

FİLPA AMBALAJ VE DIŞ TİCARET A.Ş.
PERSONAL DATA PROCESSING, PROTECTION AND PRIVACY POLICY

Content

SECTION 1.....	3
§ 1.PREVIEW	3
1.1. Preview.....	3
1.2. Policy Objectives.....	3
1.3. Policy Scope and Personal Data Owners.....	3
1.4.Descriptons.....	4
1.5. Policy Effect	5
SECTION 2.....	5
§ 2. PERSONAL DATA PROCESSING AND TRANSFER	5
2.1. General Policies on Personal Data Processing	5
2.2. Personal Data Processing Conditions.....	6
2.3. Special Personal Data Processing Conditions.....	6
2.4. Personal Data Transfer Conditions.....	6
2.4.1. Personal Data Foreign Transfer Conditions.....	7
2.5. Special Personal Data Transfer Conditions	7
2.5.1. Special Personal Data Foreign Transfer Conditions	8
SECTION 3.....	8
§ 3. PERSONAL DATA PROCESSING AND TRANSFER OBJECTIVES AND TRANSFERRABLE PARTIES .	8
3.1. Personal Data Processing and Transfer Objectives	8
3.2. Transferrable Parties	9
SECTION 4.....	9
§ 4. PERSONAL DATA COLLECTION METHOD AND APPLICABLE LAW, ERASURE, DESTRUCTION AND ANONYMISATION VE AND STORAGE PERIOD	9
4.1. Personal Data Collection Method and Applicable Law	9
4.2. Personal Data Erasure, Destruction and Anonymisation	9
4.3. Personal Data Storage Period.....	10
SECTION 5	

§ 5. PERSONAL DATA PROTECTION MATTERS	10
5.1. Personal Data Security	10
5.1.1. Technical and Administrative Measures Ensuring Legal Processing of Personal Data	10
5.1.2. Technical and Administrative Measures Ensuring Legal Access to Personal Data	11
5.1.3. Personal Data Secure Storage.....	12
5.1.4. Supervision of Personal Data Protection Measures	13
5.1.5. Measures on Unauthorized Disclosure of Personal Data	13
5.2. Rights of Personal Data Owners	14
5.3. Special Personal Data Protection.....	14
SECTION 6	14
§ 6. RIGHTS OF PERSONAL DATA OWNER, EXERCISE AND EVALUATION OF RIGHTS	14
6.1. Informing Personal Data Owner	14
6.2. Rights of Personal Data Owner under Personal Data Protection Law (PDPL)	14
6.3. Cases Annulling Exercise of Rights of Data Owner	15
6.4. Exercise of Personal Data Owner’s Rights	15
6.5. Company’s Response to Applications and Timetable of Response	16
6.6. Personal Data Owner’s Right to File a Complaint at Personal Data Protection Commission.....	16
SECTION 7	16
§ 7. FOOTAGE PROCESSING	16
SECTION 8	16
§ 8. COMPANY’S MANAGEMENT STRUCTURE UNDER PERSONAL DATA PROCESSING AND PROTECTION POLICY	
16	
SECTION 9	16
§ 9. MISCELLANEOUS.....	17
9.1. Update and Orientation.....	17
9.2. Amendments	17
9.3. Validity	17
9.4. Distribution	17
9.5. Attachments	17

SECTION 1

1. PREVIEW

1.1. Preview

We, Filpa Ambalaj ve Diş Ticaret Anonim Şirketi (“Company”), under the Personal Data Protection Law #6698 (“PDPL” or “Law”) give utmost importance to ensuring legal and lawful processing and protection of all personal data we come to know by force of any business relationship we engage in and maximum diligence in planning and business operations. In this regard, we hereby furnish you the Personal Data Processing, Protection and Privacy Policy (“Policy”) to fulfill our responsibility for informing Personal Data Owners and to clarify our technical and administrative measures on Personal Data processing and protection in accordance with Article 10 of the Law.

