



PERSONAL DATA RETENTION AND DESTRUCTION POLICY

Version Dated: 10/12/2022

Contents

1.	
INTRODUCTION.....	2
1.1 Objective	2
1.2 Scope.....	2
1.3 Abbreviations and Definitions.....	2
2. RESPONSIBILITY AND ALLOCATION OF DUTIES.....	4
3. RECORDING MEDIUMS.....	5
4. EXPLANATIONS ON RETENTION AND DESTRUCTION	5
4.1 Explanations on Retention	5
4.1.1 Legal Grounds Requiring Retention.....	6
4.1.2 Processing Purposes Requiring Retention.....	6
4.2 Grounds Requiring Destruction.....	8
5. TECHNICAL AND ADMINISTRATIVE MEASURES.....	8
5.1 Technical Measures.....	8
5.2 Administrative Measures.....	8
6. METHODS FOR DESTRUCTION OF PERSONAL DATA.....	8
6.1 Erasure of Personal Data	8
6.2 Destruction of Personal Data.....	9
6.3 Anonymization of Personal Data.....	10
7. RETENTION AND DESTRUCTION PERIODS.....	10
8. PERIODIC DESTRUCTION INTERVALS.....	14



9. POLICY'S PUBLICATION AND SAFEKEEPING.....	14
10. POLICY'S UPDATE INTERVAL.....	14
11. EFFECTIVENESS AND REPEAL OF THE POLICY	14

1. INTRODUCTION

1.1 Purpose

According to article 20 ("Right to Privacy") of the T.R. Constitution, everyone has the right to request the protection of personal data pertaining to themselves. This right covers the right to be informed about personal data pertaining to such person, to access such data, to request that such data be corrected or erased and to discover whether such data is being used in line with its purpose.

As the Personal Data Protection Law no. 6698 published in the Official Gazette dated 07 April 2016 and numbered 29677 (the "Law") protects the fundamental rights and freedoms of persons, in particular their right to privacy in the processing of personal data, and sets forth the obligations of and rules and principles applicable to natural persons and legal entities processing personal data, this Personal Data Retention and Destruction Policy (the "Policy") has been prepared with the aim of establishing the principles and procedures to be applied with respect to the retention and destruction of personal data processed by **YEŞİL SİYAH DENİZCİLİK LOJİSTİK LİMİTED ŞİRKETİ** ("Company"). Within this context, all acts and actions taken with respect to the retention and destruction of personal data must be carried out in line with the Policy.

1.2 Scope

The personal data of "Company employees, potential employees, lecturers, employees of the group companies, business partners, references, employees of suppliers, officers of suppliers, persons who purchase products or services, directors, visitors and other persons" fall under the scope of this Policy and all personal data processing recording mediums owned or managed by the Company as well as all activities aimed at processing personal data fall under the scope of this Policy.

1.3 Abbreviations and Definitions

- Recipient Group: Category of natural persons or legal entities to whom personal data is transferred by the data controller.
- Explicit Consent: Freely given, specific and informed consent.
- Anonymization: Rendering personal data impossible to link with an identified or identifiable natural person, even by matching such personal data with other data.
- Employee: Company employees.
- Digital Medium: All media on which personal data can be created, read, changed and written by means of electronic devices.
- Non-Digital Medium: all other written, printed, visual, etc media outside of digital media.
- Data Subject: Natural person whose personal data is being processed.
- Concerned User: Persons who process personal data within the organization of the data controller or upon authorization and instructions received from the data controller, other than the person or department responsible for the technical storage, protection and back up of personal data.
- Destruction: Deletion, erasure, or anonymization of personal data.
- Law: Personal Data Protection Law no. 6698.
- Recording medium: Any type of environment that keeps personal data processed wholly or partially by automated means or through non-automated means provided that it is part of a data filing system.
- Personal Data: Any information relating to an identified or identifiable natural person.
- Personal Data Processing Inventory: Inventory describing in detail the personal data processing activities of data controllers in connection with their business processes; purpose of and legal grounds for the personal data processing; data category; maximum data retention period required for the purposes for which the data is processed in connection with the data subject groups and with the recipient group to whom the data are transferred; personal data expected to be transferred to foreign countries; and measures taken with respect to data security.
- Processing of Personal Data: Any operation which is performed on personal data, wholly or partially by automated means or non-automated means provided that it is part of data filing system, such as the collection, recording, storage, retention, alteration, adaptation, disclosure, transfer, retrieval, acquisition, making available, categorization, or preventing the use thereof.
- Board: Personal Data Protection Board
- Sensitive Data: Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership in associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and biometric and genetic data.
- Periodic Destruction: Erasure, destruction, or anonymization process specified in the personal data retention and destruction policy which is to be carried out at regular



intervals ex officio in the event that all of the conditions for processing laid down in the Law cease to exist.

