FLORENCE NIGHTINGALE
PERSONAL DATA PROTECTION POLICY

Grup Florence Nightingale Hastaneleri A.Ş., Göktürk Florence Nightingale Tıp Merkezi A.Ş., Florence Nightingale Tıp Merkezi A.Ş., Istanbul Florence Nightingale Hastanesi A.Ş., Fulya Sağlık Tesisleri ve Tic. A.Ş (hereinafter collectively referred to as **"Florence Nightingale"**) undertake to comply with the principles and rules introduced by the Constitution of the Republic of Türkiye, the Personal Data Protection Law No. 6698 (**"PDPL"**) and other legislation regarding the protection of personal data and to protect the rights and freedoms of the relevant persons whose personal data it processes.

Accordingly, Florence Nightingale has adopted this Personal Data Protection Policy (**"Policy"**) to be implemented and developed in order to determine the procedures and principles to be followed in fulfilling its legal obligations regarding the protection and processing of personal data.

This Policy aims to ensure that Florence Nightingale establishes its own standards in the management of personal data and achieves them; to determine and support organizational goals and obligations within this scope, to fulfill the obligations that Florence Nightingale is subject to in accordance with international contracts, the Constitution, laws, contracts and professional rules concerning protection of personal data, and to securely protect the fundamental rights and freedoms of individuals.

1. Definitions

The definitions of the terms included in the Policy are as follows:

Explicit consent	**:** Refers to consent given solely for a specific subject, based on information and free will, with clarity leaving no room for doubt, and limited exclusively to that transaction,
Anonymization	**:** Refers to rendering personal data in such a way that it can no longer be associated with an identified or identifiable natural person under any circumstances, even when matched with other data,
Employee	**:** Refers to the Florence Nightingale personnel,
Employee candidate	**:** Refers to people who have applied for a job with Florence Nightingale,
Electronic media	**:** Refers to media where personal data can be created, read, changed and written using electronic devices,
Physical Media	**:** Refers to all written, printed, visual, etc. media other than electronic media,
Relevant Person	**:** Refers to natural persons whose personal data is processed,

Personal data	**:** Refers to any information regarding an identified or identifiable natural person,
Processing of Personal Data	**:** Refers to any processing of personal data, whether fully or partially by automatic means or, provided that it is part of a data recording system, by non-automatic means, such as obtaining, recording, storing, retaining, altering, rearranging, disclosing, transferring, acquiring, making available of, classifying, or preventing the use of the data,
PDP Board	**:** Refers to Personal Data Protection Board,
Sensitive personal data	**:** Refers to data regarding individuals' race, ethnic origin, political views, philosophical beliefs, religion, sect or other beliefs, appearance and dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, as well as biometric and genetic data,
Data controller	**:** Refers to a natural person or legal entity who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

2. Scope

2.1 Scope in terms of subject matter

Information relating to an identified or identifiable natural person is considered personal data for the purposes of the implementation of this Policy. Without prejudice to the special provisions in legal regulations, the protection, processing and use of all kinds of personal data in electronic or physical media constitute the scope of this Policy in terms of subject matter. Florence Nightingale undertakes to comply with personal data protection legislation and data protection principles.

The principles adopted by Florence Nightingale include, in particular:

- Respecting the privacy and confidentiality of individuals,
- Processing personal data only if it is clearly necessary for legitimate corporate purposes,
- Processing the minimum amount of personal data necessary for these purposes and not processing more data than necessary,
- Providing information to individuals about how and by whom their personal data is processed,
- Processing only personal data that is relevant and appropriate for the intended use,
- Processing personal data in accordance with equity and law,
- Keeping personal data accurate and updated when necessary,
- Storing personal data only for as long as required by legal regulations, Florence Nightingale's legal obligations or legitimate corporate interests,

- Respecting the rights of individuals in relation to their personal data, including the right of access,
- Keeping personal data in strict security and confidentiality,
- Identifying personnel with specific authority and responsibilities related to the implementation of the Policy.

2.2. Scope in terms of person

Florence Nightingale, as a legal entity, is covered by this Policy as a data controller.

Florence Nightingale's managers at all levels; employees, employee candidates, service providers, visitors and other third parties listed below are covered by this Policy as natural persons. Explanations regarding these persons are made in Article 12 of the Policy.