1.2. Policy Objectives

The fundamental objective of this Policy is to provide a general information on lawful and legal Personal Data processing systems and to inform parties whose data are subjected to processing, including the Company, its affiliates, sharers, officers, business partners, suppliers, consultants, employees and employees-to-be, visitors, clients, potential clients and third parties, public enterprises, banks and independent auditing firms. By this means, we shall ensure that Personal Data processing and protection by our Company are conducted in a legal and lawful manner and Personal Data Owners’ rights granted under the applicable Personal Data protection laws and regulations are duly reserved.

1.3. Policy Scope and Personal Data Owners

This Policy is designed for and shall be exercised for parties whose Personal Data are subjected to processing, whether manually on a data storage unit or automatically, including the Company, its affiliates, sharers, officers, business partners, suppliers, consultants, employees and employees-to-be, visitors, clients, potential clients and third parties, public enterprises, banks and independent auditing firms.

Our Company duly informs parties, whose Personal Data are processed, by ensuring online access to the Policy on its website. In the event that the data is not categorized as “Personal Data” as specified below or our Company processes the Personal Data in a manner contrary to the abovementioned, this Policy shall not be effective.

1.4. Descriptions

Terms included in this Policy represent the following:

Company/Us	FİLPA AMBALAJ VE DIŞ TİCARET AŞ.
Personal Data	All information possessed by identified or identifiable parties.
Special Personal Data	Data, biometric data or genetic data related to nationality, ethnicity, political ideas, philosophical ideas, religion, communion or other beliefs, appearance, memberships to associations, foundations or unions, health status, sexual life, criminal record and security measures .
Personal Data Processing	Any actions executed on data, including obtaining, saving, storing, protecting, changing, amending, disclosing, exchanging, transferring, publicizing, categorizing or prohibiting, whether manually on a data storage unit or automatically.
Storage Environment	All environments where personal data, obtained whether manually on a data storage unit or automatically, are stored.
Personal Data Owner/Respective Person	Real persons whose data are processed by the Company, including the Company's affiliates and sharers, officers, business partners, suppliers, consultants, employees and employees-to-be, visitors, clients, potential clients and third parties, public enterprises, banks and independent auditing firms.
Data Storage System	Data storage system where personal data are configured and stored based on certain criteria.
Data Supervisor	Business entity responsible for determining objectives and methods of data storage and setup and management of data storage system.
Data Processor	Real persons and business entities processing personal data using the powers granted by the data supervisor on behalf of them.
Respective User	Person processing personal data as directly instructed by data supervisor or in compliance with the instructions and suggestions of data supervisor, except persons or entities responsible for technical storage, protection and backup of personal data.
Explicit Consent	Information-based explicit consent on a specific matter given with own free-will.
Destruction	Erasure, destruction and anonymisation of personal data.
Anonymisation	Invalidating relation of personal data, previously related with other persons, with identified or identifiable persons, including by matching with other data.
Deletion of Personal Data	Nullification of access and use of personal data by any respective person.
Destruction of Personal Data	Making personal data irrevocably inaccessible, deleted and disused by any party.
Periodical Erasure	Erasure, destruction and anonymisation <i>ex-officio</i> of personal data at certain intervals specified in personal data storage and destruction policy in the event of complete termination of personal data processing liabilities set forth in the Law.
Law/PDPL	Personal Data Protection Law #6698.

Regulation	Regulation on Personal Data Erasure, Destruction and Anonymisation announced in the Official Gazette on October 28 th , 2017.
PDPL Commission	Personal Data Protection Commission.

1.5. Policy Effect

This Policy, formed and taken into effect in September 3rd, 2019, is available on the Company's website (www.filpa.com.tr) and can be accessed by respective persons upon request by Personal Data Owners.

SECTION 2

2. PERSONAL DATA PROCESSING AND TRANSFER

2.1. General Policies on Personal Data Processing

Personal Data are processed by the Company in compliance with PDPL and applicable laws and terms and conditions specified in this Policy. In this regard, the Company shall process Personal Data taking into consideration the following:

- Personal Data shall be processed in compliance with the applicable law and within the context of principle of honesty. By force of this provision, the Company shall process Personal Data within the context of principle of honesty in accordance with the Constitution and PDPL and applicable laws and regulations.
- Personal Data shall be kept precise and up-to-date by notification. In this regard, data sources should be exact and accurate, data accuracy should be checked and necessity of an update should be evaluated.
- In this regard, necessary measures shall be taken to ensure accuracy and up-to-dateness of Personal Data and Personal Data Owners shall be assured that the processed Personal Data are based on realities.
- Personal Data shall be processed for obvious, clear and lawful purposes. Lawfulness herein refers to the Company's processing Personal Data for the business relationship or services offered herein.

