PERSONAL DATA RETENTION AND DESTRUCTION POLICY

I. INTRODUCTION

Law No. 6698 on the **Protection of Personal Data** (the "Law") entered into force on April 7, 2016 and governs the procedures and principles concerning the processing of personal data relating to identified or identifiable natural persons ("Data Subjects").

As CCN Hastane Hizmetleri ve İşletme Anonim Şirketi (the "Company"), we attach utmost importance to the lawful processing and protection of personal data under the Law and conduct all our activities in line with this approach. Within this scope, we take the necessary administrative and technical measures to protect personal data and ensure their security.

This Policy sets out the fundamental principles and procedures governing the processing, protection, retention, and destruction of the personal data of our employees, employee candidates, Company shareholders, Company officials, visitors, employees, shareholders, and officials of institutions with which we cooperate, and third parties.

Pursuant to Article 20 of the Turkish Constitution, every individual is entitled to request the protection of their personal data. The Company recognizes the protection of personal data as a fundamental right and, accordingly, considers personal data security an integral part of its corporate governance approach.

The fundamental principles we adopt in the processing of personal data under this Policy are as follows:

- Processing personal data in accordance with applicable law and the principles of good faith.
- Keeping personal data accurate and, where necessary, up to date.
- Processing personal data for specific, explicit, and legitimate purposes.
- Processing personal data that is relevant, limited, and proportionate to the purpose for which they are processed.
- Retaining personal data for the period prescribed in the applicable legislation or required for the purpose for which they are processed.
- Informing and notifying data subjects.
- Establishing the necessary mechanisms to enable data subjects to exercise their rights.
- Taking the necessary technical and administrative measures to ensure the security of personal data.
- Acting in compliance with applicable legislation and the decisions of the Personal Data Protection Board when transferring personal data to third parties.

- Exercising the necessary diligence in the processing and protection of special categories of personal data.

1. Purpose of the Policy

The purpose of this Policy is to inform personal data subjects about the obligations of the Company arising from Law No. 6698 on the Protection of Personal Data and the relevant legislation, as well as the principles, procedures, and rules adopted by the Company under the Law.

Accordingly, this Policy sets out the fundamental principles governing the processing, protection, retention, and destruction of the personal data of our employees, employee candidates, Company Shareholders, Company Officers, visitors, the employees, shareholders, and officers of institutions with which we cooperate, and third parties.

The Company aims to ensure full compliance with the applicable legislation in all activities relating to the processing and protection of personal data, safeguard the fundamental rights and freedoms of data subjects, and ensure the highest level of data security.

The purpose of the Personal Data Retention and Destruction Policy is to set out the procedures and principles governing the secure retention, deletion, destruction, and anonymization of personal data processed within the scope of activities carried out by the Company.

2. Scope of the Policy

This Policy covers all personal data of our Employees, Employee Candidates, Company Shareholders, Company Officers, Visitors, the Employees, Shareholders, and Officers of Institutions with which We Cooperate, and Third Parties, processed by fully or partially automated means or by non-automated means provided that they form part of a data recording system.

In this context, the Policy covers the collection, recording, storage, preservation, alteration, reorganization, disclosure, transfer, acquisition, making available, classification, prevention of use, deletion, destruction, and anonymization of personal data, as well as all administrative and technical measures taken to ensure the security of personal data.

3. Implementation of the Policy and Applicable Legislation

This Policy has been prepared to adapt the provisions of applicable legislation to the Company’s practices.

In the event of any discrepancy between the provisions of applicable legislation regarding the processing and protection of personal data and this Policy, the applicable legislation shall prevail.

The Company establishes the necessary systems to fulfill the obligations prescribed under the Law and applicable legislation and maintains its practices in compliance with current legislation.

4. Effective Date of the Policy

This Policy enters into force on the date it is approved by the Company.

The Policy is reviewed and updated as necessary. The current version is published on the Company's official website.

5. Definitions

The key terms used in this Policy are defined below:

- **Explicit Consent:** Refers to consent that is specific to a particular matter, informed, and freely given.
- **Anonymization:** Refers to rendering personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching it with other data.
- **Data Subject:** Refers to the natural person whose personal data is processed.
- **Relevant User:** Refers to the person who processes personal data within the data controller's organization or in line with the authorization and instructions given by the data controller.
- **Destruction:** Refers to the deletion, destruction, or anonymization of personal data.
- **The Law:** Refers to Law No. 6698 on the Protection of Personal 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 as defined in the Law.
- **Personal Data Processing Inventory:** Refers to the inventory that sets out the personal data processing activities of the data controller.
- **Personal Data Retention and Destruction Policy:** Refers to the policy setting out the principles governing the retention, deletion, destruction, and anonymization of personal data.
- **Board:** Refers to the Personal Data Protection Board.
- **Authority:** Refers to the Personal Data Protection Authority.