2.3. Scope in terms of time

The Policy is published on Florence Nightingale's website and remains in effect for an indefinite period of time. It reserves the right to make changes and/or updates to the Policy in parallel with legal regulations and functioning.

3. Legal obligations

The legal obligations of Florence Nightingale as the data controller within the scope of protection and processing of personal data are listed below:

3.1. Obligation of clarification

Florence Nightingale has an obligation to inform the Relevant Person on the following matters;

- For what purpose personal data will be processed,
- Information about the Company's trade name,
- To whom and for what purpose personal data may be transferred,
- The method of data collection and the legal reason and
- Rights of the Relevant Person arising from the PDPL when collecting personal data as the data controller.

The Company must fulfill this obligation through the unit that obtains the personal data in question from the Relevant Person. Each unit should identify the personal data collection channels in its own workflow and design appropriate processes by informing the Relevant Persons with clarification points and texts with the guidance of the PDP Committee (continuous posting of clarification texts at workplaces, informing employee candidates during application processes, etc.). The Company must take care to ensure that the Policy is understandable and easily accessible and design the method (written notification, e-mail, etc. against signature) in accordance with the workflow of the units and employees involved in the processing of personal data. The obligation of clarification is fulfilled through Florence Nightingale's website, employee portal, boards in the physical premises or printed or electronic information texts belonging to the relevant groups of people.

3.2. Obligation to ensure data security

The Company, as the data controller, must take the administrative and technical measures stipulated in the legislation to ensure the security of the personal data it processes. The obligations and measures taken regarding data security are explained in detail in Article 16 of the Policy.

4. Classification of personal data

4.1. Personal data

The protection of personal data relates only to natural persons and information belonging to legal entities that does not contain information about natural persons is excluded from personal data protection. For this reason, this Policy does not apply to data belonging to legal entities. The policy applies to information directly referring to a person, such as a person's name, surname, Turkish ID number, as well as information that indirectly identifies the relevant person, such as height, weight, educational status.

4.2. Sensitive personal data

Personal data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data are sensitive personal data. Sensitive personal data are also subject to the provisions of this Policy.

5. Data protection principles

All personal data processing activities must be carried out in accordance with the following data protection principles. Florence Nightingale's policies and procedures aim to ensure compliance with these principles:

- ***Being in compliance with the law and the rules of honesty***

Florence Nightingale takes into account the interests and reasonable expectations of relevant persons when trying to achieve its objectives in data processing; in other words, it acts in a way that prevents the occurrence of consequences that the relevant person does not expect and should not expect.

- ***Being accurate and up to date when necessary***

Florence Nightingale keeps channels open to ensure that the relevant person's information is accurate and up-to-date. In order to ensure that personal data is kept accurate and up-to-date; the sources from which personal data is obtained are identified, care is taken to ensure that the source from which personal data is collected is accurate, requests arising from inaccurate personal data are carefully examined and reasonable measures are taken in this context. The accuracy and up-to-dateness of the data kept on personnel is the responsibility of the relevant personnel.

- ***Processing for specific, clear and legitimate purposes***

Florence Nightingale has clearly and precisely determined the purposes of data processing and confirms that these purposes are legitimate. Personal data shall not be used for purposes other than those specified to the relevant person.

- ***In connection, limited and proportionate with the purposes for which they are processed***

Florence Nightingale undertakes that the personal data processed are suitable for the realization of the specified purposes and that it does not process personal data that are not related to or needed for the realization of the purpose.

- ***Storing for the period stipulated in the relevant legislation or required for the purpose for which they are processed***

Florence Nightingale takes the necessary administrative and technical measures to ensure that personal data are stored for the period necessary for the purpose for which they are processed.

Accordingly, Florence Nightingale shall comply with the period stipulated in the legislation for the relevant personal data; if no such period is stipulated, Florence Nightingale shall store the data only for the period necessary for the purpose for which they are processed. If there is no valid reason for further storage of a data, that data will be deleted, destroyed or anonymized. It will not be possible to store personal data on the grounds that it may be reused in the future or for any other reason.

