**KVK POLICY OF PRİNTPARK OFSET VE AMBALAJ SAN.TİC.A.Ş.**

1. **INTRODUCTION**
	1. **General**

Ensuring the confidentiality and security of personal data and compliance with the relevant legal regulations are among the PRİNTPARK OFSET VE AMBALAJ SAN.TİC.A.Ş. ’s ("Company") top priorities, and utmost care is taken in this regard. In this context, the process managed by this KVK Policy on the processing and protection of personal data ('' Policy '') and other written policies within the Company and the targeted aim is to process, store and protect data the personal data of our employees, employee candidates, visitors and other third parties (''Relevant Persons'') is in accordance with the law and to reflect our corporate culture.

In the preparation of this Policy, we see Constitution of Turkey and 6698 numbered Personal Data Protection Act (the ''**KVKK**'') located regulations, especially in the legal norms relevant for the protection of personal data and the Personal Data Protection Committee of the provisions in the decision as a guide to our company. In this Policy, explanations regarding the following basic principles adopted by our Company for the processing of personal data will be made:

* + - Processing of personal data in accordance with the law and good faith,
		- Keeping personal data accurate and up-to-date when necessary,
		- Processing of personal data for specific, clear and legitimate purposes,
		- Being linked, limited and measured with the purpose for which personal data are processed,
		- Keeping personal data for the period stipulated in the relevant legislation or for the purpose for which they are processed,
		- Enlightening the relevant persons,
		- Establishing necessary processes for the relevant persons to exercise their rights,
		- Taking necessary measures in the processing and preservation of personal data,
		- Transfer of personal data to third parties in line with the requirements of the processing purpose,
		- Showing the necessary sensitivity in the processing and protection of special quality personal data,
		- Deletion, destruction or anonymization of personal data whose processing purpose has been lost.
	1. **Purpose of the Policy**

The main purpose of this Policy is to make explanations about the personal data processing activities carried out by our Company in accordance with the law and the procedures adopted for the protection of personal data and to inform the Relevant Persons in this context and to ensure transparency. In addition, this KVK Policy and other written policies aim to make our principle of compliance with KVKK and other relevant legal regulations regarding personal data security sustainable.

* 1. **Scope of the Policy**

The scope of this policy is for real persons whose personal data are processed by our Company automatically or by non-automatic means provided that they are part of any data recording system, and an Internal Directive on the Protection of Personal Data has been created within the scope of this Policy.

* 1. **Implementation of the Policy and Relevant Legislation**

This Policy has been concretized and organized within the principles set forth by the relevant legislation. Our company undertakes and accepts that in case of inconsistency between the current legislation and this Policy, the applicable legislation will be applied.

* 1. **Enforcement of the Policy**

This policy enters into force after being approved by the Board of Directors of our Company, is published on the website (http://www.printpark.com/) and made available to the Related Persons in this way.

1. **TANIMLAR VE KISALTMALAR**

|  |  |
| --- | --- |
| **Explicit Consent**  | Consent on a specific subject, based on information and expressed with free will |
| **Constitution** | TR Constitution dated 1982 |
| **Anonymization** | Making personal data unable to be associated with an identified or identifiable natural person under any circumstances, even by matching other data. |
| **Employee** | Employees of PRİNTPARK OFSET VE AMBALAJ SAN.TİC.A.Ş.. |
| **Employee Candidate**  | Real persons who have applied for a job to our company in any way or who have submitted their curriculum vitae and related information to our Company for review. |
| **Related Person** | Real person whose personal data is processed |
| **Personal Data** | All kinds of information regarding an identified or identifiable natural person |
| **Processing of Personal Data** | All kinds of action performed on data such as obtaining, recording, storing, preserving, changing, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data, which are fully or partially automatic or non-automatic, provided that they are part of any data recording system. |
| **Committee** | Personal Data Protection Committee |
| **Board** | Personal Data Protection Board |
| **Institution** | Personal Data Protection Agency |
| **KVKK** | Law No. 6698 on the Protection of Personal Data |
| **Special Quality Personal Data** | Data on race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, attire, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data |
| **Periodic Destruction Process** | The deletion, destruction or anonymization process specified in the personal data storage and disposal policy and will be carried out |

