01.01.2020

FİSTAŞ Inc.

KVKK PERSONAL DATA STORAGE AND DESTRUCTION POLICY

Contents

1. INTRODUCTION

1.1 Purpose

FİSTAŞ Fantasy Yarn San. Ve Tic A.S.("**FİSTAŞ**" or "Company"), we pay the utmost attention and care to the protection of personal data and we observe the protection of personal data in accordance with the law in all our activities. We take all necessary administrative and technical measures regarding personal data processing activities carried out by us in accordance with the law.

This policy has been prepared in order to determine the procedures and principles regarding the business and transactions related to storage anddestruction activities.

FİSTAŞ; In line with the mission, vision and basic principles determined in the Strategic Plan; Processing personal data of company employees, employee candidates, service providers, visitors and other third parties in accordance with the Constitution of the Republic of Turkey, international agreements, the Law on the Protection of Personal Data No. 6698 ("Law") and other relevant legislation, and ensuring that the relevant persons use their rights effectively identified as a priority.

Work and transactions regarding the storage and destruction of personal data are carried out in accordance with the Policy prepared by the Company in this direction.

1.2 Scope

Personal data belonging to Company employees, employee candidates, service providers, visitors and other third parties are within the scope of this Policy, and this Policy is applied in all recording environments where personal data owned or managed by the Company are processed, and in activities for personal data processing.

2. DISTRIBUTION OF RESPONSIBILITIES AND DUTIES

All departments and employees of the company are responsible for the proper implementation of technical and administrative measures taken within the scope of the Policy, training and awareness of unit employees, monitoring and continuous supervision of personal data, prevention of illegal processing of personal data, prevention of unlawful access to personal data and protection of personal data. It actively supports the responsible units in taking technical and administrative measures to ensure data security in all environments where personal data is processed in order to ensure that it is stored in accordance with the law.

FİSTAŞA "Personal Data Protection Board" has been established in accordance with the decision of the Company's top management to manage the Personal Data Protection and Processing Policy and other policies related to and related to this Policy.

The Board consists of the units with the title, job unit and job description below, and the duties of the Board in the storage and destruction processes of personal data are given in Table 1.

Table 1: Task distribution of storage and disposal processes

Unit/Title	**Job Description**
Chairman of the Board **FINANCE DIRECTOR**	Convening the Board, implementing and executing policies, performing secretarial services and informing the Board of Directors about the process, following up the relations with the Personal Data Protection Board, following up and implementing the Board Decisions and managing the processes. Representation of the company before the Board.
RESPONSIBLE FOR INFORMATION PROCESSING	Creating, tracking, implementing, destroying and anonymizing information processing systems, creating the necessary mechanisms for transferring them in and out of the country, ensuring the security of data, proposing and implementing systems that provide data security.
HUMAN RESOURCES RESPONSIBLE	The Human Resources Officer is responsible for the execution and planning of FİSTAŞ human resources affairs, the execution of the Policies in accordance with their duties, and the appropriate protection of personal data.
QUALITY ASSURANCE RESPONSIBLE	It is responsible for preparing, developing, executing, publishing and updating the policies in relevant environments.

3. RECORDING ENVIRONMENTS

Personal data is stored securely by the Company in the environments listed in Table 2, in accordance with the law.

Table 2: Personal data storage environments

Electronic Media	Non-Electronic Media
Servers (Domain, backup, email, database, web, file sharing, etc.) - Software (office software, portal, EBYS, VERBIS.) - Information security devices (firewall, intrusion detection and prevention, log file, antivirus, etc.) - Personal computers (Desktop, laptop) - Mobile devices (phone, tablet, etc.) - Optical discs (CD, DVD, etc.) - Removable memories (USB, Memory Card etc.) - Printer, scanner, copier	- Paper - Manual data recording systems (survey forms, visitor logbook) - Written, printed, visual media

4. EXPLANATIONS ON STORAGE AND DISPOSAL

By the company; Personal data belonging to the employees, employee candidates, visitors and third parties in relation as service providers, the employees of the Company or the company affiliated to the company are stored and destroyed in accordance with the Law.

In this context, detailed explanations regarding storage and disposal are given below, respectively.