6. Purposes of data processing

The purposes for processing personal data within Florence Nightingale are determined in accordance with the data protection principles and the use of personal data for purposes other than those specified and the processing of personal data for discriminatory purposes are strictly prohibited.

The purposes for which personal data is processed within Florence Nightingale are as follows:

- To contact and fulfill requests within the scope of forms filled out on the website,
- To contact as part of the offered services,
- To meet appointment requests,
- To provide appointment reminders, changes and other information regarding the provision of the service,
- To provide the requested health service,
- To provide medical diagnosis, treatment and care services,
- To perform requested remote examinations or home healthcare procedures, to share the necessary information with business partners to provide these services and to confirm legal contact with contracted institutions,
- To ensure that the results of the procedures performed in the hospital are displayed,
- To plan and execute patient relationship management processes,
- To meet requests and applications, respond to them and resolve problems,
- To perform the processes related to the presentation and execution of products and services,

- To inform about campaigns and notifications, to perform advertising and promotional activities, to carry out organization procedures such as openings, invitations and celebrations,
- To send important information about changes to terms of service, changes to electronic services and other administrative information,
- To provide quality, training and safety improvement (for example, in relation to recorded or monitored phone calls to our contact numbers),
- To resolve complaints and process requests for data access or correction,
- To prevent, detect and investigate crimes and analyze and manage other business risks,
- To comply with applicable laws and regulatory obligations (including those outside your country of residence); comply with due process of law; and respond to requests from public authorities and governmental authorities (including those outside your country of residence),
- To fulfill legal obligations,
- To manage infrastructure and business operations and comply with internal policies and procedures, including those in connection with auditing, finance and accounting; billing and collections, IT systems, data and website hosting, business continuity and records, document management,
- To identify and defend legal rights; to protect our activities or the activities of our business partners, our rights, our privacy, our security,
- To keep patient records,
- To make notifications to relevant institutions and organizations as required by legislation regarding events such as birth, death, and judicial cases within the scope of the provided healthcare services,
- To conduct job application, interview and recruitment processes,
- To perform transfer procedures,
- To perform private health insurance processes and provision transactions,
- To defend the company's rights in legal disputes and conflicts,
- To create and track visitor records,
- To carry out management operations,
- To carry out talent/career development operations,
- To conduct work and residence permit procedures for international personnel,
- To ensure the security of data controller operations,

- To carry out the marketing processes of products and services,
- To carry out the wage policy,
- To carry out the supply chain management process,
- To ensure the security of movable goods and resources,
- To carry out contract processes,
- To carry out storage and archive operations,
- To carry out performance evaluation processes,
- To carry out organization and event processes,
- To carry out activities aimed at customer satisfaction,
- To carry out customer relationship management processes,
- To carry out goods, services production and operation processes,
- To carry out the purchasing processes of goods and services,
- To carry out logistics operations,
- To ensure business continuity,
- To receive and evaluate suggestions for improving business processes,
- To carry out occupational health and safety operations,
- To carry out and supervise business operations,
- To plan human resources processes,
- To carry out communication operations,
- To carry out internal audit, investigation and intelligence operations,
- To ensure the follow-up and execution of legal affairs,
- To carry out assignment processes,
- To ensure the security of physical space,
- To ensure that activities are carried out in accordance with legislation,
- To carry out access authorizations,
- To carry out training operations,
- To carry out audit and ethics activities,
- To carry out the fringe benefits and interest processes for employees,

- To fulfill the obligations of employees arising from employment contracts and legislation,
- To carry out employee satisfaction and loyalty processes,
- To carry out the selection and placement processes of employee candidates/students/interns,
- To carry out information security processes,
- To carry out emergency management processes.

Your personal data, limited to the personal data categories listed above, are processed in accordance with articles 5 and 6 of the PDPL.

7. Processing of personal data collected within the scope of wireless network access

Wireless internet service is provided within the Company and Florence Nightingale is defined as "Internet Mass Use Provider" within the scope of the service in question. Pursuant to the legislation, internet mass use providers are obliged to record access records electronically in their own systems and store them for two years.

IP address information, start and end time of use, MAC address, destination IP address, port information and mobile phone number information of the Relevant Persons who want to use the internet service within Florence Nightingale are processed.