|  |  |
| --- | --- |
|  | ex officio at repetitive intervals in the event that all the conditions for processing personal data in the Law are eliminated. |
| **Policy** | KVK Policy |
| **Potential Customer** | Persons who have requested to use our services or who have been evaluated in accordance with the rules of business practice and honesty. |
| **Company** | PRİNTPARK OFSET VE AMBALAJ SAN.TİC. A.Ş. |
| **Related Person Application Form** | Application form to be used by the relevant persons while using their applications regarding their rights stated in Article 11 of the KVKK. |
| **Data Processor**  | Real and legal person who processes personal data on behalf of the data controller based on the authority given by it |
| **Data Record System** | Registry system, directory where personal data are structured and processed according to certain criteria |
| **Data Responsible** | Natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system. |
| **Data Deleting** | Making personal data inaccessible and unavailable in any way for relevant users. |
| **Data Destruction** | Making personal data inaccessible, unrecoverable and reusable in any way. |
| **Visitor** | Real persons who enter the physical premises owned by the institution for various purposes or visit the websites |

1. **PRINCIPLES REGARDING THE PROCESSING OF PERSONAL DATA**
	1. **Processing of Personal Data in Compliance with the Principles Stipulated in Legislation**
		1. **Processing in Compliance with Law and Integrity Rules**

Our company has adopted the basic principle to comply with the law and the rules of honesty in all kinds of transactions on personal data. In this context, by adopting the principle of transparency, it informs the Related Persons about the purpose of use of the personal data collected through this Policy and other texts.

* + 1. **Ensuring Personal Data is Correct and Updated When Necessary**

Our company has a system and process to ensure the accuracy and up-to-datedness of the personal data it processes while conducting its personal data processing activity. In this context, Relevant Persons may make it possible to keep their personal data accurate and up-to-date by applying to our Company.

* + 1. **Processing for Specific, Explicit and Legitimate Purposes**

Our company clearly determines the purpose of processing personal data within legitimate and legal limits, and presents it to the Related Persons, through this Policy and other texts, before the personal data processing activity begins.

* + 1. **Being Connected, Limited and Measured with the Purposes for which They are Processed**

Our company processes personal data for the purposes required to carry out the activity in a proportionate and related manner to the field of activity. In this context, while carrying out data processing activities, it carefully avoids processing personal data that are not related to the realization of the purpose and are not needed now / in the future.

* + 1. **Retaining for the Period Stipulated in the Relevant Legislation or Required for the Purpose for which they are processed**

Our company preserves personal data only for the period specified in the relevant legislation or for the purpose for which they are processed. In this context, first of all, it is determined whether a period is determined in the relevant legislation for the storage of personal data, if a period is determined, the appropriate action is taken, and if a period is not specified, the time required for the purpose of processing each personal data is determined and kept for this period.

In this context, our Company prepares and implements a policy and directive for deletion, destruction or anonymization of personal data.

* 1. **Processing of Personal Data in Compliance with the Personal Data Processing**

**Conditions specified in Article 5 of the KVKK and Limited to These Conditions**

Our company processes personal data only based on the express consent of the Related Person or in cases where express consent is not sought in the KVKK, without express consent, in a manner limited to these conditions and conditions.

***3.2.1. Explicit Consent***

Explicit consent is the statement made by the Related Person with free will on a specific subject and based on information. Pursuant to Article 5/1 of the KVKK, our Company respects and abides by the explicit consent of the Relevant Person, if required in personal data processing.

***3.2.2. Cases Where Explicit Consent is not Required***

In Article 5/2 of the KVKK, it has accepted the processing of personal data in some cases without the explicit consent of the Related Person. Since obtaining explicit consent from the relevant person in the presence of any of the specified conditions will be considered as misleading the relevant person, our Company does not apply for express consent under these conditions below:

* + - 1. Existence of the provision of law,
			2. Cases of actual impossibilities,
			3. It is necessary to process the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of the contract,
			4. It is mandatory for the data controller to fulfill his legal obligation,
			5. The personal data of the relevant business have been developed by him / her,
			6. Data processing is mandatory for the establishment, use or protection of a right,
			7. Obligation of data processing for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the relevant person are not harmed.
		1. **Processing Special Quality Personal Data**

Our company shows maximum sensitivity in the processing and protection processes of personal data determined as "special quality" by the KVKK due to the risk of causing greater victimization or discrimination when processed, and the principles accepted for special quality personal data are discussed separately in this Policy.