- Policy: Personal Data Retention and Destruction Policy.
- Supplier: Natural person or legal entity who supplies services under the framework of a specific contract with the Company.
- Data Processor: Natural person or legal entity who processes the personal data on behalf of the data controller based on authority granted by the data controller.
- Data Filing System: System where personal data are processed by being structured according to specific criteria.
- Data Controller: natural person or legal entity who determines the purposes for and means of processing personal data and is responsible for the establishment and management of the data filing system – **Company**
- Data Controllers' Registry Information System: Information system created and managed by the Presidency and accessible online for use by data controllers when registering with the Registry and with respect to other actions before the Registry.
- Regulation: Regulation on the Erasure, Destruction or Anonymization of Personal Data.

2. RESPONSIBILITY AND ALLOCATION OF DUTIES

All Company departments and employees actively support the concerned departments with implementing technical and administrative measures enacted within the context of the Policy as required, preventing the unlawful processing of personal data by increasing, monitoring and constantly checking the training and awareness of employees, preventing unlawful access to personal data and ensuring lawful retention of personal data with the aim of ensuring data security in all media on which personal data is processed.

The titles, departments and duty descriptions of those assigned to personal data retention and destruction procedures have been set forth in Table 1.

Table 1: Allocation of duties for retention and destruction procedures:

TITLE	DEPARTMENT	DUTY

--	--	--

3.RECORDING MEDIUMS

The Company lawfully and securely stores personal data on the media listed in Table 2 below.

Table 2: Personal data storage media

DIGITAL MEDIA	NON-DIGITAL MEDIA
<ul style="list-style-type: none"> • Servers • Software • Information security devices (firewall, intrusion detection and prevention system, daily log files, anti-virus, etc.) • Computers • Mobile devices (telephones, etc.) • External discs (USB, etc..) • Printers, scanners, photocopiers • Cloud systems 	<ul style="list-style-type: none"> • Paper • Manual data recording systems (survey forms, visitor entry & exit log, HR forms, etc.) • Written, printed, visual media
SOFTWARE AND DATA RECORDING MEDIUMS USED IN THE OFFICE	
<ul style="list-style-type: none"> • Google Systems • https://www.gnbmar.com/ • Skype • ICE Messenger • WhatsApp • XERO 	

4. EXPLANATIONS ON RETENTION AND DESTRUCTION

The Company shall retain and destroy the personal data belonging to "Company employees, potential employees, lecturers, employees of the group companies, business partners, references, employees of suppliers, officers of suppliers, persons who purchase products or services, directors, visitors and other persons" in accordance with the Law. Detailed explanations on retention and destruction within this context have been included below respectively.

4.1 Explanations on Retention



Article 3 of the Law defines the processing of personal data, article 4 states that personal data must be relevant, limited and proportionate to the purpose for which they are being processed and should only be stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data are processed and articles 5 and 6 list the conditions for processing personal data. Accordingly, within the context of our Company's activities, personal data is retained for a period specified in the relevant legislation or as required by the purpose of our processing.

4.1.1 Legal Grounds Requiring Retention

The personal data processed at the Company within the framework of its activities shall be retained for the duration of the period specified in the relevant legislation. Personal data is stored within this context with the explicit consent of the data subject or without the explicit consent of the data subject if one or more of the grounds listed below is present in the specific instance:

a) Explicitly provided for in the laws:

- Personal Data Protection Law no 6698,
- Law no 5651 on Regulation of Online Publications and Fight Against Crimes Committed by means of such Publications,
- Law no 6331 on Work Health and Safety,
- Turkish Code of Obligations no 6098,
- Turkish Commercial Code no 6102
- Tax Procedure Law no 213
- Social Security and General Health Insurance Law no 5510,
- Right to Information Act no 4982,
- Law no 3071 on Exercising the Right to Petition,
- Labor Law no 4857,
- Other laws and secondary legislation on this and the Company's business

b) Processing the personal data of the parties to a contract is necessary provided that such processing is directly related to the execution or performance of the contract,

c) It is necessary for compliance with a legal obligation to which the data controller is subject;

d) Personal data have been made public by the data subject themselves,

e) the data processing is necessary to establish, exercise or preserve a right,

f) the data processing is necessary for the legitimate interests of the data controller provided that this processing shall not violate the fundamental rights and freedoms of the data subject.