4.1 Remarks on Retention

Article 3 of the Law*processing of personal data*The concept of personal data processed in Article 4 is defined.*to be relevant, limited and proportionate to the purpose for which they are processed and to be kept for the period required for the purpose for which they are processed or stipulated in the relevant legislation.*It is stated that it is necessary, and in Articles 5 and 6 it is stated that *terms of processing personal data*counted.

Accordingly, personal data within the framework of our Company's activities,*It is stored for a period of time stipulated in the relevant legislation or suitable for our processing purposes.*

4.1.1 Legal Reasons for Retention

Personal data processed within the framework of the company's activities are kept for the period stipulated in the relevant legislation. In this context, personal data;

- Law No. 6698 on the Protection of Personal Data,
- Turkish Code of Obligations No. 6098,
- Labor Law No. 4857,
- Occupational Health and Safety Law No. 6331,
- Social Insurance and General Health Insurance Law No. 5510,
- Tax Procedure Law No. 213,
- Law on Access to Information No. 4982,
- Law No. 5651 on Regulation of Broadcasts on the Internet and Combating Crimes Committed Through These Broadcasts,

• Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Attachments,
• Regulation on Archive Services
• It is stored for as long as the storage periods stipulated in the framework of other secondary regulations in force in accordance with these laws.

4.1.2 Processing Purposes Requiring Storage

The Company stores the personal data it processes within the framework of its activities for the following purposes.

-Managing human resources processes.
-Providing company communication.
-Ensuring company security,
-To be able to do statistical studies.
-To be able to perform work and transactions as a result of signed contracts and protocols.
-Within the scope of VERBIS, employees, data controllers, contact persons, data controller representatives and data To determine the preferences and needs of the processors, to organize the services provided accordingly and to update them if necessary.
-To ensure the fulfillment of legal obligations as required or mandated by legal regulations.

-To liaise with real / legal persons who have a business relationship with the company.
-Making legal reports.
-Execution of Communication Activities (Managing call center processes)
-Obligation of proof as evidence in legal disputes that may arise in the future.
-Execution of Management Activities

4.2 Reasons for Disposal

Personal data;

• Amendment or repeal of the provisions of the relevant legislation, which are the basis for processing,
• The disappearance of the purpose that requires processing or storage,
• In cases where the processing of personal data takes place only on the basis of explicit consent, the data subject withdraws his explicit consent,
• Approval of the application made by the Company regarding the deletion and destruction of personal data within the framework of the rights of the person concerned, pursuant to Article 11 of the Law,
• In cases where the company rejects the application made by the person concerned for the deletion, destruction or anonymization of his personal data, finds the answer insufficient or does not respond within the time stipulated in the Law; Making a complaint to the Board and this request being approved by the Board,
• The maximum period for keeping personal data has passed and there are no conditions that justify keeping personal data for a longer period of time,

In such cases, it is deleted, destroyed or ex officio deleted, destroyed or anonymized by the Company upon the request of the person concerned.

5. TECHNICAL AND ADMINISTRATIVE MEASURES

In accordance with Article 12 of the Law and the fourth paragraph of Article 6 of the Law, in accordance with the adequate measures determined and announced by the Board for the personal data to be stored securely, illegally processed and accessed, and for the destruction of personal data in accordance with the law, the technical and administrative measures are taken.

5.1 Technical Measures

The technical measures taken by the company regarding the personal data it processes are listed below:

- Network security and application security are provided.
- Security measures are taken within the scope of procurement, development and maintenance of information technology systems.
- An authorization matrix has been created for
- employees. Access logs are kept regularly.
- The authorizations of employees who have a change in duty or quit their job in this field are
- removed. Current anti-virus systems are used.
- Firewalls are used. Personal data
- security is monitored.
- Necessary security measures are taken regarding entry and exit to physical environments containing personal data. The
- security of physical environments containing personal data against external risks (fire, flood, etc.) is ensured. The
- security of environments containing personal data is ensured.
- Personal data is backed up and the security of the backed up personal data is also ensured. User
- account management and authorization control system are implemented and these are also
- followed. Log records are kept without user intervention.
- Intrusion detection and prevention systems are used.
- Cyber security measures have been taken and their implementation is constantly
- monitored. Data loss prevention software is used.