Personal data of special nature can be processed by our company in the following cases, if the person concerned does not have the express consent of the person concerned, provided that adequate measures are taken by the Board.

1. Special quality personal data other than the health and sexual life of the person concerned, in cases stipulated by the law,
2. Special quality personal data regarding the health and sexual life of the person concerned can only be processed without the express consent of the person concerned by persons or authorized institutions and organizations under the obligation of secrecy for the purpose of protecting public health, conducting preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing.

Our Company has determined additional precautions and processes regarding the processing of special quality data and access to these data. In this context, the environments where private personal data are stored are protected by secondary lock and secondary passwords, and can only be processed by authorized persons within the framework of the authorization matrix.

* + 1. **Transfer of Personal Data**

Personal data are provided to supervisory institutions within the framework of auditing activities in order to fulfill the purposes specified in this Policy, to our shareholders for reasons arising from their supervision and partnership rights in accordance with the relevant legal regulations, to legally authorized public institutions and organizations, to our domestic and / or abroad suppliers and business partners, to real persons for whom services are provided or to third parties to whom services are provided within the framework of the personal data processing conditions and purposes specified in Article 8 and Article 9 of the KVKK.

1. **PRINCIPLES ON THE PROTECTION OF PERSONAL DATA**
	1. **Technical and Administrative Measures Taken by Our Company Regarding the Security of Personal Data**
		1. **Technical Precautions**

**The main technical measures taken by our company to ensure the legal processing of personal data and to prevent unlawful access to personal data are as follows:**

* + - * Personal data processing activities carried out within our company are audited by established technical systems.
			* Knowledgeable and experienced personnel are employed in technical matters..
			* Departments related to technical issues have been established.
			* The technical measures taken are periodically reported to the authorized unit / person as per the internal audit mechanism.
			* In order to ensure the safe storage of personal data, a legal backup program is used.
			* New technological developments are followed and technical measures are taken on systems, especially in the field of cyber security, the measures taken are periodically updated and renewed.
			* Access and authorization technical measures are used within the framework of legal compliance requirements specified in each department within our company.
			* Access authorizations are restricted, authorizations are regularly reviewed, former employees' accounts are closed.
			* Software and hardware including virus protection systems and firewalls are used.
			* The use of counterfeit software and hardware is strongly avoided. All of our products we use are original and licensed.

In this context, our Company is constantly working on the following technical measures determined by the Board:

* + - * Authorization Matrix
			* Authority Control
			* Access Logs
			* User Account Management
			* Network Security
			* Application Security
			* Encryption
			* Penetration Test
			* Intrusion Detection and Prevention Systems
			* Log Records
			* Data Masking
			* Data Loss Prevention Software
			* Backup
			* Firewalls
			* Current Anti-Virus Systems
			* Deletion, Destruction or Anonymization
			* Key Management
		1. **Administrative Measures**

The main administrative measures taken by our company to ensure the legal processing of personal data and to prevent unlawful access to personal data are as follows:

* + - * Our personnel are informed and trained on the law of protection of personal data and the processing of personal data in accordance with the law.
			* Personal data processing activities carried out by the business units of our company; the requirements to be fulfilled in order to ensure that these activities comply with the data processing conditions specified in the KVKK are examined for each business unit and the activity carried out.
			* With the agreements and documents that govern the legal relationship between our company and the employees, records imposing the obligation not to process, disclose and use personal data, except for the Company's instructions and exceptions imposed by law, are placed and the awareness of employees on this issue is increased.
			* In order to meet the legal compliance requirements determined on the basis of our business units, awareness is created and implemented specific to the relevant business units. Necessary administrative measures are implemented through internal policies and trainings to ensure the supervision of these issues and the continuity of the implementation.
			* Access to personal data and authorization processes are designed and implemented within our Company in accordance with activity-based legal compliance requirements.
			* It is followed by the Personal Data Protection Committee, which has been established for the convenience and compliance in the follow-up of the work and transactions related to the Personal Data Protection Law and related legal regulations.
			* In the contracts established by our company with third parties to whom personal data are legally transferred, provisions regarding that necessary security measures will be taken in order to protect the transferred personal data and that these measures will be followed in their own organizations.

