Cengiz Holding A.Ş.

Record Retention Policy

Revision No. : 01
Revision Date : 15.09.2025

Table of Contents

1. Purpose and Scope

The Record Retention Policy ("Policy") has been prepared to establish the rules to be followed regarding the retention, protection, access, and, where necessary, disposal of physical documents and digital records maintained by Cengiz Holding Inc. and its Group Companies ("Cengiz Holding", "Holding" or "Group") that contain information relating to customers, personnel, business partners, and all other third parties.

This Policy applies to:

- All employees, managers, and Group Companies of Cengiz Holding,
- All types of records used in business processes (written, printed, electronic, audio, visual, etc.),
- Records shared with or obtained from the Group's suppliers, business partners, and consultants.

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.

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

Record: Refers to all information and documents created, received, or retained within the scope of company activities, whether written, printed, electronic, audio, or visual.

Electronic Record: Refers to any record stored in digital environments, including but not limited to servers, e-mails, invoicing systems, camera recordings, and mobile devices.

Physical Record: Refers to records kept in portable physical media such as files, folders, notebooks, written documents, magnetic tapes, CDs/DVDs, USB drives, and external hard drives.

Record Medium: Refers to any environment in which personal data is processed, whether fully or partially automated, or non-automated provided that it forms part of a data recording system.

Retention Period: Refers to the period for which records must be kept in line with legal, administrative, contractual obligations, or business requirements.

Disposal: Refers to the permanent deletion, destruction, or anonymisation of records whose retention period has expired or which no longer need to be retained.

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

Third Party: Refers to any supplier, contractor, subcontractor, dealer, distributor, intermediary, or any representative and consultant acting on behalf and account of the Holding.

3. General Principles

Records belonging to employees, job candidates, customers, visitors, and Third Parties are retained by Cengiz Holding in compliance with applicable legislation and securely disposed of when their retention periods expire.

This Policy applies to, but is not limited to, the following types of records:

- Physical or digital documents containing personal information,
- Contracts concluded with employees, customers, and all third parties,
- Documents including meeting materials and minutes of the Board of Directors and company management committees,
- Documents of a trade secret nature,
- Documents relating to sales and marketing processes,
- Accounting records, expense reports, invoices, receipts, and vouchers,
- Employee and candidate records relating to human resources processes,
- E-mails and internal company correspondence,
- Portable storage devices.

4. Implementation Principles

All information and documents obtained within the scope of the Holding's activities must be retained in a manner that ensures their confidentiality and integrity. Records may be documented in physical or digital environments.

Cengiz Holding takes the necessary measures to ensure the secure preservation of all recorded information and documents. In this context, the safe storage of information and documents recorded in physical environments is the responsibility of the units that produce and/or obtain them as part of their job descriptions. The physical conditions of archive environments must be monitored, and the necessary measures must be taken to prevent incidents such as fire or flooding. Access to archives must be monitored by the Information Technology (IT) Department, and only authorised personnel may enter the archives.

The IT Department is responsible for the security of records kept in digital environments. Necessary measures must be taken to prevent system failures, and where deemed necessary, information and documents recorded in digital environments must also be stored in a cloud environment outside the Holding's systems. Furthermore, the contract with the cloud service provider must stipulate adherence to confidentiality principles.

With regard to the processing of personal data, Cengiz Holding acts in compliance with local and international legislation. Detailed information on this matter is set out in the Cengiz Holding Information Confidentiality Policy.

4.1 Classification of Records

The classification of records plays a key role in ensuring confidentiality. Records are classified according to their confidentiality levels as "public, internal documents, confidential, and special categories of personal data." Special categories of personal data (e.g., health information, biometric data) are processed only with explicit consent or within the exceptions stipulated by law, and are retained with the highest security measures.

Public records refer to records which, if disclosed outside the Holding, would not negatively affect Cengiz Holding. The information in such documents does not violate data protection legislation and does not pose a reputational risk for the Holding. Information such as

newspapers, websites, brochures, leaflets, or published marketing research falls within this category.

Internal documents cover almost all records related to the Holding's activities. Unauthorised sharing of such records may pose a reputational risk to the Holding. Sharing is permitted only if it is essential for carrying out activities and with senior management approval. Examples include office documents, employee information, travel information, policies and procedures, and presentations.

Confidential records refer to documents containing commercial information relating to the Holding's activities. These records require a high level of caution, restricted access, and specific controls. Unauthorised disclosure of these records may constitute a legal violation. Such records may only be shared with employees and/or third parties on a need-to-know basis and in a manner appropriate to their purpose. Examples include third-party due diligence reports, committee reports, employee personal data, internal financial and commercial documents, and customer information.

4.2 Retention of Records

Cengiz Holding retains all information and documents obtained in the course of its operations for at least the periods specified in legislation, and for longer where necessary without creating a conflict with the law. Records whose retention period has expired must be deleted or destroyed. Where maximum retention periods are not prescribed by legislation, each unit may determine appropriate retention periods.

Retention periods are determined by taking into account the following:

- The period required for the specific data category,
- The duration of the legal relationship,
- The duration of the Holding's legitimate interest arising from the purpose of processing,
- The legal risks, costs, and responsibilities associated with retaining the data,
- The statutory limitation period for claims relating to the data.

Records are archived in groups according to date or category. Both physical and digital archives must be accessible only to authorised persons.

Physical records may be stored at Holding facilities or in a supplier archive, depending on need. If supplier archive services are used, due diligence must be conducted on the supplier by the procurement unit, contracts must clearly regulate confidentiality, access control, and data security matters, and archive areas must be periodically inspected. The supplier must have adequate protective measures in place against internal and external risks (e.g., fire, earthquake, flood, poor ventilation, theft). The supplier's security measures must also be checked periodically

4.3 Disposal of Records

All confidential and sensitive information recorded in physical or digital form must be securely disposed of when no longer needed, when retention periods expire, or upon the request of the data subject, in accordance with legal provisions.

As part of its daily operations, Cengiz Holding may record a large number of documents physically. The secure disposal of these records is highly important. Once the statutory retention periods of official records have expired, no special approval process is required for their disposal. Each unit is responsible for monitoring and disposing of the records it maintains within its remit. Units must review their records at least once a year to determine which retention periods have expired. In cases of uncertainty regarding statutory periods, the Legal Department must be consulted.

The disposal of physical records must be carried out securely, for example, through shredding, incineration, or authorised disposal companies.

For digital records, deletion from the device alone is not sufficient; irreversible methods must be used.

The date, method, and responsible unit for each disposal must also be documented and retained by the relevant department.

5. Roles and Responsibilities

All Cengiz Holding employees are required to comply with this Policy. If an employee witnesses a situation that conflicts with the rules set out in the Policy, the matter must be promptly reported to one of the following:

- Legal Department,
- Human Resources Department, or
- Information Technology Department

The Legal, Human Resources, and Information Technology Departments are jointly responsible for communicating the requirements of this Policy to employees and for establishing an internal control environment to ensure compliance. The Information Technology Department is additionally responsible for ensuring the digital security of records, maintaining access logs, and conducting regular checks.

In the countries where Cengiz Holding operates, if the legal regulations falling within the scope of this Policy are stricter than the provisions of the Policy, the relevant legal regulations shall apply.

Failure to comply with the Policy may result in various disciplinary sanctions for employees, including termination of employment.

6. Revision History

This Policy has been approved and enacted by the relevant Resolution of the Company's Board of Directors, and it is the joint responsibility of the Legal, Human Resources, and Information Technology Departments 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.