4.1.2 Processing Purposes Requiring Retention

The Company shall retain the personal data it processes within the context of its activities in line with the purposes listed below:

- Running information security procedures,
- Running procedures for selecting and assigning potential employees/interns/students,
- Conducting the application procedures for potential employees,
- Fulfilling obligations toward employees arising from their employment contracts and legislation,
- Managing the procedures for employee side benefits and other interests,
- Managing employee satisfaction and loyalty procedures,
- Conducting talent / career development activities,
- Engaging in auditing and ethics activities,
- Running training activities,
- Managing access authorizations,
- Conducting activities in compliance with legislation,
- Managing financial and accounting affairs,
- Company/product/service loyalty management,
- Ensuring the security of physical locations,
- Managing appointment procedures,
- Following up on and managing legal affairs,
- Running internal audits / investigations / intelligence affairs,
- Engaging in communication activities,
- Planning human resources procedures,
- Conducting/auditing business activities,
- Managing work health / work safety affairs,
- Engaging in activities aimed at ensuring business continuity,
- Logistics activities,
- Managing goods/services sales procedures,
- Managing goods/services procurement procedures,
- Managing goods/services manufacturing and operations procedures,
- Organization and event management,
- Conducting marketing analysis research,
- Running performance evaluation procedures,
- Management of advertisements, campaigns, and promotional offers,
- Running risk management procedures,
- Safekeeping and record keeping activities,
- Conducting contract negotiations,
- Ensuring the security of chattel and resources,
- Running supply chain management procedures,



- Managing goods/services marketing procedures,
- Ensuring the security of the data controller's operations,
- Conducting talent / career development activities,
- Informing competent persons, authorities, and institutions,
- Conducting management activities,
- Generating and monitoring visitor logs.

4.2 Grounds Requiring Destruction

The Company shall erase or destroy personal data upon the data subject's request, or the Company shall erase, destroy or anonymize personal data *ex officio* if:

- The legislative provisions on which the processing is based are amended or repealed,
- The purpose requiring the processing or retention of the personal data ceases to exist,
- When personal data is being processed based on explicit consent, the data subject rescinds their explicit consent,
- The Company accepts the data subject's request to have their personal data erased and destroyed within the context of their rights under article 11 of the Law,
- The data subject files a complaint with the Board and the request is granted by the Board in instances where the Company denies the data subject's request for the erasure, destruction or anonymization of their personal data, the data subject finds the Company's response inadequate or the Company fails to respond within the time period specified under the Law,
- The maximum period specified for the retention of personal data expires and no condition exists that would justify the retention of the personal data for a longer period of time.

5. TECHNICAL AND ADMINISTRATIVE MEASURES

The Company shall enact technical and administrative measures to retain personal data in a secure manner, to prevent the unlawful processing of or access to personal data and to have personal data destroyed lawfully in line with the measures specified and announced by the Board as adequate with respect to sensitive data pursuant to articles 12 and 6(4) of the Law.

5.1 Technical Measures

The technical measures enacted by the Company with respect to personal data being processed are as follows:

5.2 Administrative Measures



The administrative measures enacted by the Company with respect to personal data being processed are as follows:

6. METHODS OF DESTRUCTION OF PERSONAL DATA

At the end of the period specified in the relevant legislation or when the retention period necessary for the purpose of their processing expires, personal data shall be destroyed, either by the Company *ex officio* or upon request by the data subject, in accordance with the provisions of the relevant legislation using one of the below methods deemed suitable by the Company.

6.1 Erasure of Personal Data

Personal data are erased according to the methods provided in Table 3.