In this context, the Company shall process Personal Data only for the obvious and exact lawful purposes herein and avoid processing Personal Data for other purposes. As such, the Company shall process Personal Data only within the scope of the business relationship they engaged in with Personal Data Owners and only if necessary.

- The Company shall process only Personal Data which are related to execution of the business purpose herein and avoid processing unnecessary data or data unrelated to the purpose herein. While processing, the company shall keep in the due limits designated for successful conduct of the purpose. As such, Personal Data should be related with their purpose, limited and reasonable.
- In case that the applicable law prescribes a legal period of storing Personal Data, the Company shall obey such period; if no such period is designated, the Company shall store Personal Data only for a period necessary for concluding the business relationship herein. In

the event that there is no more any reason for storing Personal Data, they shall be erased, destructed or anonymised.

2.2. Personal Data Processing Conditions

The Company shall not process any Personal Data without explicit consent of the Data Owner, with the only exception of certain provisions in the Law. However, the Company shall be entitled to process Personal Data without the Data Owner's explicit consent if the following is the case:

- If the applicable law stipulates so, the Company can process the Data Owners' Personal Data. For example, Article 230 of Tax Procedure Law stipulates that the relevant person's explicit consent is not necessary for the addition of their name on invoices.
- Personal Data can be processed without explicit consent of the relevant person if the situation calls for processing to protect a person's life or physical or mental health if the relevant person is literally unable to express his/her consent or if his/her consent is not to be considered. For example, if the person is unconscious or has mental issues and if the situation calls for protecting life or physical or mental health, for instance if a surgery is needed, Personal Data Owner's Personal Data can be processed without explicit consent. By this force, data such as blood type, past issues and operations and medicines used can be processed on the relevant medical database.
- Parties' Personal Data can be processed providing that such data are directly related to a contract or agreement entered into. For example, a party's account number can be processed if the contract calls for payment.
- The Company can process Personal Data to fulfill legal responsibilities if necessary.
- The Company may process Personal Data if Data Owner publicizes, in other words, discloses such data, since there is no more legal interest to protect.
- The Company may process Personal Data without Data Owners' explicit consent if it is necessary for protecting or exercising any legal rights.
- The Company may process Personal Data to protect its legitimate interests by ensuring protection of the Data Owners' fundamental rights and freedoms granted by applicable laws and policies. The Company shall show due diligence to comply with general policies on Personal Data protection and protect Data Owners' interests.

2.3. Special Personal Data Processing Conditions

The Company shall not process Personal Data without explicit consent of the Respective Person. However, if the applicable law prescribes so, Personal Data can be processed, except health and sexual life. The Company can process Personal Data such as health and sexual life without explicit consent of the Respective Person only to protect public health, conduct protective medicine, medical examination, treatment or healthcare and plan and manage health services and funding within the context of your confidentiality obligations. The Company shall take necessary measures to process Special Personal Data as specified by the Commission.

2.4. Special Personal Data Transfer Conditions

Our Company can rightfully transfer Special Personal Data to third parties by establishing privacy conditions and taking security measures in line with Personal Data processing objectives. Our Company transfers Personal Data in accordance with the provisions of the Law. By force of lawful and legal Personal Data processing objectives, the Company can transfer Personal Data to third parties, as specified in Article 5 of the Law, if:

- the Data Owner explicitly consents to processing;
- there is an explicit regulation in the Law allowing Personal Data transfer or calling for it for protecting life or physical or mental health of the Data Owner or another third party;
- the Data Owner is literally unable to express his/her consent or his/her consent is not to be considered;
- the contractual persons' data need transfer directly as a result of a contract being entered into between parties;
- Personal Data transfer is required for our Company to fulfill its legal responsibilities;
- Personal Data have been publicized or disclosed by the Data Owner;
- Personal Data transfer is necessary for establishing, exercising and protecting any rights, or;
- our Company is obliged to transfer Personal Data to protect our legitimate interests by protecting the Personal Data Owners' fundamental rights and freedoms.

