Cengiz Holding A.Ş.

Retention of Records Policy

Table of Contents

1. Objective

The Retention of Records Policy ("**Policy**") has been prepared to determine the rules to be followed for the storage of data kept as physical documents and in digital media containing information about the customers, personnel, business partners and all other third parties within Cengiz Holding and its Group Companies ("**Cengiz Holding", "Holding"** or **"Group**").

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.

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

Recording Environment: Any media in which personal data are processed, which are fully or partially in automated way or non-automated way provided that it is part of a 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.

Third Party: Shall refer to the supplier, contractor, subcontractor, dealer, distributor, broker or all representatives and consultants acting on behalf and on account of the Holding.

3. General Principles

Employee, employee candidate, customer, visitor and Third-Party data will be stored and destroyed by Cengiz Holding in accordance with the provisions of the relevant legislation.

This Policy shall apply to the information in the records listed below, including but not limited to:

- Printed or unprinted documents containing all kinds of personal information,
- Contracts concluded with employees, customers and all third parties,
- Documents including the meeting materials and meeting minutes of the Board of Directors and the management committees of the companies,
- Documents containing Group trade secrets with the organizations with which operations are carried out,
- Documents used in sales and marketing processes,
- Expense forms and invoices, receipts and vouchers related to expenses,
- All personnel and personnel candidate records kept for the realization of human resources processes,
- Electronic mails,
- Flash memories.

4. Application Principles

All information and documents obtained within the scope of Holding activities should be kept in a manner that will ensure their confidentiality and authenticity. Records can be retained in physical or digital media.

Cengiz Holding will take the necessary measures for the safe storage of all recorded information and documents. In this context, it is the responsibility of the units that produce and/or provide the information and documents recorded in physical environments in accordance with the job description, and the physical conditions of the archive environments should be monitored, and necessary measures should be taken to prevent situations such as fire or flood. The authority to enter the archives should be monitored by the Information Technology (IT) Unit and only authorized personnel should be allowed to enter the archives.

The IT Unit shall be responsible for the security of the records kept in digital environment. It should be ensured that the necessary precautions are taken to prevent any system failure and, if deemed necessary, the information and documents recorded in digital environment are recorded in a cloud environment other than Holding systems. In addition, it should be stated that the confidentiality principles will be respected in the contract with the cloud environment provider.

Regarding the processing of personal data, Cengiz Holding acts in accordance with local and international legislation. For detailed information, please refer to the *Cengiz Holding Policy on the Confidentiality of Information.*

4.1 Classification of Records

Classification of records plays an important role in protecting privacy and confidentiality. Records are classified as "public, internal document or confidential" according to the value they bear.

Public records can be expressed as the records that cannot have an adverse impact on Cengiz Holding when taken outside the Holding. The information contained in these documents shall not violate the legal regulations applied within the scope of the protection of personal data and shall not jeopardize the reputation of the Holding. Information about the newspapers, websites, brochures, flyers, or published marketing research will be evaluated under this category.

The records expressed as **internal documents** will cover almost all documents related to the activities of the Holding. Unauthorized sharing of these records may pose a reputational risk for the Holding. Sharing of these documents will only be carried out if it is necessary in the realization of the activities and upon the approval of the senior management. Documents such as office documents, employee information, travel information, policies and procedures, presentations, etc. shall be evaluated under this category.

Records that are considered **confidential** are those that contain commercial information related to the activities of the Holding. These listings require a high level of attention, limited access, and special controls. Unauthorized publication of these records may constitute a violation of the law. These records may only be shared with the employees and/or third parties reasonably, if access is required, but only for the intended purpose. Third party due diligence studies,

committee reports, personal employee information, internal financial and commercial documents and customer information shall be evaluated under this category.

4.2 Retention of Records

Cengiz Holding retains all the information and documents it has obtained for the performance of its activities for at least the periods specified in the legislation and for a longer period of time in cases where there will be no violation of the legislation. Records that have expired should be deleted and destroyed. For information and documents for which the maximum retention period has not been determined by the legislation, each unit may determine the appropriate retention period.

Retention periods can be determined considering the following:

- The period specifically required for the data category,
- Term of the legal relationship,
- The duration of the legitimate interest obtained by Cengiz Holding depending on the purpose of processing the relevant data,
- Legal risks, costs and responsibilities arising from the storage of relevant data,
- The statutory statute of limitations for claiming data.

Records can be archived in groups by date or category. All physical or digital archives must be accessible only to authorized persons.

Physical records can be stored in Holding facilities or in a supplier archive as required. If it is necessary to work with a supplier for the archiving process, it will be necessary to carry out due diligence studies for the relevant supplier by the purchasing unit and to periodically inspect the archive areas.[4]The supplier must have taken adequate measures of protection from internal and external factors (fire, earthquake, flood, lack of air, theft, etc.) for the archive location.

4.3 Destruction of Records

All confidential and sensitive information recorded in physical or digital media must be destroyed securely when no longer needed.

Cengiz Holding can physically record many information and documents due to its daily activities. It is very important that these records are destroyed safely. If the legal retention periods of official records have expired, no special approval process shall be required for their destruction. Each unit shall be responsible for the follow-up and destruction of the records it keeps under its job description. Units should check at least once a year to determine which records have expired. It is essential to consult the Legal Counsel in cases where there is no certainty about the legal periods.

Physical records shall be destroyed by appropriate methods in accordance with the confidentiality rules.

[4]Detailed information regarding the process has been included in the *Cengiz Holding Policy on the Prevention of Laundering Proceeds of Crime*.

As for the destruction of digital records, it may not be enough to delete them from the physical devices they are stored in. In these cases, devices that offer electronic recording may also need to be irreversibly destroyed.

The date and reasons for the destruction of the records shall also be recorded and retained by the relevant unit.

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,
- Human Resources or
- to the IT

departments.

The Legal, Human Resources and IT Department 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 Legal, Human Resources and IT Departments to periodically update the Policy in line with the changing legislation and Group processes.

Revision	Date	Description