FİLPA AMBALAJ VE DIŞ TİCARET A.Ş.

"PERSONAL DATA RETENTION AND DESTRUCTION POLICY"

Contents

THE CHAPTER ONE

QUALIFICATION AND PURPOSE OF PERSONAL DATA RETENTION AND DESTRUCTION POLICY

1.1. INTRODUCTION

This Personal Data Retention and Destruction Policy ("**Policy**") is prepared in order to determine rules and procedures which will be implemented by our company regarding erasure, destruction and Anonymization of personal data which we have as FİLPA AMBALAJ VE DIŞ TİCARET A.Ş in the capacity of data controller with principles of determination of maximum retention period which is necessary for purpose of use of personal data and to fulfil our commitments in compliance with relative regulations and Law on Personal Data Protection and in accordance with Law on Personal Data Protection no: 6698 ("**KVKK**" or "**LAW**") and the Regulation on Erasure, Destruction and Anonymization of Personal Data ("**Regulation**") published in Official Gazette on 28 October 2017 and entered into force as secondary regulation of law.

Within this context, the personal data of our workers, workers candidates, customers, any natural or legal persons who have their data in our company because of any reasons is being governed in compliance with law in the framework of Personal Data Processing and Protection Policy and this Personal Data Retention and Destruction Policy.

1.2. DEFINITIONS

Explicit Consent	freely given, specific and informed consent,
Relevant User	Except those who are responsible for the technical storage, preservation and backup of the data, those who process personal data within the organization of the data controller or with the authority given by the data controller
Personal Data/Data	all the information relating to an identified or identifiable natural person,
Private Qualified Personal Data/Data	Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data
Processing of Personal Data	Any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means,
Direct Definer	They are the definers who can unveil, disclose the person with whom they have relation by themselves and making them discernible
Indirect Definer	They are the definers who can unveil, disclose the person with whom they have relation by themselves and making them discernible by getting together with other definers.
Personal Data Owner/Data Subject	natural persons whose data is being processed by company such as company internal and external shareholders, company authorities, company's business partners, suppliers, advisors, workers, worker candidates, visitors, customers, potential customers and third persons, official institutions, banks, independent audit institutions.
Data Controller	The legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.
Data processor	the natural or legal person who processes personal data on behalf of the controller upon his authorization,

Law	It means Law on Personal Data Protection no: 6698.
Regulation	It means the Regulation on Erasure, Destruction and Anonymization of Personal Data ("**Regulation**") published in Official Gazette on 28 October 2017
KVK Board	Personal Data Protection Board
Registry Media	Any media in which data is processed such data fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means
Processing and Protection Personal Data and Privacy Policy	The policy determining principles and procedures on managing the data which the company has or be accessible via the link: www.filpa.com.tr
Data Registry System	The registry system which the personal data is registered into through being structured according to certain criteria,
Destruction	Erasure, Destruction and Anonymization of Personal Data
Anonymization	Rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data,
Erasure of personal Data	Erasure of personal data and making them inaccessible and non-reusable for relevant user.
Destruction of Personal Data	Destruction of personal data and making them inaccessible and non-reusable for relevant user.
Periodic Destruction	Periodic ex officio destruction, erasing or anonymization of personal data, upon disappearance of reasons which require the Process in law, as described in the Personal Data Retention and Destruction Policy,

THE SECOND TWO

MEDIA AND SECURITY MEASURES

2.1. MEDIA IN WHICH PERSONAL DATA ARE STORED

Protected personal data by the Company are stored in registration media which are compatible with its qualifications and our legal obligations. In general, registrations media which are used for protection of personal data are shown as below. However, some data that we have can be stored in different media than those which are show below as result of their qualifications and our legal obligations. Our company acts in capacity of data controller and process and protects personal data in accordance with law, Personal Data Processing and Protection Privacy Policy and this Personal Data Retention and Destruction Policy

a) Printed Material **:** The material in which data was kept by printing on paper and microfilm such as Units Case, Archive,

b) Local Digital Media **:** Miscellaneous media such as stationary and portable discs and servers in our company

c) Cloud Storage : The media in which our company used internet-based systems which is encrypted with cryptographic methods even it is not located in company.

c) Electronic Media **:** LOGO TIGER – BORDRO, FILE SERVER, MS SQL , PDKS SYSTEMS

2.2. MAINTAINING SECURITY OF MEDIA

On the purpose of protection in safety, processing unlawfully, prevention of access and destruction of your personal data, In the framework of the principles in 12th article of in KVK Law, our company takes necessary technical and administrative measures in compatible with qualifications of media in which personal data are stored for the purpose of prevention of access, processing unlawfully, and protection of personal data in safety.
These measures cover administrative and technical measures, including but not limited to, as long as it is compatible with qualifications of relative personal data and the media in which they are stored.