In this context, our Company is constantly working on the following administrative measures determined by the Board:

* + - * Preparation of Personal Data Processing Inventory
			* Corporate Policies (Access, Information Security, Use, Storage and Destruction etc.)
			* Contracts (Between Data Controller - Data Controller, Data Controller - Data Processor)
			* Confidentiality Commitments
			* Internal Periodic and / or Random Inspections
			* Risk Analysis
			* Labor Contract, Discipline Regulation (Addition of Provisions According to Law)
			* Corporate Communication (Crisis Management, Informing the Board and Related Person Processes, Reputation Management etc.)
			* Training and Awareness Activities (Information Security and Law)
			* Notification to Data Controllers Registry Information System (VERBİS)
	1. **Raising Awareness and Control of Our Employees in the Field of Personal Data Protection**

Our company provides the necessary trainings and meetings to raise awareness to prevent unlawful processing of personal data, to prevent unlawful access to data and to ensure safe storage of data.

In order to increase the awareness of the current employees of our company about the protection of personal data, we work with professional people in case of need.

* 1. **Protection of Special Quality Personal Data**

Personal data determined by our company as special with KVKK and processed in accordance with the law are protected with precision. In this context, the technical and administrative measures taken by our Company for the protection of personal data have been determined on the basis of the relevant legal regulation and the "Adequate Precautions to be Taken by Data Controllers in the Processing of Specially Qualified Personal Data" published by the Personal Data Protection Authority, and carefully is implemented.

* 1. **The Process to be Followed in Case of Unauthorized Disclosure of Personal Data**

Our company will notify the relevant person and the Board within 72 hours if the personal data it processes are illegally obtained by others.

If deemed necessary by the Board, this may be announced on the Board's website or by any other method.

* 1. **Personal Data Inventory**

Each unit of our company creates an up-to-date personal data processing inventory. Unit manager is responsible for the accuracy, timeliness and submission of this inventory to the contact person when necessary. Up-to-date developments in keeping the inventories accurately, applying the current Company policy on the protection of personal data and protecting personal data are always followed.

1. **APPLICATION OF RELATED PERSONS TO THE DATA CONTROLLER, OUR COMMUNICATION CHANNELS AND THE EVALUATION PROCESS OF THE APPLICATION**
	1. **Subject of the Application**

Our company attaches great importance and value to the rights of the relevant people and we provide them with the opportunity and opportunity to exercise these rights. An Application Form for Data Supervisor has been prepared and published on our website by our company, where the relevant persons can easily submit their requests.

By applying to our company, in relation to themselves, everybody has right;

1. To learn whether personal data is processed or not,
2. To request information if personal data has been processed,
3. To learn the purpose of processing personal data and whether they are used appropriately for their purpose,

ç) To know the third parties to whom personal data are transferred domestically or abroad,

1. To request correction of personal data in case of incomplete or incorrect processing,
2. To request the deletion or destruction of personal data within the framework of the conditions stipulated in Article 7 of KVKK,
3. To request notification of the transactions made pursuant to subparagraphs (d) and (e) to third parties to whom personal data have been transferred,
4. To object to the occurrence of a result against the person itself by analyzing the processed data exclusively through automated systems,

ğ) In case of damage due to unlawful processing of personal data, to demand the compensation of the damage.