2.4.1. Personal Data Foreign Transfer Conditions

Our Company shall transfer Personal Data and Special Personal Data abroad by taking necessary precautions in line with Personal Data processing objectives. Personal Data can be transferred only to countries deemed "secure" by the Commission; if the country is not secure according to the Commission, the data can be transferred only upon written agreement on sufficient security by Data Supervisors in Turkey and the relevant country and with the Commission's written consent.

2.5. Special Personal Data Transfer Conditions

The Company can transfer Personal Data to the belowmentioned third parties in line with Personal Data processing objectives by showing due diligence and taking measures specified by the Commission;

- (i)** Upon explicit consent of the Data Owner or
- (ii)** In the presence of the below conditions;

- Applicable laws and regulations stipulate that persons or authorized companies or entities can transfer Special Personal Data of the Personal Data Owner, such as nationality, ethnicity, political ideas, philosophical ideas, religion, communion or other beliefs, appearance, memberships to associations, foundations or unions, health status, sexual life, criminal record and security measures, except health and sexual life, and;
- Special Data transfer is needed to protect public health, conduct protective medicine, medical examination, treatment or healthcare and plan and manage health services and funding.

SECTION 3

3. PERSONAL DATA PROCESSING AND TRANSFER OBJECTIVES, TRANSFERRABLE PARTIES

3.1. Personal Data Processing and Transfer Objectives

The Company shall process and transferr Personal Data in compliance with the Personal Data processing conditions specified in Articles 5 and 6 of the Law for and limited to the reasons below:

- Ensuring general and commercial security of our enterprises;
- Keeping up with employment procedures and ensuring employees' security;
- Optimal planning and execution of human resource policies;
- Accurate planning, conduct and management of commercial partners and strategies;
- Ensuring legal, commercial and physical security of itself and its business partners;
- Ensuring corporate activeness and planning and executing managerial and communicative activities;
- Ensuring best benefit of Data Owners from goods and services and optimizing them based upon Data Owners' requests, needs and options;
- Creating a database for clients, commercial partners, suppliers, employees and employees-to-be;
- Contacting Data Owners for their requests and complaints and managing them;
- Managing business partner and supplier relations;
- Dealing with recruitment;
- Executing and pursuing financial reporting and risk management;
- Executing and pursuing legal proceedings featuring the Company;
- Protecting the Company's reputation;
- Managing investor relations;
- Informing authorized firms of legal proceedings;
- Managing footages and on-site ID card or permit checks for security purposes and in accordance with legal obligations, coordinating OHS trainings and recording work accident footages, coordinating guest visits and emergency operations, carrying out health procedures, keeping visitor wi-fi data use records and obtaining communication forms;
- Creating and managing visitor register book.

In the event that the processing for the above reasons does not meet the criteria specified in the relevant articles and provisions of the Law, the Company shall ask for your explicit consent to processing.

3.2. Transferrable Parties

Personal Data can be shared on a reasonable level only with our business and solution partners, banks and other third parties which provide technical, logistical etc. support to provide all targeted services satisfactorily and efficiently. These third parties refer to parties that need access to Personal Data for satisfactory and successful conclusion of the business herein.

In the events that our Company is obliged to share Personal Data with other parties for the conclusion of the business, that sharing of Personal Data is ordered by the law or that a legal or administrative warrant to share Personal Data is present, your Personal Data might be subjected to transfer limited to the relevant third parties.

Part of Personal Data can also be shared with advertisers only with other parties' information and/or completely to make advertisements easier to access by the target market.

In the event of transfer of anonymised data, the data shall not have any connection whatsoever with your clients/visitors and shall not include your credentials or make you identifiable. Your privacy is protected under anonymised data.