5.2 Administrative Measures

The administrative measures taken by the Company regarding the personal data it processes are listed below:

- The representative and contact person of the data controller, who will be responsible for the protection of personal data within the company and will observe the relevant rules, has been selected.
- Before starting to process personal data, the Company fulfills its obligation to inform the relevant persons. is brought.
- In-company access to stored personal data is limited to only the personnel required to access it, as per the job description.
- In case the processed personal data is obtained by others unlawfully, it notifies the relevant person and the Board as soon as possible with the form available on the Board's website.
- Regarding the sharing of personal data, data security is ensured by signing a framework agreement on the protection of personal data and data security with the persons to whom personal data is shared, or by the provisions added to the existing agreement.
- Unlawful processing of personal data in order to improve the quality of employees Trainings are provided on the prevention of illegal access to personal data, the protection of personal data, communication techniques, technical knowledge and skills, Law No. 4857 and other relevant legislation.
- The Company carries out the necessary audits in order to ensure the implementation of the provisions of the Law. Confidentiality and security vulnerabilities that arise as a result of audits are eliminated.
- A letter of undertaking containing confidentiality provisions has been signed with the personnel for the protection
- of personal data. Devices such as laptops, desktop computers or smartphones, which are embezzled and personal data are processed, are delivered to the personnel only with the password notified to the personnel and authorized units, and if the password is known by third parties, necessary information is given about changing the password.
- Access of personnel to third cloud and file transfer systems, including file transfer, has been blocked.

- Personal data processing inventory has been prepared.
- Periodic and random audits are carried out within the company.

6. PERSONAL DATA DISPOSAL TECHNIQUES

At the end of the storage period required for the period stipulated in the relevant legislation or for the purpose for which they are processed, the personal data shall be collected by the Company ex officio or upon the application of the relevant person in accordance with the provisions of the relevant legislation.

disposed of using the following techniques.

6.1 Deletion of Personal Data

Personal data is deleted with the methods given in Table-3.

Table 3: Deletion of Personal Data

Data Recording Environment	Explanation
On servers Place **Area** **Personal Data**	The system administrator removes the access authorization of the relevant users and deletes the personal data on the servers for those whose period of time has expired.
Electronic in the environment Place **Field Personal Data**	Among the personal data in the electronic environment, the ones whose period has expired are rendered inaccessible and non-reusable for other employees (related users) except the database administrator.
Personal Data in Physical Environment	Among the personal data kept in the physical environment, it is made inaccessible and non-usable in any way for other employees, except for the unit manager responsible for the document archive, for those whose period of time has expired. In addition, the process of blackening is applied by drawing/painting/erasing in a way that cannot be read.
Portable in the media **Personal Data Found**	Of the personal data kept in flash-based storage media, the expired ones are encrypted by the system administrator and the access authorization is given only to the system administrator, and they are stored in secure environments with encryption keys.

6.2 Destruction of Personal Data

Personal data is destroyed by the methods given in Table-4 by the Company.

Table 4: Destruction of Personal Data

Data Recording Environment	Explanation
Personal Data in Physical Environment	Of the personal data in the paper medium, the ones that need to be kept, which have expired, are irreversibly destroyed in the paper clipping machines.
Personal Data in Optical / Magnetic Media	The physical destruction of the personal data in optical media and magnetic media, such as melting, burning or pulverizing, is applied. In addition, magnetic media is passed through a special device, and the data on it is rendered unreadable by exposing it to a high magnetic field.

6.3 Anonymization of Personal Data

Anonymization of personal data means that personal data cannot be associated with an identified or identifiable natural person under any circumstances, even if it is matched with other data.

In order for personal data to be anonymized; recording environment and related activity, such as returning personal data by the data controller or third parties and/or matching the data with other data

It must be rendered unrelated to an identified or identifiable natural person, even through the use of appropriate techniques for its field.

7. STORAGE AND DISPOSAL TIMES

Regarding the personal data being processed by the Company within the scope of its activities;

- The retention periods on the basis of personal data regarding all personal data within the scope of the activities carried out in connection with the processes are in the Personal Data Processing Inventory;
- Storage periods on the basis of data categories are recorded in VERBIS;
- Process-based retention periods are included in the Personal Data Retention and Disposal Policy.

If necessary, updates are made on the storage periods in question by the Quality Department.

The deletion, destruction or anonymization of personal data whose storage period has expired is carried out by the INFORMATION PROCESSING Department.