The administrative and technical measures taken by our company are stated below.

2.2.1. Technical Measures

Our company takes mainly the following technical measures which is compatible with qualifications of relative personal data and a media in which they are stored,

- Only Up-to date and reliable systems which are compatible with technological advances are used in media in which personal data are stored.
- Internal controls are being made within installing systems.
- Security systems are being used for media in which personal data are stored.
- Security tests and investigations are being made in order to detect security vulnerability on Information systems and the points which constitute the current and possible risks detected as result of the above-mentioned tests and investigations are being eliminated.
- Only authorized persons are parochially permitted to access date on the purpose of protection of personal data by limiting their access to data in media in which personal date are stored and all access is being recorded
- The procurement of technical infrastructure which observes and hinders penetration of data out of company and formation of relative matrix are maintained. Vulnerabilities of systems are controlled regularly and as needed by taking services of penetration test.
- Sufficient technical personnel are assigned in order to maintain the security of media in which personal data are stored at the company.
- It is maintained that access authorization given to personnel working in Information technologies units are being kept under control.
- Destruction of personal data is maintained by means of being unrecoverable and not leaving any audit trail.
- In accordance with 12th article of the law, digital media in which personal data are stored are secured with encrypted or cryptographic methods by means of maintaining the requirements of information security.

2.2.2. Administrative Measures

Our company takes mainly the following administrative measures which are compatible with qualifications of relative personal data and media in which they are stored,

- The studies have been performed in order to raise awareness of Company's worker, whom have access to personal data, on information security, personal data and right of privacy and personnel are provided with necessary trainings in the framework of regulations on personal data protection and data security
- The access to the personal data in company is limited to the personnel who have to have access as required by job description. It was taken consideration into the importance level of data and whether or not data has special qualifications.

- Legal and technical consulting services are taken in order to follow the developments on information security, right of privacy, personal data protection and to perform necessary actions.
- In case of thirds parties' obtaining the data processed by using unlawful means, the Board is immediately informed about this situation.
- In case of transferring personal data to third parties as required by law, the protocols are signed with third parties in order to protect personal data or it is maintained data security by adding the appendix to the contract. It is paid necessary attention to thirds parties' complying with obligations in the protocols.
- It is conducted audit or made it conducted for the performance of the obligations of law by its legal person. Any vulnerabilities detected as a result of the audits are eliminated.

2.2.3. Internal Audit

Our company conducts internal audits in order to perform the obligations of Personal Data Retention policy and Personal Data Processing and Protection policy in accordance with 12th article of Law.
Any faults or deficiency regarding the performance of this obligations are immediately eliminated in case of detection of them as a result of internal audit.
In case of detection of third parties' obtaining unlawfully the personal data under responsibility of our company during the period of audit or any time, our company immediately inform this situation to related person and the Board.

THE CHAPTER THREE

DESTRUCTION OF PERSONAL DATA

3.1. REASON OF RETENTION AND DESTRUCTION

3.1.1. Reason of Retention

The personal data in our company have been preserved in accordance with the related law and our personal data policy (it is accessible via the link: www.filpa.com.tr) and for the purposes and reasons wherein.

3.1.2. Reasons of Destruction

The personal data in our company are erased, destructed and anonymized in accordance with this destruction policy in the event of any demand of related person or upon disappearance of the reasons which are stated in the 5th and 6th article of Law is shown below.