Table 3: Erasure of Personal Data

DATA RECORDING MEDIUM	EXPLANATION
PERSONAL DATA IN THE SERVERS	<p>A request will be made to the relevant service provider for the erasure of data found in digital media by one of the following means:</p> <p>1- With respect to the relevant information on record, all areas of this record shall be anonymized, and the anonymized version of the relevant record is re-submitted as proof.</p> <p>2- The relevant information on record is permanently erased from the server or memory or recording medium and the service provider shall provide written feedback about such act of erasure.</p>

6.2 Destruction of Personal Data

The Company shall destroy personal data y according to the methods provided in Table 4.

Table 4: Destruction of Personal Data

DATA RECORDING MEDIUM	EXPLANATION
DATA FOUND IN A PHYSICAL MEDIUM	All devices storing or physically recording digital data shall be crushed, burned or its magnetic field will be destroyed (by wiping).
DATA FOUND IN AN OPTICAL / MAGNETIC MEDIUM	

6.3 Anonymization of Personal Data

Anonymization of personal data is the process of rendering personal data impossible to link with an identified or identifiable natural person, even when matched with other data.

For the personal data to become anonymized, the data should be rendered impossible to associate with an identified or identifiable person, even by using techniques appropriate for the recording medium or relevant field of activity, such as the recovery of data by the data controller or third persons and by matching such personal data with other data.

7. RETENTION AND DESTRUCTION PERIODS

The retention periods for personal data being processed by the Company within the scope of its activities are specified in the:

- Company Personal Data Processing Inventory on a personal data basis concerning all personal data being processed in connection with the actions being taken;
- Personal Data Retention and Destruction Policy on a procedure basis.

The yearly of Company may update these retention periods as required if it becomes necessary. The Corporate Management department of the Company will, *ex officio*, erase, destroy, or anonymize personal data, the retention period of which has expired.

Table 5: Table of retention and destruction periods on a procedure-based

ACTION	RETENTION PERIOD	DESTRUCTION PROCEDURE

Freight invoice	10 Years as of the end of the legal obligation	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
E-invoice, e-archive integration	10 Years as of the end of the legal obligation	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Lease contracts and other contracts	10 years as per the general provisions of the TCO	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Cheques and instruments	10 Years as of the end of the legal relationship	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Loan utilization processes	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Information shared with accountants	10 Years as of the end of the legal relationship	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Job application procedures	3 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Hiring personnel and file procedures	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Entrusting employees with computers, laptops and other electronic devices	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Entrusting employees with office cards	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Entrusting employees with meal tickets	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Entrusting employees mobile phones with MDM uploaded	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Call statements for office telephones	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Entrusting employees with credit cards	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date

Performance evaluation process	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
salary / attendance fee payment procedures	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Travel abroad procedures	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
APS insurance process	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
SSI insurance process	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
OPF insurance process	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Health insurance process	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Group organizations and other events for employees	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Social media management process	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Documents of Company directors at the trade registry and circulars	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Legal support process	10 years as per the general provisions of the TCO	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Attachment notice (BEL art. 89/1)	10 years as per the general provisions of TCO	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Birth date records	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Signing of documents relating to the danger levels at the workplace	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date

Business cards of customers	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Business cards of employees / shareholders	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Forms submitted to Zorlu Center	Corlu Center Process	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Leasing process for commission contracts	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Process of issuing invoices, instruments, checks	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Business follow-up process	10 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Use of personal accounts on office devices	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Use of Skype, WhatsApp and ICE Messenger	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date
Use of Google Drive	5 Years as of the end of the contract	Within First Scheduled Periodic Interval Following the Expiration of the Retention Date

8. PERIODIC DESTRUCTION INTERVALS

As required under article 11 of the Regulation, the Company determined the periodic destruction be yearly. Accordingly, regular destruction will occur at the Company in the months of All employees are obligated to ensure that the data under their control is destroyed in compliance with this policy. Within this scope, they must notify those responsible for destruction about the expiry of the retention periods.

9. POLICY PUBLICATION AND SAFEKEEPING

The Policy shall be published in two different mediums, namely digitally and in printed form (on paper), bearing a wet signature. It will be made public on the website of <https://www.gnbmar.com/>. The printed paper copy shall be kept in the relevant file maintained at the Company's Corporate Management department.

10. POLICY'S UPDATE INTERVAL



The Policy will be reviewed as necessary, with the relevant sections updated as required. The most up-to-date version of the Policy can be accessed at the website of <https://www.gnbmar.com/>.

11. EFFECTIVENESS AND REPEAL OF THE POLICY

The Policy will be deemed to enter into effect once it is published on the Company's website.