The storage and destruction periods of personal data obtained by FİSTAŞ in accordance with the provisions of the Law and other relevant legislation are determined within the framework of the following principles;

a) If the relevant legislation or the Board decision regulates how long the personal data will be kept, this period is complied with.

b) If the legislation or Board decision does not regulate how long the personal data will be stored, a limited period of time is determined in accordance with the purpose of keeping the personal data, taking into account the above-mentioned principles. Accordingly, your personal data processed in your personnel file or due to the employer-employee relationship will be processed during your employment contract and after the termination of the employment contract, in accordance with the relevant statute of limitations.**5 (five)**or **10 (ten)**throughout the year, health data in accordance with the legislation**15 (fifteen)**It will be stored throughout the year. In case of a change in legislation, this period may be updated in accordance with the change in legislation.

Personal data whose storage period has expired and whose destruction period has come,**6 month old**It is destroyed in accordance with the procedures specified in the Policy during the destruction processes carried out periodically at intervals, and all transactions are recorded and at least**3 years**is stored for a period of time.

8. PERIODIC DISPOSAL TIME

Pursuant to Article 11 of the Regulation, the Company determines the period of periodic destruction.**6 months**determined as. Accordingly, the Company performs periodic destruction in June and December every year.

9. PUBLICATION AND STORAGE OF THE POLICY

The policy is published in two different media, with wet signature (printed paper) and electronically, and is disclosed to the public on the website. The printed paper copy is also kept by the Quality Department.

10. POLICY UPDATE PERIOD

The policy is reviewed as needed and the necessary sections are updated.

11. ENFORCEMENT AND REVOCATION OF THE POLICY

The policy is deemed to have entered into force after its publication on the Company's website. In the event that it is decided to be annulled, the wet signed old copies of the Policy are canceled and signed by the Quality Department (with a cancellation stamp or written cancellation) and at least**5 years**It is kept by the Quality Department for a period of time.

Annex-1 Abbreviations and Definitions

Buyer Group	:	The category of natural or legal person to whom personal data is transferred by the data controller.
Open Consent	:	Consent on a particular subject, based on information and expressed with free will.
Anonymization	:	Making personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching with other data.
Worker	:	FISTA staff.
EBYS	:	Electronic Document Management System
Electronic environment	:	Environments where personal data can be created, read, changed and written by electronic devices.
Non-Electronic Environment	:	All written, printed, visual etc. other than electronic media. other environments.
Service provider	:	A natural or legal person who provides services within the framework of a certain contract with FİSTAŞ.
Related person	:	The natural person whose personal data is processed.
Related User	:	Persons who process personal data within the organization of the data controller or in line with the authorization and instruction received from the data controller, excluding the person or unit responsible for the technical storage, protection and backup of the data.
Destruction	:	Deletion, destruction or anonymization of personal data.
Law	:	Law on Protection of Personal Data No. 6698.
Recording Media	:	Any environment where personal data is processed wholly or partially automatically or by non-automatic means provided that it is a part of any data recording system.
Personal Data	:	Any information relating to an identified or identifiable natural person.
Personal Data Processing inventory	:	Personal data processing activities carried out by data controllers depending on their business processes; The inventory, which is created by associating the personal data processing purposes and legal reason, data category, transferred recipient group and data subject group, by explaining the maximum storage period required for the purposes for which personal data is processed, personal data foreseen to be transferred to foreign countries, and the measures taken regarding data security.
Your Personal Data Processing	:	Obtaining, recording, storing, storing, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data in whole or in part by automatic or non-automatic means provided that it is a part of any data recording system Any operation performed on data such as
Board	:	Personal Data Protection Board
Special Qualified Personal Data	:	Data on race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, costume and clothing, membership in associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.
Periodic Destruction	:	The deletion, destruction or anonymization process that will be carried out ex officio at repetitive intervals and specified in the personal data storage and destruction policy, in the event that all of the personal data processing conditions in the law are eliminated.
Policy	:	Personal Data Retention and Disposal Policy
Data Processor	:	The natural or legal person who processes personal data on behalf of the data controller, based on the authority given by the data controller.
Data Controller	:	The 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 Controllers Registry Information System	:	An information system created and managed by the Presidency, accessible over the internet, to be used by the data controllers in the application to the Registry and other related transactions related to the Registry.
VERBIS	:	Data Controllers Registry Information System
regulation	:	Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette dated 28 October 2017.