SECTION 4

4. PERSONAL DATA COLLECTION METHOD AND APPLICABLE LAW, ERASURE, DESTRUCTION AND ANONYMISATION VE AND STORAGE PERIOD

4.1. Personal Data Collection Method and Applicable Law

In accordance with Article 1 regulating the Law's objective and Article 2 regulating its scope, Personal Data; shall be processed in any way including orally, in written, on the phone, fax, e-mail and other electronic services, in technical or similar ways and in different ways such as on the Company's website or mobile app within the context of the contract, demands and applicable law in order to fulfill responsibilities granted by the Law.

4.2. Personal Data Erasure, Destruction and Anonymisation

In the event that Personal Data Protection liabilities go void, the Company shall erase, destroy or anonymise the Personal Data, even if they have processed them, in accordance with the applicable laws and regulations on Personal Data erasure, destruction and anonymisation. Erasure refers to making data inaccessible and unavailable, destruction to exterminating all data sources including documents, CDs, storage units etc. making them impossible to access in any way and anonymisation to making data unrelated to identified or identifiable person even if they have actually been related to them previously.

4.3. Personal Data Storage Period

The Company shall store Personal Data for the legal period allocated by the laws. If there is any legal period available allocated by the laws, the Company shall store Personal Data only for such period allocated in order to execute the business purpose herein. Upon expiration of such period, the Company shall erase, destroy or anonymise such data.

If Personal Data processing objectives are no longer viable or if the storage period has expired, exception will be made to storing Personal Data only if there is any threat available for legality or if storing is necessary for exercising rights. Even if Personal Data storage period has expired, exceptional storage period can be assigned by referring to equivalent cases. Upon establishment of such cases, the Personal Data can be processed and stored even after expiration of the storage period for some time. Eventually after such exceptional period, the data shall be erased, destroyed and anonymised.

Further technical information on Personal Data storage, erasure, destruction and anonymisation are available on the Company's Personal Data Storage and Destruction Policy.

SECTION 5

5. PERSONAL DATA PROTECTION MATTERS

In accordance with Article 12 of the Law, the Company shall bear responsibility for taking sufficient technical and administrative measures to ensure prevention of illegal processing or access of Personal Data and protect them.

5.1. Personal Data Security

5.1.1 Technical and Administrative Measures Preventing Illegal Processing of Personal Data

The Company shall be responsible for taking necessary technical and administrative measures to prevent illegal processing of Personal Data, based on their technological and economical status.

(i) Technical Measures Preventing Illegal Processing of Personal Data

Below are the major technical measures taken by the Company in order to prevent illegal processing of Personal Data:

- Access of unauthorized parties to Personal Data shall be prevented by means of authorization system.
- Personal Data processing shall be supervised through appropriate technical systems.
- Technical measures shall be reported to the respective authorities periodically as part of the internal audit mechanism.
- Technical personnel shall be recruited.

(ii) Administrative Measures Preventing Illegal Processing of Personal Data

Below are the major administrative measures taken by the Company in order to prevent illegal processing of Personal Data:

- The employees shall be trained on applicable laws on Personal Data protection and legal processing of Personal Data.
- The Company shall conduct necessary audits to ensure implementation of legal provisions.
- The Company's business activities shall be analyzed by the relevant service units to obtain statistical information on Personal Data processing.
- The Company's relevant service units shall establish requirements for the lawful and legal execution of the business activities herein in accordance with the Law.
- The Company's relevant service units shall raise awareness of and establish rules for lawful execution of the activities herein. In this regard; awareness of this matter is provided by training and corporate policies.
- The Company shall recruit experienced personnel for Personal Data processing and ensure their sufficient training on the PDPL.
- Provisions on non-processing, non-disclosure and misuse of Personal Data shall be included in contracts and documents between the Company and its employees, awareness shall be raised in this regard and audits shall be conducted to ensure compliance with the Law.
- In the event that the processed data are accessed by unauthorized parties, the Company shall immediately inform the addressee or the Commission/Board of this.
- In regard to transfer of Personal Data, the Company shall sign framework agreements with transferees or add provisions in contracts to ensure protection Personal Data

5.1.2. Technical and Administrative Measures Preventing Illegal Access to Personal Data

The Company shall take necessary technical and administrative measures to prevent illegal access, disclosure, processing or use of unauthorized parties based on the nature of data and their technological and economical status.