The reasons stated in the 5th and 6th article of Law are shown below.

a) It is clearly provided for by the laws.
b) It is mandatory for the protection of life or physical integrity of the person or of any other person who is bodily incapable of giving his consent or whose consent is not deemed legally valid.
c) Processing of personal data belonging to the parties of a contract, is necessary provided that it is directly related to the conclusion or fulfilment of that contract.
d) It is mandatory for the controller to be able to perform his legal obligations.
e) the data concerned is made available to the public by the data subject himself
f) Data processing is mandatory for the establishment, exercise or protection of any right

g) it is mandatory for the legitimate interests of the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

3.2. DESTRUCTION METHODS

Our company shall erase, destruct or anonymize personal data which is stored in accordance with law and regulations and Personal Data Processing and Protection policy ex officio or upon demand by the data subject, upon disappearance of reasons which require the process within the period stated in personal data retention and destruction policy.

3.2.1. Erasure of Personal Data

Personal data can be erased by company by using following methods

Data Registry Media	**Statement**
Personal Data in Servers	System Administrator erases by removing access authorization of relevant user for personal data in server, the ones which retention period ends
Personal Data in Electronic Media	Personal Data in electronic media, for ones which retention period ends, is turned into non accessible and non-reusable data for other workers (relevant user) except database administrator.
Personal data in physical Media	Personal Data in in physical media, for ones which retention period end, is turned into non accessible and non-reusable data for other workers (relevant user) except unit manager who is responsible for document archive. Besides blacking is conducted in order to make it unreadable by striking out, overdyeing and erasing
Personal Data in portable media	Personal Data in storage media such as flash memory, for ones which retention period ends, are stored with encryption key by system administrator by encrypting and giving access authorization to system administration

3.2.2. Destruction of Personal Data

Personal data can be destructed by company by using following methods

Data Registry Media	**Statement**
Personal data in Physical Media	Personal data on hard copy, for ones which retention period end, destroyed in unrecoverable manner by using paper shredder.
Personal data in optical magnetic media	Personal data in optical magnetic media, for ones which retention period ends are physically destroyed with methods such as melting, burning, pulverising. Besides, data can be made to be unreadable by putting magnetic media into special equipment and exerting it to high value magnetic field.

3.2.3. Anonymizing of personal data

Anonymizing is a rendering personal data impossible to link with an identified or identifiable natural person, even though matching them with other data. In order to anonymize personal data, rendering personal data impossible to link with an identified or identifiable natural even by using the techniques which is suitable for activity area and registry media such as recovery of data by controller or third parties or/and matching them with another data.

3.3. RETENTION AND DESTRUCTION PERIODS

3.3.1. Retention Periods

PROCESS	SAVING PERIOD	DESTRUCTION PERIOD
Management of Human Resource process	10 years in pursuit of finalization of activity	The first periodic destruction period in pursuit of finalization of retention period
Management of purchasing and marketing process	10 years in pursuit of finalization of activity	The first periodic destruction period in pursuit of finalization of retention period
Preparation of contract	10 years in pursuit of finalization of activity	The first periodic destruction period in pursuit of finalization of retention period
Performing of communication activity	10 years in pursuit of finalization of activity	The first periodic destruction period in pursuit of finalization of retention period
System of Pursuance of log registry	10 years	The first periodic destruction period in pursuit of finalization of retention period
Execution of Hardware and Software Access Process	2 years	The first periodic destruction period in pursuit of finalization of retention period
visitors	2 years	The first periodic destruction period in pursuit of finalization of retention period
Camera Records	2 years	The first periodic destruction period in pursuit of finalization of retention period

- In the event of determining the longer period as per the regulation or in the event of foreseeing the longer periods such as timeout, foreclosure, retention period as per the regulation, the periods in regulation is accepted as maximum retention period.
- Besides, in need of longer retention period of document as per qualifications of document, because of legal and commercial reasons, related documents can be preserved until max 20 years without being subject to any above-mentioned periods.