- **Periodic Destruction:** Refers to the deletion, destruction, or anonymization process carried out at recurring intervals when the conditions specified in the Law no longer exist.
- **Registry:** Refers to the Data Controllers' Registry (VERBIS).
- **Data Processor:** Refers to the natural or legal person that processes personal data on behalf of the data controller based on the authority granted by the data controller.
- **Data Recording System:** Refers to the recording system in which personal data is processed by being structured according to specific criteria.
- **Data Controller:** Refers to the natural or legal person who determines the purposes and means of processing personal data and is responsible for establishing and managing the data recording system.
- **Third party:** Refers to individuals who apply to the hospitals and integrated health facilities served by the Company for examination or treatment and receive outpatient or inpatient care.

2. PROTECTION OF PERSONAL DATA

As CCN Hastane Hizmetleri ve İşletme Anonim Şirketi, pursuant to Article 12 of Law No. 6698 on the Protection of Personal Data, we take the necessary technical and administrative measures to prevent the unlawful processing of and unlawful access to personal data and to ensure their secure preservation.

2.1. Security

The Company takes the necessary technical and administrative measures to ensure an appropriate level of security, taking into account technological developments, implementation costs, and the level of risk, in order to prevent the unlawful processing of personal data and unlawful access to personal data and to ensure their secure preservation.

2.2. Audit

The Company regularly conducts the necessary audits to ensure that activities relating to the protection of personal data are carried out in accordance with the provisions of the Law and the Company's policies and procedures.

Within this scope, internal audits are conducted, and independent audit mechanisms are also utilized where deemed necessary. Based on the audit results, the necessary actions relating to identified areas for improvement are planned and implemented.

2.3. Confidentiality

The Company takes the necessary technical and organizational measures to ensure

that employees and data processors involved in the processing of personal data do not disclose,

share personal data in violation of the provisions of the Law or use such data for purposes other than those for which they are processed.

Within this scope, employees receive regular training on the protection of personal data, information security, and confidentiality, and the necessary confidentiality undertakings are obtained from them.

2.4. Prevention of Unauthorized Access to Personal Data

The Company regularly implements access authorization, log monitoring, network security, system security, and information security controls to prevent unlawful access to personal data.

In the event of unlawful access to personal data, the incident is assessed without delay, and the notifications required under the Law are made to the Personal Data Protection Board and the relevant data subjects within the statutory time limits.

2.5. Protection of Data Subjects' Rights

The Company establishes the necessary administrative and technical infrastructure to enable data subjects to exercise their rights under Article 11 of the Law and ensures that applications are finalized in accordance with applicable legislation.

2.6. Protection of Special Categories of Personal Data

Data relating to individuals' race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, attire, association, foundation or trade union membership, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data, which are classified as special categories of personal data under the Law, are protected through enhanced security measures compared with other personal data.

The Company implements all necessary technical and administrative measures in the processing and storage of special categories of personal data in accordance with the Law, applicable legislation, and the decisions of the Personal Data Protection Board.

2.7. Ensuring the Security of Personal Data

The Company implements the following practices to ensure the security of personal data:

- The personal data processed and the relevant data categories are regularly analyzed, and risk assessments are conducted.
- The necessary technical and administrative security measures are implemented to mitigate or eliminate identified risks.
- Employees receive regular training on the protection of personal data and information security.

- Confidentiality undertakings are obtained from employees involved in personal data processing activities, and their compliance with security policies and procedures is monitored.
- Access authorizations to personal data are determined based on job descriptions and reviewed regularly.
- Personal data processing activities are logged, and access activity is monitored.
- Access controls are implemented in information systems in line with the principle **"Access is Prohibited Unless Authorized"**.
- Security solutions aligned with current technologies are used to ensure that personal data are stored in secure environments.
- Network, system, and user activities are regularly monitored; the necessary technical controls are carried out to enable the early detection of potential security breaches.

3. PERSONAL DATA DESTRUCTION POLICY AND RETENTION PERIODS

The Company retains personal data only for the periods prescribed in the applicable legislation or for as long as necessary for the purpose for which they are processed. Upon expiry of the retention period or when the legal grounds requiring the processing of personal data cease to exist, personal data are deleted, destroyed, or anonymized in accordance with the provisions of applicable legislation.

3.1. Reasons Requiring the Retention and Destruction of Personal Data

The Company processes personal data where one or more of the following legal grounds apply:

- The Data Subject's explicit consent has been obtained;
- It is explicitly provided for by law;
- The Data Subject is unable to provide explicit consent due to actual impossibility;
- It is directly related to the establishment or performance of a contract;
- It is necessary for the Company to fulfill its legal obligations;
- The Data Subject has made the personal data public;
- It is necessary for the establishment, exercise, or protection of a right;
- Processing of personal data is necessary for the legitimate interests of the Company.

Detailed information on the processing of personal data can be accessed through the **www.ccnholding.com Personal Data Protection Policy** available at this address.

The personal data of data subjects are deleted, destroyed, or anonymized during the first periodic destruction following the cessation of the conditions for processing personal data specified above.

All records relating to the deletion, destruction, and anonymization of personal data are created and retained for at least **three (3) years**.

