Cengiz Holding A.Ş.

Policy on the Confidentiality of Information

Table of Contents

1. Objective and Scope

Policy on the Confidentiality of Information (the "**Policy**") has been prepared in order to comply with all legal regulations regarding the registration and protection of personal and commercial data of the customers, third parties, business partners, employees and employee candidates, shareholders, visitors and employees of the cooperating institutions with present or potential business relationship with Cengiz Holding A.Ş. and Group Companies (**"Cengiz Holding", "Holding"** or **"Group"**) and to determine the principles of application within the scope of the confidentiality of information.

This Policy covers all persons whose personal data has been acquired by the Holding while performing its activities.

2. Definitions

If the terms, words, and expressions used in the policy have not been defined under this title, their meanings shall be taken from the applicable laws, regulations and sectoral meanings.

Explicit Consent: Shall refer to a consent about a specific subject based on information and expressed in free will.

Anonymization: Shall refer to making personal data unlikely to be associated with any identifiable real person in any manner even when personal data is paired with other data.

Personal Data: Shall refer to any information related to the identity of a specific or identifiable real person.

Processing of Personal Data: Shall refer to any transaction performed on the data such as obtaining, recording, storage, preservation, alteration, rearrangement, disclosure, transfer, acquisition, recapture, classification or preventing the use of the same by non-automated means provided that personal data is a part of a wholly or partially automated data recording system.

Legislation: Shall refer to all relevant legislation in force in Türkiye and in the countries and regions where the Holding operates, particularly the Law on the Protection of Personal Data No. 6698.

Phishing: Shall refer to the fraud method aimed at capturing user data by sending fake messages via e-mail.

Data Controller: Shall refer to the real person and legal entity responsible for establishing and managing the data recording system that specifies the objectives and means of processing personal data.

Data Processor: Shall refer to the real person or legal entity who processes personal data on behalf of the data controller based on the authority vested to it by the data controller.

3. General Principles

In the process of processing personal data, the Holding acts in accordance with the following rules abiding by the principles specified in the Law on the Protection of Personal Data.

Compliance with the Law and Rules of Integrity

Personal data should be processed within the framework determined by the legislation, taking into account the interests and expectations of the data owner and only to the extent and limited to what is required by the activities.

Being accurate and up-to-date when necessary

The data owner and the business that processes the data may be harmed due to outdated and incorrectly processed personal data. In this context, the sources from which personal data has been obtained should be specific, and the accuracy of the source from which personal data has been collected should be determined.

Processing data for specific, clear, and legitimate purposes

Personal data should only be used for the purpose for which they are processed. In this context, it is necessary to make understandable explanations about the data processing to the person whose personal data has been processed.

Personal Data being linked, limited to and measured with the purpose of being processed

Personal data must have a reasonable balance between the processing of the data and the transactions to be carried out. In this context, the information of a person should only be in connection with the activity to be carried out and the process should cover the necessary information at a minimum level.

Personal data may not be transferred to another person or institution in the country or abroad without the consent of the data owner.

Conditions for Processing Sensitive Personal Data

Sensitive personal data should not be processed without the consent of the data owner. In the case of processing data, the measures specified by the Personal Data Protection Board should be taken. Sensitive personal data other than related to health and sexual life may be processed without the explicit consent of the data owner in a manner that does not violate the legislation. Personal data covering health and sexual life may be processed without the explicit consent of the data owner in cases specified in the legislation such as the protection of public health, the execution of treatment and care services.

Retaining data for the period of time stipulated by the relevant legislation or as deemed necessary for the purpose of processing

The Data Controller shall be obliged to take the necessary technical and administrative measures to ensure the appropriate level of security in order to prevent the unlawful processing of and access to personal data and to ensure the protection of the same.

Disclosure Obligation of the Data Controller

The Data Controller of Cengiz Holding should provide information to the relevant data owners on the following during the acquisition of personal data:

- ✓ Identity of the Data Controller and that of his/her representative, if any,
- ✓ To whom and for what purpose the processed personal data shall be transferred,
- ✓ Management of personal data collection and legal reasons.