(i) Technical Measures Preventing Illegal Access to Personal Data

Below are the technical measures taken by the Company in order to prevent illegal access to Personal Data:

- Measures shall be regularly taken and updated according to technological developments.
- Technical solutions on access and authorization shall be referred to in line with legal orientation requirements specified by the relevant service units.
- Access authorities shall be limited and supervised on a regular basis.
- Technical measures shall be reported to the respective authorities periodically as part of the internal audit mechanism and potential risks shall be re-evaluated and the necessary technological solutions shall be generated.

- Software and hardware featuring anti-virus systems and firewall shall be set up.
- Technical personnel experienced on technical issues shall be recruited.
- Personal Data collection softwares shall undergo security scan to detect security vulnerabilities. All vulnerabilities shall be solved.
- The systems set up shall undergo internal audits.
- The systems shall undergo risk analyse, data categorization, risk evaluation and business impact analysis.
- Appropriate technical infrastructure shall be supplied and appropriate matrixes shall be established to supervise or prevent information leakage out of the Company.
- Information technologies unit workers' authorities to access Personal Data shall be kept under limit.

(ii) Administrative Measures Preventing Illegal Access to Personal Data

Below are the administrative measures taken by the Company in order to prevent illegal access to Personal Data:

- The employees shall be trained on the prevention of unauthorized access to Personal Data.
- Personal data access and authorization mechanisms shall be designed within the Company for legal orientation requirements specified by the relevant service units.
- The employees shall be warned that they will not disclose data to any other party than those specified in the Law, will not use them for purposes other than specified and their liabilities shall last even if they resign. They shall accept, undertake and declare these officially (by agreement, signature etc.)
- Additional provisions shall be added in contracts entered into and signed between the Company and transferrable parties, including that the Company shall take necessary measures to protect personal data and that they shall ensure compliance with this provision within the corporation.

5.1.3. Personal Data Secure Storage

The Company shall take necessary measures to ensure secure storage of Personal Data and their unlawful termination, loss or change, based on their technological and economical status.

Below are the measures specified in Article 12(1) of the PDPL:

- Preventing illegal processing of Personal Data;
- Preventing illegal access to and change of Personal Data, and;
- Protecting Personal Data.

Below are the measures taken by the Company in this regard:

(i) Technical Measures Ensuring Secure Storage of Personal Data

Below are the technical measures taken by the Company to ensure secure storage of Personal Data:

- The Company shall use recent technologies to ensure secure storage of Personal Data.
- Technical personnel shall be recruited.
- Security systems shall be installed in storage units, security scans and researches shall be carried out on information systems and certain or potential risks detected shall be eliminated. The technical measures taken shall be reported to the relevant authorities periodically as part of the internal audit mechanism.
- Backup softwares shall be used in line with the applicable laws and regulations to ensure secure storage of Personal Data.
- Only authorized persons shall be allowed to access Personal Data on storage systems for the Personal Data storage objectives and unauthorized accesses or attempts to do so shall be monitored by logging storage units.

(ii) Administrative Measures Ensuring Secure Storage of Personal Data

Below are the administrative measures taken by the Company to ensure secure storage of Personal Data:

- The personnel shall be trained on secure storage of Personal Data.
- Legal and technical counselling services shall be provided to get a general idea about keeping up with developments in the fields of information security, right to privacy and Personal Data Protection and basics shall be practised.
- In the event that external technical services are utilized for Personal Data storage, additional provisions shall be added in contracts entered into and signed between the Company and transferees including that transferees shall take necessary measures to protect Personal Data and cooperate with and train their employees in this regard.

5.1.4. Supervision of Personal Data Protection Measures

The Company shall, in accordance with Article 12 of the Law, conduct due audits on its own. Results of such audits shall be reported to the relevant service units and improvements shall be made based on them.

5.1.5. Measures In Case of Unauthorized Disclosure of Personal Data

The company possesses a system that immediately informs the Data Owner or PDP Commission in the event of unauthorized access to or possession of Personal Data processed in accordance with Article 12 of the Law. If necessary, the PDP Commission might officially announce this on their website or in any other way.