* 1. **Application Method and Address**

Our communication channels and method to use the above rights are as stated in the table below:

|  |  |  |
| --- | --- | --- |
| **Application Method** | **Application Address** | **Application Subject Heading** |
| *Application by hand (If the applicant applies to us, a document certifying the identity, and a notarized power of attorney must be available in case of an application by proxy.)* | …………………… | "*Request for Information within the Scope of the Law on Protection of Personal Data*" will be written on the envelope. |
| Notification through notary | ………………………… | "*Request for Information under the Law on Protection of Personal Data*" will be written in the notification envelope. |
| Email via E-signature / Mobile Signature | ………………………… | "*Request for Information under the Law on Protection of Personal Data*" will be written in the subject part of the e-mail. |
| Application via Registered Electronic Mail (KEP) address | ……………………… | "*Request for Information under the Law on Protection of Personal Data*" will be written in the subject part of the e-mail. |
| E-mail address registered in our systems (Your e-mail address must have previously been matched with your identity in our systems.) | ……………………… | "*Request for Information under the Law on Protection of Personal Data*" will be written in the subject part of the e-mail. |

* 1. **Post-Application Process**

Applications submitted to us are answered within 30 (thirty) days at the latest from the date of receipt of the request to our Company, depending on the nature of the request. Our responses are sent to the Data Supervisor based on the form of notification specified by the applicant in the Application Form.

In case the application is rejected in accordance with Article 14 of the KVKK, the response is found to be insufficient or the application is not answered in time; it can make a complaint to the Board within thirty days from the date our company learns its answer and in any case within sixty days from the date of application.

* 1. **Application Fee**

Applications are made free of charge as a rule. However, if the transaction requested by the relevant persons requires an additional cost, the fee in the tariff determined by the Board will be charged by our Company.

1. **ENLIGHTENING AND INFORMING RELATED PERSONS**

Our company, in accordance with the regulation in Article 10 of the KVKK, enlightens the relevant persons about the process of obtaining personal data through this Policy and the Clarification Text and other texts that are easily accessible on our website. In this context, our Company informs the relevant persons about the identity of the data controller, the purpose for which personal data will be processed, to whom and for what purpose the processed personal data can be transferred, the method and legal reason for collecting personal data and other rights of the person concerned.

An Application Form for Data Supervisor has been created and published on the website of our Company in order for the relevant Person to use his / her rights stated in the KVKK more easily. The relevant section is explained in detail under the title number 5.

1. **PROCESSING PURPOSES OF PERSONAL DATA AND STORAGE PERIOD**
	1. **Purposes of Processing Personal Data**

Our company processes personal data as personal data limited to the purposes and conditions within the personal data processing conditions specified in Article 5 and 6 of the KVKK. These terms and conditions;

* + - *The processing of personal data is clearly stipulated by the law for our Company to engage in relevant activities,*
		- *The processing of personal data by our Company is directly related and necessary with the establishment or performance of a contract,*
		- Processing of personal data is mandatory for our Company to fulfill its legal obligation,
		- The processing of your personal data by the Company in a limited way for the purpose of making you public, provided that it has been made public by the person concerned,
		- Processing of personal data by the Company is mandatory for the establishment, use or protection of a right of the Company,
		- It is mandatory to perform personal data processing for the legitimate interests of the Company, provided that the fundamental rights and freedoms of the relevant persons are not damaged,
		- It is compulsory for our company to process personal data for the protection of the life or body integrity of the relevant persons or another person, and in this case, the persons concerned are unable to disclose their consent due to the actual impossibility or legal invalidity,
		- Special quality personal data other than the health and sexual life of the relevant persons, in the cases stipulated by the law,
		- Special quality personal data related to the health and sexual life of the relevant persons are processed by persons or authorized institutions and organizations under the obligation of secrecy for the purpose of protecting public health, conducting preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing.
	1. **Storage Periods of Personal Data**

As a company, we keep personal data for the period specified in this legislation if it is stipulated in the relevant legislation. In addition, our obligations arising from the relevant contracts, our administrative and legal responsibilities / liabilities are also taken into account in determining the retention periods.

When the purpose of processing personal data has expired and the retention period determined by the relevant legislation and the company has reached the end, these personal data are deleted and backed up only to provide evidence in possible legal disputes or to assert the relevant right related to personal data. In this case, access to personal data is not provided for any other purpose. Personal data are destroyed or anonymized after the expiration of the periods specified in our Company's Personal Data Storage and Destruction Policy.

The processed personal data and personal data inventories are reviewed in 6-month periods and the personal data that need to be deleted / destroyed are deleted / destroyed within these 6-month periodic destruction periods and the transaction is recorded.