The Company may collect, transfer, store and otherwise process personal data through cookies on its website. The cookie policy, which includes detailed information and necessary warnings regarding the cookies used on Florence Nightingale's website, is available on the website.

8. Processing of personal data within the scope of ensuring general security

The Company may process the personal data of visitors, employees, interns and subcontractor employees for the purposes of ensuring the security of the physical space and carrying out the activities in accordance with the legislation. In this context, if the Company obtains the camera images of the persons in its facilities through CCTV (closed circuit camera recording systems), it stores these records for the periods stipulated by the relevant legislation and deletes, destroys and anonymizes them in accordance with the Data Storage and Destruction Policy. In order to fulfill the clarification obligation arising from this data processing activity, the Company may publish a clarification text or post a notification letter regarding the monitoring/visitor registration at the entrances of the areas where monitoring and registration are carried out.

In order for the data processing activity to be in compliance with the principles set out in the PDPL, the monitoring areas, the number and the time of monitoring of the security cameras are implemented as sufficient to achieve the security purpose and limited to this purpose (for example, building entrances and exits and areas such as the data room where the entrance and exit must be controlled). Areas that may result in interference with a person's privacy in excess of security purposes (e.g. toilets) are not subject to monitoring. Only a limited number of employees have access to live camera footage and digitally recorded and stored records.

9. Method and legal reason for collecting personal data

Florence Nightingale collects your personal data through the creation of your patient record and submission of information-documents by you or through intermediary organizations, recording your personal data through the systems in our hospital, obtaining your personal data from the Ministry of Health systems and recording your personal data within the scope of the health services provided. In addition, if you disclose your personal data by contacting our Hospital by other methods, personal data can also be obtained in this context.

It is processed in accordance with the general principles listed in Article 4 of the PDPL and within the scope of the data processing purposes listed in Article 6 of this Policy within the personal data processing conditions specified in Articles 5 and 6. However, if none of the exceptions for the processing of personal data is in question; only then, explicit consent shall be obtained from the Relevant Person.

10. Data processing tools

Data processing tools are the physical media and information processing systems used for physical or electronic recording, storage and processing.

In terms of the implementation of this policy, information in the nature of personal data contained in documents or annexes such as contracts, correspondence, etc., which are physically or electronically transmitted to our company without the purpose of data processing, shall be subject to the provisions of this policy from the moment they are separated from the integrity of the original document for any purpose and subjected to a process in physical or electronic environment.

11. Processed personal data categories

Identity Information	Name, surname, Turkish ID number, passport number or temporary Turkish ID number, place and date of birth, marital status, gender and other information included in the identity document
Contact Information	E-mail address, mobile phone number and address
Personnel	Payroll information, disciplinary investigations, employment entry and exit document records, resume information, performance evaluation reports
Legal Process	Information in correspondence with judicial authorities, information in the case file
Customer Transaction Information	Call center records, invoice, promissory note, check information, service information and other information within the scope of your contact with us as a patient
Financial Information	Bank account information, credit card information, information about your invoices

Physical Space Safety	Camera footage recorded during hospital visits
Legal Process Information	Correspondence with judicial authorities
Transaction Security	Navigation information, IP address, browser information obtained during website or mobile application use, and medical documents, surveys, forms sent with consent
Risk management	Information processed to manage commercial, technical and administrative risks
Finance	Balance sheet information, financial performance information, credit and risk information, asset information
Occupational Experience	Diploma information, courses taken, vocational training course information, certificates, transcript information
Marketing	Information obtained through surveys, cookie records, and campaign studies
Audio-Visual Recordings	Photos, call center calls, remote examination footage
Philosophical Belief, Religion, Sect and Other Beliefs	Information about philosophical beliefs, religion, sect and other beliefs
Appearance	Information about appearance
Association, Foundation and Union Membership	Information about association, foundation and union membership
Health Information	Health data obtained while performing medical diagnosis, treatment and care services, and past health data provided by you, especially appointment information, examination information, prescription information, laboratory results

Sexual Life	Data on sexual life obtained while performing medical diagnosis, treatment and care services
Criminal Conviction and Security Measures Information	Criminal record
Biometric Data	Fingerprint information
Genetic Data	Genetic data obtained while performing medical diagnosis, treatment and care services
Other	Vehicle license plate information in the event of entering the car park