5.2. Rights of Personal Data Owners

The Company shall consider Personal Data Owners' rights specified in the Policy and the Law and take measures necessary in order to protect them. Details on Personal Data Owners' rights are included in Section 6 of this Policy.

5.3. Special Personal Data Protection

The Law gives particular importance to certain data (Special Personal Data) due to the fact that their unlawful processing may lead to victimization of or racism against Data Owners. Special Data refers to data, biometric data or genetic data related to nationality, ethnicity, political ideas, philosophical ideas, religion, communion or other beliefs, appearance, memberships to associations, foundations or unions, health status, sexual life, criminal record and security measures. The Company pays particular attention to protecting Special Data that bear the statement “special” processed in line with the applicable laws and regulations. By this force, the technical and administrative measures taken to protect Personal Data shall be implemented on exactly the same level for Special Personal Data as well and the Company shall carry out necessary supervisions to ensure that.

SECTION 6

6. RIGHTS OF PERSONAL DATA OWNER, EXERCISE AND EVALUATION OF RIGHTS

6.1. Informing Personal Data Owner

In accordance with Article 10 of the Law, the Company shall inform Personal Data Owners during possession of Personal Data. In this regard, the Company shall provide brief information on its manager’s credentials, the processing purposes of Personal Data, transferees and transfer conditions, Personal Data collection method, legal causes and Personal Data Owner’s rights.

6.2. Rights of Personal Data Owner under Personal Data Protection Law (PDPL)

In accordance with Article 10 of the Law, the Company shall inform you about your rights, guide you on know-hows of practising them and carry out internal audits and take necessary technical and administrative measures. In accordance with Article 11 of the Law, the Company shall inform Personal Data Owners on their rights to:

- Verify whether their Personal Data are processed or not;
- Request information on processing of their Personal Data if processed;
- Receive information on the processing purpose of their Personal Data and whether they are used for their purposes or not;
- Get to know third party transferees whether within the borders or abroad;
- Request correction in the event of misprocessing of Personal Data;
- Request erasure and deletion of Personal Data in accordance with Article 7 of the Law;
- Request notification of transferees on actions taken in accordance with Paragraphs (d) and (e) of Article 11 of the Law;
- To object against consequences arising out of fully-automatic processing of Personal Data, and;
- To request indemnification in the event of unlawful processing of Personal Data.

6.3. Cases Annuling Exercise of Rights of Data Owner

According to Article 28 of the Law, Personal Data Owners cannot exercise their rights specified in Clause 6.2 of this Policy in the event of the following as they are excluded from the Law:

- Processing of Personal Data by real persons for purposes in connection with persons who stay with them or in the same building, providing not disclosing them to third persons or compliance with data security provisions;
- Processing of Personal Data for purposes such as planning and statistics by anonymising them with official statistics;
- Processing of Personal Data for purposes such as arts, history, literature, scientific purposes or freedom of expression, providing non-violation of national defence and security, public security and order, economical security, right to privacy or personal rights and non-incrimination;
- Processing of Personal Data for preventive, protective or intelligence activities carried out by legally or officially authorized bodies or companies in order to ensure national defence and security, public security and order and economical security, and;
- Processing of Personal Data by legal authorities or enforcement offices for proceedings, jurisdiction and enforcement procedures.

According to Article 28/2 of the Law, Personal Data Owners cannot exercise their rights specified in Clause 6.2 of this Policy, except right to request indemnification:

- Necessity of processing Personal Data for prevention or investigation of a crime;
- Processing of Personal Data publicized by the Data Owner himself/herself/themselves;
- Necessity of processing Personal Data by authorized bodies, firms or professional organizations for audits and amendments and disciplinary proceedings, and;
- Necessity of processing Personal Data to protect economical and financial interests of the State in budget, tax and financial issues.