3.3.2. Destruction Periods

Our company shall erase, destruct or anonymize personal data for which it is responsible in the first destruction period in pursuit of the date of appearance of obligation to erase, destruct or anonymize personal data in accordance with law and regulations and Personal Data Processing and Protection Policy and Personal Data Retention and Destruction Policy.
when data subject requests for erasing or destructing his/her personal data by applying to the company referring to 13th article of the law.

a) If the reasons which require the process disappear, company erase, destruct or anonymize related personal data within 30 (thirty) days as for the date of receiving the request by explaining the reason of destruction with suitable destruction methods. Data subject have to make destruction request in compliance with Personal Data Processing, Protection and Privacy Policy for being counted that company received the request. Our company informed data subject about the action in any case.
b) If the reasons which require the process did not completely disappear, this request may be refused by or Company by explaining the reason in accordance with 13th article of Law and the reason of refusal will be informed at the latest 30 days in written form or electronically.

3.4. PERIODIC DESTRUCTION

In the event of completely disappearance of reasons which require the process in Law, our Company erase, destruct or anonymize the personal data which requirements of process disappeared in the recurring periods as required in this Personal Data Retention and Destruction Policy. Periodic Destruction Process starts on 02.01.2020 for the first time, repeats for each 6 (six) months.

3.5. LEGALITY AUDIT FOR COMPLIANCE OF DESTRUCTION

Our company maintains destruction activity in compliance with Law, regulations and Personal Data Processing and Protection Policy and this Personal Data Retention and Destruction Policy both upon of request for destruction and as destruction activity which is conducted ex officio in periodical destruction period.

Our company takes some administrative and technical measures in order to maintain the conformity of destruction with these regulations.

3.5.1. Technical Measures

- To provide technical equipment's and tools which are suitable for destruction methods stated in the Policy
- To maintain security of the place where the destruction is conducted.
- To keep access log of persons who destruct.
- To employ the capable and experienced person which can destruct and take service for third parties as necessary.

3.5.2. Administrative Measures

- Our company performs the studies on information security, personal data and right of privacy in order to raise the awareness of worker who will make destruction.

- It takes legal and technical consulting services in order to follow the developments on information security, right of privacy, personal data protection and to perform necessary actions.
- In the event of making third parties destructed because of technical and legal requirements, the protocols are signed with third parties in order to protect personal data. It is paid necessary attention to thirds parties' complying with obligations in the protocols.
- It regularly conducts audit in order to control whether or not the destruction was made in compliance with provisions in Personal Data Retention and Destruction policy and takes necessary action.
- It was recorded all actions regarding Erasure, destruction or anonymizing of personal data and these records are preserved for minimum three years except other legal obligations

CHAPTER FOUR

4.1. PERSONAL DATA COMMITTE

The Company established a Personal Data Committee. Personal Data Committee performs /makes it performed necessary action to process and preserve personal data of data subject in compliance with Personal Data Processing and Protection Policy and this Personal Data Retention and Destruction Policy and having been assigned and authorized for audit the process.

Personal Data Committee is composed of 3 members including 1 president, 1 full member, 1 reserve member. Title and job description of company workers who have duty in Personal Data Committee are stated below.

TITLE	JOB DESCRIPTION
President of Personal Data Committee	Responsible for managing risk assessment process, research, analysis, planning activity in all projects which are managed in compliance process with law, and managing the process which have to be conducted in accordance with Personal Data Processing and Protection Policy and this Personal Data Retention and Destruction Policy and making decision regarding the requests from which data subject are taken.
Committee members	Responsible for reporting of the request of data subject to in order to assess and scrutinize (legal, technical and administrative) Manager of Personal Data Committee, performing the action regarding the request on which is assessed and taken a decision by Manager of Personal Data Committee in accordance with decision of Manager of Personal Data Committee and auditing for retention and destruction process, reporting this audits to Manager of Personal Data Committee and maintaining retention and destruction process

CHAPTER FIVE

UPDATE AND CONFORMITY

Our company reserves its all right to make amendments in Personal Data Retention and Destruction Policy and Personal Data Processing and Protection Policy in accordance with any amendment in law and the body decision, any developments in sector and information fields.

Any Amendments in this Personal Data Retention and Destruction Policy are immediately added to text and the explanations regarding the amendments are added to the end section of policy.

In case of any inconsistency between KVKK Law, related other regulations and this the policy, the provision of KVKK Law and related other regulation will be applied.

5.1. AMENDMENTS NOTES

03.09.2019 **:** Personal Data Retention and Destruction Policy was published

*There was no amendment which belongs to previous term. *