12. Personal data subjects

Shareholder/Partner	Florence Nightingale natural person shareholders
Company officials	Florence Nightingale's board members and other authorized natural persons
Reference	Someone who has knowledge about a relevant person's competencies, skills, and sense of responsibility based on previous work or involvement in a project
Patient Relative	Relatives of the person who received health care from Florence Nightingale
Event participant	People who participated in events organized by Florence Nightingale
Test subject	Volunteers who were experimented on
Person mentioned in news	Person about whom news has been made

Employees	Natural persons working at Florence Nightingale under employment contracts and other private law contracts
Employee candidate	Natural persons who have applied for a job with Florence Nightingale by any means or who have made their CV and related information available for review by companies
Intern	Natural persons who are working as interns at Florence Nightingale
Supply executive and supplier employee	Persons from whom goods and services are supplied for data processing purposes and their employees
Customer	Natural persons who use or have used the products and services offered by the companies, regardless of whether they have any contractual relationship with Florence Nightingale
Potential Customer	Natural persons who have requested or shown interest in using Florence Nightingale's products and services, or who have been assessed in accordance with commercial practices and rules of good faith as potentially interested
Parent/Guardian/Representative	Information on the parents, guardians and representatives of natural persons whose personal data is processed within Florence Nightingale
Visitor	All natural persons who enter Florence Nightingale's physical premises for various purposes or visit its websites or social media accounts for any purpose

13. Transfer of personal data

Florence Nightingale, for the purposes of processing personal data and by taking necessary security measures, may transfer the personal data and sensitive personal data of the data subject to its business partners, distributors, agents, representatives, and similar entities and organizations within the scope of legal relationships in Türkiye. Regarding the transfer of personal data, the regulations stipulated in the PDPL and the decisions taken by the PDP Board are followed.

14. Recipients to whom personal data is transferred

Recipient Groups	Description	Transfer Purpose
Business Partners and Suppliers	Natural persons and legal entities who are third parties from whom goods and services are supplied or	Carrying out the purchase-sale and contract processes of the product or service to be supplied from/to the supplier

	to whom goods and services are offered in line with data processing purposes	
Shareholders	Florence Nightingale's shareholders	Management and execution of business operations
Authorized Public Institutions and Organizations	Public institutions and organizations authorized to receive information and documents from Florence Nightingale within the scope of relevant legal regulations	Carrying out operations in accordance with the legislation, fulfilling obligations, and providing information to authorized persons, institutions and organizations within the scope of the relevant legal regulation
Group companies	Group companies with which Florence Nightingale has legal relations	Florence Nightingale being able to continue its activities
Natural persons or legal entities of private law	All natural persons or private law entities to whom Florence Nightingale transfers personal data within the scope of legal relationships	Within the scope of the activities carried out by Florence Nightingale, the follow-up and execution of legal affairs, and the execution of fringe benefits and interest processes for employees

15. Distribution of responsibilities and duties

The titles, units and job descriptions of those involved in ensuring the security of personal data and in the storage and destruction processes are as follows:

Title	***Unit or Branch***	***Duty***
PDP Committee Members	PDP Committee	Following of all necessary regulations for compliance with personal data protection legislation, ensuring the implementation of the Policy, following required updates, and providing recommendations for improvements within the scope of the legislation.
Members of the Board of Directors	Board of Directors	Carrying out the PDPL compliance process.
Director of Information Technologies	Information Technology Unit	Providing and implementing the technical solutions needed in the implementation of the Policy.
HR, Legal, Financial Affairs	Other Units	Execution of the Policy in accordance with their duties

The deletion, destruction and anonymization of data are performed only by the unit authorized for such operation(s).

16. Security of personal data

16.1. Obligations regarding the security of personal data

Florence Nightingale is responsible for taking administrative and technical measures, taking technological capabilities and implementation costs into consideration, to prevent the unlawful processing of personal data, prevent unauthorized access to personal data, and ensure the lawful storage of personal data.