By applying to the Data Controller, the Data Owner shall have the right to learn whether the personal data has been recorded, for what purpose it has been recorded, how long the retention period is, to learn whether the personal data will be transferred or not, to receive information about the accuracy of the personal data, to request the deletion of the personal data and to request compensation for any damage in case of unlawful processing of the personal information.

Issues requiring the processing of personal data can be listed as follows:

- ✓ To carry out the human resources processes,
- ✓ To provide the corporate communication activities,
- ✓ To ensure company security,
- ✓ To conduct statistical studies,
- ✓ To perform the works and transactions as the result of the signed contracts,
- ✓ To ensure that the legal obligations are fulfilled as required or as rendered obligatory by legal regulations,
- ✓ To be able to communicate with real persons and legal entities who have a business relationship with the company,
- ✓ To ensure the fulfillment of occupational health and safety processes,
- ✓ To conduct information systems processes.

Deletion, destruction, and anonymization of personal data

The personal data kept in the records should be automatically deleted, destroyed or anonymized by the Data Controller upon the request of the data owner or when the reasons for the data to be kept in the records have been eliminated.

4. Application Principles

Clean Desktop, Clean Screen and User Passwords

All physical documents containing sensitive, personal, or confidential information belonging to the customer and third parties or those inside the holding must be kept in locking cabinets or drawers when the employees are not at their desk.

Employees should not keep the information they obtain as required by their duties and responsibilities on their computer desktop and keep the same on platforms that provide data protection in the common area.

Employees must not share their computer boot passwords with another employee or a third party in any manner.

Electronic Mail (E-Mail)

Employees should not use the e-mail addresses they use as a means of communication inside and outside the company to conduct their personal business. For this reason, employees should not use their e-mail addresses defined by the Holding on non-business platforms, should not subscribe to an entity or social media platforms with this e-mail address, and should not publish their business e-mail addresses on social media.

Employees should not open e-mails and their attachments where they suspect about the sender and should ensure that these e-mails are directed to the relevant Information Technology (IT) Unit to confirm whether there are any phishing attacks or not.

Employees should not disclose information containing personal data to an external third party by e-mail, except where it is necessary to share personal data due to the nature of the work performed and the consent of the data owners has been obtained. In such cases, personal data must be masked.

Access to Common Area

Employees should only have access to the information they require due to their duties and responsibilities. The access rights to the files in the common area shall be controlled and monitored by the Information Technologies Unit. In order to prevent the employee from accessing the information not required by his/her duty, the access authorizations should be defined in accordance with the job descriptions by taking the necessary measures by the Information Technologies team and corrective actions should be taken if deemed necessary by regularly controlling the access authorizations under the common area. The authorization definitions of the employees shall be determined by the Human Resources Department and implemented by the IT Department.

Security of Physical and Digital Documents

Only the employees authorized in the relevant processes should be allowed to access the areas where physical documents are kept throughout the Holding. For this reason, the necessary measures are taken by the IT Department.

Documents stored in digital environment and containing information of the personnel, customers or third parties should not be taken out of the Holding physically or digitally, unless necessary.

Use of Social Media

Employees should not share any personal or commercial information that they acquire due to business and that should not be publicly available on their personal social media accounts. Employees should refrain from sharing such posts even if they use their social media accounts anonymously.

Details of the issues that the personnel should pay attention to regarding the use of social media have been specified in *Cengiz Holding Social Media and Communication Policy*.

5. Authorities and Responsibilities

All Cengiz Holding employees shall be obliged to comply with this Policy and if they witness a situation contradicting the rules mentioned in the Policy, the situation must be forthwith reported to the

- Legal or
- IT

departments.

The IT and Legal Departments shall be responsible for communicating the requirements of this Policy to the employees and creating an internal control environment where the employees act in accordance with the Policy.

If the legal regulations under this Policy in the countries where Cengiz Holding operates are stricter than those of the Policy, the relevant legal regulations should be considered.

If the policy is not abided by, employees may face various disciplinary penalties, which may include termination of employment.

6. Revision History

This Policy has been approved and entered into force with the relevant Board of Directors Decision of the Company and it will be the joint responsibility of the IT and Legal Departments to periodically update the Policy in line with the changing legislation and Group processes.

Revision	Date	Description