for the purposes for which they are processed. In this respect, clear explanations regarding the processing must be provided to the data subject.

Being Relevant, Limited, and Proportionate to the Purpose of Processing

There must be a reasonable balance between the data processed and the purpose sought to be achieved. Accordingly, the information collected about an individual must be limited to what is relevant and necessary to achieve the intended purpose.

Rules on Transfer

Personal data may not be transferred to third parties within or outside the country without the explicit consent of the data subject, unless exceptions set out in the legislation apply.

Conditions for Processing Special Categories of Personal Data

Special categories of personal data may not be processed without the explicit consent of the data subject. If such data are processed, the measures specified by the Personal Data Protection Board must be taken. Special categories of personal data other than health and sexual life may be processed without explicit consent, provided that it does not violate the relevant legislation. Personal data relating to health and sexual life may only be processed without explicit consent in exceptional cases specified in legislation, such as for the protection of public health or the execution of treatment and care services.

Retention Period

Personal data shall be retained for the period stipulated in the relevant legislation or as long as required by the purpose of processing. Once this period expires, the data shall be deleted, destroyed, or anonymised.

Obligation to Inform

As the Data Controller, Cengiz Holding informs the data subject at the time of data collection regarding:

- The identity of the Data Controller and, if applicable, its representative,

- The purpose for which the data will be processed and to whom it may be transferred,
- The method and legal grounds for collecting the data.

Rights of the Data Subject

Data subjects have the right to apply to the Data Controller to learn whether their data is being processed, to request correction or deletion of their data, to demand restriction of data transfer, and to seek compensation for damages arising from unlawful processing.

Circumstances Requiring the Processing of Personal Data:

- Execution of human resources processes,
- Corporate communication activities,
- Ensuring company security,
- Statistical studies,
- Contractual business and transactions,
- Fulfilment of legal obligations,
- Maintaining communication in business relationships,
- Execution of occupational health and safety processes,
- Operation of information systems processes.

4. Implementation Principles

Clean Desk, Clean Screen, and Password Security

All physical documents containing sensitive, personal, or confidential information belonging to the Holding, its customers, or third parties must be stored in lockable cabinets or drawers when employees are not at their desks.

Employees must not keep information obtained within the scope of their duties and responsibilities on their computer desktops but must store it on platforms that ensure data protection in shared areas.

Employees must never share their computer login passwords with other employees or any third parties. Passwords must be strong and changed periodically.

Elektronik Mail (E-mail)

Employees must not use their company e-mail addresses, which are used as a means of communication inside and outside the company, for personal matters. Accordingly, employees must not use their company e-mail addresses on non-business platforms, must not subscribe to unknown organisations or social media platforms with these addresses, and must not publish their company e-mail addresses on social media.
Employees must not open e-mails or attachments when in doubt about the sender's identity. Such e-mails must be forwarded to the Information Technology (IT) Department for verification of whether they constitute a phishing attempt.
Except in cases where the nature of the work requires the sharing of personal data and the approval of the relevant individuals has been obtained, employees must not openly transmit information containing personal data via e-mail to an external third party. In such cases, personal data must be masked.

Access to Shared Area

Employees may only access information that they require in line with their duties and responsibilities. Access rights to files in shared areas are monitored and controlled by the IT Department. To prevent employees from accessing information not required for their duties, the IT team must take the necessary precautions, assigning access rights in accordance with job descriptions. Access rights to shared areas must be reviewed periodically, and corrective actions must be taken when deemed necessary. Employees' authorisations are determined by the Human Resources Department and implemented by the IT Department.

Security of Physical and Digital Documents

Access to areas where physical documents are stored across the Holding must be restricted solely to employees authorised in the relevant processes. For this reason, the necessary measures are taken by the IT Department.

Documents containing information on personnel, customers, or third parties, which are stored in digital environments, must not be taken outside the Holding, either physically or digitally, unless necessary.

Use of Social Media

Employees must not share any personal or commercial information obtained through work, which is not publicly available, on their personal social media accounts. Employees must avoid making such disclosures even if they use their social media accounts anonymously. Details regarding matters employees must pay attention to in the use of social media are specified in the Cengiz Holding Social Media and Communication Policy.

5. Roles and Responsibilities

Cengiz Holding employees and Third Parties within the scope of this Policy are obliged to comply with it. If a situation contrary to the rules set out in the Policy is identified, or if a compliance risk arises, the matter must be promptly reported through one of the following channels:

- Legal Departant
- Information Technology Department
- Ethics Hotline[1] *(etikdestekhatti.com)*

Those who report in good faith shall in no way be subject to retaliation or adverse treatment.

The joint responsibility of the Information Technology and Legal Departments is to ensure that the requirements of this Policy are communicated to employees, understood, and that internal control mechanisms for its implementation are established.

[1] For details regarding the reporting process and the use of the ethics hotline, please refer to the *Cengiz Holding Whistleblowing and Reporting Policy*

In the countries where Cengiz Holding operates, if the legal regulations within the scope of this Policy impose stricter provisions than those contained in the Policy, the legislation of the respective country shall prevail.

Activities carried out under this Policy, as well as identified violations, shall be reported annually to the Board of Directors in line with the principles of transparency and accountability.

6. Revision History

This Policy has been approved and enacted by the relevant Resolution of the Company's Board of Directors, and the joint responsibility of the Information Technology and Legal Departments is to update it periodically in line with changes in legal regulations and Group processes.

Revision No.	Revision Date	Description
01	15.09.2025	Revised to enhance alignment with applicable legislation, international standards, and company practices.