16.2. Measures taken regarding data security

In accordance with Article 12 of the PDPL, Florence Nightingale takes necessary technical and administrative measures to ensure an appropriate level of security to prevent unlawful processing of personal data it processes, unauthorized access to data, to ensure the appropriate level of security to ensure the preservation of data and to ensure the lawful destruction of personal data, and to carry out or have the necessary audits carried out within this scope.

In the event that personal data is unlawfully obtained by third parties, Florence Nightingale operates a system that ensures the notification of the relevant Data Subject and the PDP Board, using the Violation Notification Form.

The administrative and technical measures taken in this context are stated below:

- Network security and application security are provided.
- Network security and application security are provided.
- A closed system network is used for personal data transfers performed via the network.
- Security measures are taken regarding supply, development and maintenance of the information technology systems.
- The security of personal data stored in the cloud is ensured.
- There are disciplinary regulations in place for employees that include data security provisions.
- Training and awareness operations on data security are performed for employees at regular intervals.
- Access logs are kept regularly.
- Corporate policies on access, information security, usage, storage and destruction have been prepared and implemented.
- Data masking measures are applied when necessary.
- Confidentiality commitments are made.

- The authority of employees who are reassigned or leave their jobs is revoked in this area.
- Up-to-date antivirus systems are used.
- Firewalls are used.
- The signed contracts contain data security provisions.
- Extra security measures are taken for personal data transferred via paper, and the relevant documents are sent in a confidential document format.
- Personal data security policies and procedures have been determined.
- Personal data security issues are reported quickly.
- Follow-up on personal data security is performed.
- Necessary security measures regarding entry and exit to physical environments containing personal data are taken.
- The security of physical environments containing personal data is ensured against external risks (fire, flood, etc.).
- The security of environments containing personal data is ensured.
- Personal data is minimized as much as possible.
- Personal data is backed up and the security of the backed up personal data is also ensured.
- User account management and authorization control systems are implemented and also monitored.
- In-house periodic and/or random audits are carried out and commissioned.
- Log records are kept without user intervention.
- Current risks and threats have been identified.
- Protocols and procedures for the security of sensitive personal data have been determined and implemented.
- If sensitive personal data is to be sent via e-mail, it must be encrypted and sent using a KEP or corporate mail account.
- Secure encryption/cryptographic keys are used for sensitive personal data and are managed by different units.
- Hacking detection and prevention systems are used.
- Leak test is performed.
- Cyber security measures have been taken and their implementation is constantly monitored.

- Encryption is performed.
- Sensitive personal data transferred via portable memory, CD or DVD are transferred with encryption.
- Data processing service providers are audited periodically regarding data security.
- Data loss prevention software is used.

17. Obligation of confidentiality

Confidentiality commitments and obligations are specifically included in contracts containing personal data, including employment contracts and supply contracts, regarding the confidentiality of personal data.

18. Recording medium

Personal data recording mediums can be physical or electronic environments and visual environments such as camera recordings. In this context, the recording mediums containing personal data are electronic mediums such as servers (e-mail, databases, etc.); software, information security devices (firewalls, antivirus, etc.); personal computers (desktop, laptop); mobile devices (phones); and physical environments such as files, folders, paper, written, printed, and visual media (cameras).

19. Maximum period required for the purposes for which personal data is processed

We undertake to store your personal data for the period necessary to fulfill the purpose to be achieved, to meet your needs or to fulfill our legal obligations.

This period is a maximum of ten (10) years under the general statute of limitations. Personal data related to commercial works and operations performed by our company are stored for a period of 10 years in principle, in accordance with Article 82 of the Turkish Commercial Code, unless legal or contractual obligations require a longer period. For actions and activities other than this, the general statute of limitations period of 10 years determined by Article 146 of the Turkish Code of Obligations shall be taken as basis.

However, the storage period may be shorter. When determining this period (storage period), we take into account the following aspects in particular:

- The duration of your contract;
- The time required to process your claim or complaint;
- Your interest in our hospital;
- The need to keep a record of your interactions with us to effectively manage patient processes and
- The time needed for our legal obligations

Personal data of employee candidates applying for Florence Nightingale open positions are stored for one (1) period in accordance with the principle of keeping personal data accurate and up-to-date.

While the personal data of Florence Nightingale personnel are kept for the duration of the general statute of limitations period, personal data including in the category of health information, which is considered as sensitive personal data, is kept for 15 years in order to fulfill occupational health and safety obligations.