1. **PERSONAL DATA PROCESSING ACTIVITIES CARRIED OUT IN THE WORK AREAS**
	1. **Camera Monitoring Activity at the Entrances and Inside of the Work Areas**

In order to ensure the security of the Related Persons and our Company, our company performs personal data processing activities for the place where we serve and where we carry out these services, security camera monitoring activity at the entrance and inside of the work areas, and the tracking of entrances / exits and overtime. In this context, as the Company, we act in accordance with KVKK and other relevant legislation.

* 1. **Informing About Camera Monitoring Activity**

Relevant persons are enlightened by our company in accordance with Article 10 of the KVKK; in this way, it is aimed to prevent harm to the fundamental rights and freedoms of the persons concerned and to ensure transparency. For camera surveillance activities, the Company's website clarifies both with this Policy (online Policy) and a notification letter (on-site lighting / layered lighting) that it will be monitored at the entrances of the monitoring areas.

* 1. **Purpose and Limitation of Camera Monitoring**

As a company, we process personal data in connection with the purpose for which they are processed, in a limited and measured manner in accordance with KVKK. The purpose of continuing the video camera recording and monitoring activities by the company is limited to the purposes listed in this Policy.

Accordingly, the monitoring areas of security cameras, their number and when to be monitored are put into practice as sufficient and limited for this purpose.

* 1. **Ensuring the Security of Data Obtained by Camera Monitoring**

All necessary technical and administrative measures are taken by the company to ensure the security of personal data obtained through camera recording. Detailed information can be found in technical measures for data protection.

* 1. **8.5. People to Have Access the Information Obtained As A Result of Monitoring and Information Transferred**

Only authorized persons can access the information and storage environment obtained as a result of monitoring. The live camera images can be watched by the security guards who are employees of the Company or outsourced. A limited number of people who have access to the records declare that they will protect the confidentiality of the data they access with a confidentiality commitment.

* 1. **Guest Entry / Exit Tracking Executed at the Entrances and Inside of the Work Areas**

Personal data processing activities are carried out by the company and the outsourced company for the purposes of ensuring security and for the purposes specified in this Policy, for tracking guest entry and exit in the Company's work areas.

While obtaining the names and surnames of the persons who come to our work areas as guests, the relevant persons are enlightened through the texts posted in the relevant areas or made available to the guests in other ways. The data obtained for the purpose of tracking guest entry and exit are processed only for this purpose and the relevant personal data are recorded in the data recording system in physical and / or electronic media.

* 1. **Recording Information of Electronic Devices at the Entrances of Work Areas**

As a company, we record the MAC addresses of computers or similar electronic devices when our guests use their personal computers or similar electronic devices in connection with the care and sensitivity we show to the protection of information security and personal data. The reason for this is to ensure the security of our company and the people whose personal data are within our company.

1. **REVIEW**

This policy is approved by the Company's board of directors and becomes effective. Regarding the changes to be made in the policy, the approval of the person (s) to be authorized by the board of directors is obtained. The issues regarding the implementation of this policy within the Company have been systematized with the internal policies, procedures and internal guidelines. The policy is reviewed every 6 months and, if necessary, revisions are made regarding the approval of the authorized person.

1. **PERSONAL DATA PROTECTION COMMITTEE**

The company has appointed a contact person within the framework of personal data protection law. A committee of ….. persons was formed among the employees of the company units. The committee is chaired by the Company contact person. The contact person acts with the views and recommendations of the Committee on administrative and technical measures. With regard to administrative and technical measures, the principles determined by the Committee are taken into account. The Committee makes every effort to comply with the Company's personal data protection legislation. The contact person supervises the Company units for which he is responsible within the scope of personal data protection law. As a result of these audits, it warns the relevant units when necessary and informs the senior management about the situation. The contact person ensures the coordination of the relevant person applications made to the Company to be answered within the legal terms and in accordance with the procedure. The contact person manages the relations of the Company with the Personal Data Protection Authority.

1. **ENFORCEMENT**

This Policy comes into force as of the date it is accepted and announced by the company's board of directors / authorized bodies.