6.4. Exercise of Personal Data Owner's Rights

In accordance with Article 13/1 of the Law, Personal Data Owners can communicate their requests and demands regarding the exercise of their rights specified in Clause 6.2 of this Policy in written or in other methods set forth by the PDP Commission. By this force, the communication channels and methods for communicating requests to the Company in line with Article 11 of the Law are listed below. Personal Data Owners can communicate their requests to the Company by filling the Application Form available on www.filpa.com.tr free of charge.

Personal Data Owners can communicate their requests, regarding information and documents connected with their credentials (register copies) with the exercise of their rights specified in Article 11 of the Law by;

- Printing and filling out the Application Form uploaded to www.filpa.com.tr website or; Submit a signed copy of the Form, along with documents showing your credentials, to the address 'Adana Haci Sabanci Organize Sanayi Bolgesi OSB Sabanci Cad. No: 8/2 Saricam / ADANA' by certified mail, the relevant notary office or in other ways specified in the Law (*The envelope should bear "Request for Information on Personal Data Protection Law"*).
- Submitting the Form to filpaambalaj@hs02.kep.tr e-mail address, bearing a "secure e-signature" specified in the Electronic Signature Act #5070 (*E-mail subject tab should include "Request for Information on Personal Data Protection Law"*).

The Company shall reserve its right to refusal in the event that you communicate wrong information or documentation or the application is unauthorized.

If Personal Data Owners intend to request information by their third party proxies, they should have a letter of proxy prepared between themselves and their proxies.

6.5. Company's Respond to Applications and Timetable of Response

Depending on the nature of the request, the Company shall response to all requests free of charge as soon as possible, in 30 days at the latest. If expenses should be incurred in order to conclude a transaction, on the other hand, expenses might be deducted at the amounts established according to the tariff specified by the PDP Commission. The Company might refuse a request accompanied by a reason for refusal, as well as accepting - it shall submit their response in written or electronically. If the request written in the Application Form is accepted, the Company shall do whatever is necessary to conclude that request.

6.6. Personal Data Owner's Right to File a Complaint at Personal Data Protection Commission

In the events of unfair refusal, insufficient response or failure to respond within the specified period, the Personal Data Owner shall have right to file a complaint to the PDP Commission in 30 days from the date of response or 60 days from the date of application.

SECTION 7

7. PROCESSING FOOTAGES

In accordance with the provisions set forth in the Law and the Policy, the Company shall record footages of visitors, employees and other persons and store them in physical or electronical formats for a reasonable period to ensure sufficient level of general and commercial security in its enterprises and plants.

For information purposes, the monitored areas shall be furnished with remarkable attention signs warning Personal Data Owners that that place is monitored. By force of the business activities herein, the Company shall precisely comply with all responsibilities conferred in the Law and other regulations. Highly-private areas, on the other hand, shall not be monitored.

SECTION 8

8. COMPANY'S MANAGEMENT STRUCTURE UNDER PERSONAL DATA PROCESSING AND PROTECTION POLICY

The Personal Data Commission has been formed upon the executive solution of the Company to manage this Policy and other related policies. The Personal Data Commission is the sole and exclusive competent authority to pursue actions to ensure that Personal Data Owners' Personal Data are stored and processed in line with the Law, the Policy and other related policies.

SECTION 9

9. MISCELLANEOUS

9.1. Update and Orientation

In the event of any discrepancy between the PDPL and applicable regulations and the Policy, the PDPL and applicable regulations herein shall be effective.

The Company shall be entitled to make amendments on this Policy or other related policies upon amendments on the Law, PDP Commission resolution or developments in the field or information sector.

Any amendments made on this Policy shall be immediately applied to the text and descriptions of the amendment shall be included at the end of the Policy.

9.2. Amendments

Personal Data Processing and Protection Policy has been issued in 3rd of September, 2019.

No previous amendment available

9.3. Validity

Formed by the Company, this Policy has come into force from 3rd of September, 2019.

9.4. Distribution

This Policy is available on the Company's website to third parties and the Company's employees.

9.5. Attachments

ATTACHMENT - 1 : FİLPAAMB.VE DIŞ TİC. A.Ş. Personal Data Processing Clarification Text

ATTACHMENT - 2 : FİLPAAMB.VE DIŞ TİC. A.Ş. Data Owner's Application Form under Personal Data Protection Law