Personal data that may be used as evidence in a financial, legal or criminal dispute shall be stored in accordance with the statute of limitations stipulated in the relevant legal regulations in order to constitute evidence in possible legal disputes or to assert the relevant right related to personal data or to establish a defence. In this case, stored personal data is not accessed for any other purpose and access is provided only when it is necessary to use it in the relevant legal dispute.

When we no longer need to use your personal data, it will be deleted from our systems and records or it will be anonymized so that we cannot identify you.

20. Destruction periods

The periodic destruction period is determined as 6 months, provided that it is at least twice a year. Within the scope of Article 13 above, destruction operations will be carried out at the latest during the first periodic destruction period following the end of the storage periods.

21. Methods of destruction of personal data

At the end of the storage period required for the period stipulated in the relevant legislation or for the purpose for which they are processed, personal data are destroyed ex officio or upon the request of the data subject, in accordance with the provisions of the Law, using the techniques specified below.

21.1 Deletion, destruction or anonymization of personal data

Without prejudice to the provisions of other laws regarding the deletion, destruction or anonymization of personal data, if the reasons requiring the processing of data are eliminated, the personal data is deleted, destroyed or anonymized ex officio or upon the request of the data subject.

With the deletion of personal data, these data are destroyed in such a way that they cannot be used and recovered in any way. Accordingly, personal data are deleted from the tools such as documents, files, CDs, floppy disks in which they are stored in such a way that they cannot be recovered. Destruction of Personal Data, on the other hand, refers to the destruction of materials suitable for data storage, such as documents, files, CDs, floppy disks, where the data are stored, so that the information cannot be recovered and used again. By anonymizing the data, it is meant that personal data cannot be associated with an identified or identifiable natural person, even if it is matched with other data.

Records of operations carried out to delete, destroy or anonymize personal data are kept for at least 3 (three) years, without prejudice to other laws and regulations. Florence Nightingale chooses the appropriate method of deleting, destroying or anonymizing personal data, unless otherwise specified by the PDP Board. If requested by the Relevant Person, the appropriate method is selected by explaining the reason.

22. Rights of the relevant person

Within the scope of the obligation of clarification, the Company informs the Relevant Person about the rights granted to him/her under the PDPL and listed below and establishes the necessary systems and infrastructures regarding this information. It makes the technical and administrative arrangements necessary for the Relevant Person to exercise his/her rights regarding personal data.

Relevant Person has rights listed below regarding person's personal data:

- To learn whether personal data has been processed or not,
- To request information regarding the processing of personal data, to learn the purpose of processing personal data and whether they are used in accordance with the stated purpose,
- To know the third parties to whom the personal data is transferred, domestically or abroad,
- To request the correction of personal data in case of incomplete or incorrect processing,
- To request the deletion or destruction of personal data within the framework of the conditions stipulated in Article 7 of the PDPL (within the scope of the provisions regarding the deletion, destruction or anonymization of personal data),
- To request notification of the actions taken under subparagraphs (d) and (e) (actions taken under the scope of correction, deletion or destruction of personal data) to third parties to whom personal data have been transferred,
- To object to the occurrence of any unfavorable consequences resulting from the analysis of personal data exclusively by automated systems,
- To claim compensation for damages in case of unlawful processing of personal data.

Personal data subjects have the right to apply to Florence Nightingale with the necessary information and documents to establish their identity and an explanation of which right they wish to exercise. Florence Nightingale will finalize the request free of charge as soon as possible and no later than thirty days, according to the nature of the request. However, if the process incurs an additional cost, a reasonable fee may be charged.

In case the application is rejected, the response is found insufficient or the response is not given in a timely manner, the applicant has the right to complain to the PDP Board within 30 (thirty) days from the date of learning the response and in any case within 60 (sixty) days from the date of application.

23. Publication and storage of the policy

This policy was approved by the Board of Directors on the date of publication and published with the signature of the General Manager.

The current version of this document is available to all Florence Nightingale personnel and is published on the company website.

24. Update and enforcement of the policy

The policy is reviewed regularly and updated if deemed necessary. Each update made is considered to have entered into force after its publication.