3.2. Deletion, Destruction, and Anonymization of Personal Data

The Company deletes, destroys, or anonymizes personal data ex officio or upon the request of the data subject when the reasons requiring their processing cease to exist, in accordance with Article 138 of the Turkish Penal Code No. 5237, Article 7 of Law No. 6698, and the provisions of the Regulation on the **Deletion, Destruction, or Anonymization of Personal Data,** provided that the provisions of other laws are reserved.

All deletion, destruction, and anonymization activities carried out pursuant to Article 7 of the Regulation are documented, and such records are retained for at least **three (3) years**, provided that other legal obligations are reserved.

Deletion of Personal Data

Deletion of personal data refers to rendering the relevant data completely inaccessible, irretrievable, and unusable by the relevant users.

Prior to deletion:

- The personal data to be deleted are identified.
- The users authorized to access the relevant data are identified.
- The users' access, retrieval, and reuse authorizations are revoked.

Personal data in paper form are deleted using the **redaction method**. Redaction refers to rendering personal data invisible, using indelible ink or physical methods, in such a way that they cannot be recovered or read.

Personal data in electronic media are deleted using appropriate technical methods such as database commands (e.g., DELETE), operating system commands, or the removal of access authorizations.

Destruction of Personal Data

Destruction of personal data refers to the physical destruction of data storage media containing the data, such as documents, files, CDs, DVDs, magnetic media, hard disks, and similar media, in a manner that renders the data irretrievable and unusable.

The methods used within this scope include:

- Degaussing,
- Melting,
- Incineration,
- Pulverization,
- Processing through an industrial metal shredder,
- Physical destruction using paper

shredders.

Anonymization of Personal Data

Anonymization refers to rendering personal data incapable of being associated with an identified or identifiable natural person in any manner whatsoever, even when matched with other data.

For this purpose, anonymization techniques such as:

- Grouping,
- Masking,
- Derivation,
- Generalization,
- Randomization

may be used.

3.3. Methods for the Deletion, Destruction, and Anonymization of Personal Data

The Company applies technical methods in compliance with applicable legislation in the processes of deleting, destroying, and anonymizing personal data.

a) Methods for Deletion and Destruction of Personal Data

- **Physical Destruction:** Personal data stored in physical media that do not form part of a data recording system are physically destroyed in a manner that prevents them from being accessed or used again.
- **Sending to a Specialist for Secure Deletion:** Where deemed necessary, personal data are securely destroyed through individuals or organizations specializing in this field.

b) Anonymization Techniques

In accordance with Article 28 of the Law, anonymized personal data may be processed for purposes such as research, planning, and statistics. In such data processing activities, the data

subject’s explicit consent is not required, and anonymization methods approved by the Authority are applied.

3.4. Personal Data Retention and Periodic Destruction Periods

The Company retains personal data for the periods prescribed in the applicable legislation.

Where no specific retention period is prescribed by legislation, personal data are retained for as long as required for the purpose for which they are processed; once the retention obligation ceases, they are deleted, destroyed, or anonymized during the first periodic destruction process.

All records relating to the deletion, destruction, and anonymization of personal data are retained for at least **three (3) years**.

4. CATEGORIZATION OF DATA SUBJECTS AND MAPPING OF PERSONAL DATA

The data subjects whose personal data are processed by the Company are exclusively natural persons, pursuant to Article 3 of Law No. 6698 on the Protection of Personal Data.

For the proper management of personal data processing activities, data subjects are categorized as follows.

4.1. Categorization of Data

Subjects Employee Candidate

Refers to natural persons who have applied for a job with the Company through any means or have submitted their résumé and related information for the Company’s review.

Company Customer

Refers to natural persons who benefit from or have benefited from the products or services offered by the Company and whose personal data are processed within this scope.

Note: The current text contains two definitions of “Company Customer.” The first refers to “persons whose personal data are obtained through the Company,” while the second refers to “persons who use or have used the products and services.” These two definitions are repeated under the same heading.
The content may be left unchanged; however, from a corporate document perspective, it would be more appropriate to consolidate them under a single definition.

Company Business Partner / Shareholder, Authorized Representative, or Employee of Business Partners

Refers to natural persons with whom the Company has any type of commercial relationship, as well as the employees, shareholders, and authorized representatives of natural or legal persons that are business partners, suppliers, or otherwise have a business relationship with the Company.

Potential Customer

Refers to natural persons who have shown interest in the Company's products and services, requested to benefit from them, or are assessed, pursuant to commercial practice and good-faith principles, as potentially having such interest.

Company Employee

Refers to natural persons employed by the Company and its subsidiaries.

Company Shareholder

Refers to natural persons who are shareholders of the Company and its subsidiaries.

Company Official

Refers to members of the board of directors and other authorized natural persons of the Company and its subsidiaries.

Third Party

Refers to natural persons who do not fall within the scope of the Company policies prepared for Company Employees and who do not fall under any of the other data subject categories defined in this Policy.

For example, patients, companions, and similar persons are considered within this scope.

Visitor

Refers to all natural persons who visit the Company's physical premises for any purpose or use our websites.