PERSONAL DATA OF EMPLOYEES CONSERVATION AND PROCESSING POLICY

1. Introductry

Erensoy Food and Packaging Mak. Singing. ve Tic. Ltd. Sti. (hereinafter referred to as the "Data Controller"), has a high sensitivity to comply with legal regulations in accordance with the ethical values that support its commercial assets and successes, and establishes all kinds of necessary structures within the framework of compliance with the legislation on the protection of personal data.

The Policy on the Protection and Processing of Personal Data of the Employees (hereinafter referred to as the Policy on the Protection and Processing of the Personal Data of the Employees or the Policy) and the principles and principles adopted in the processing of the data of the employees who have an employment relationship with the Data Controller, and in this context, the personal data processing carried out by the Data Controller is regulated. Legal security of data owners is ensured and transparency is ensured in its activities.

The Policy on the Protection and Processing of Personal Data of the Employees is defined in the Law on the Protection of Personal Data No. 6698 (hereinafter referred to as the "KVK Law") regarding the activities carried out by the Data Controller regarding all the personal data of the Company employees processed automatically or non-automatically, provided that they are part of any data recording system. Within the scope of compliance with the regulations, the basic principles and the principles to be fulfilled by the Data Controller are determined.

Although this Policy has a parallel content with the relevant legislation, in case of conflict between the Policy and the applicable legislation, the provisions of the legislation will be applied.

2. DATA SPEAKER

Data Controller; Pursuant to the KVK Law, it has the title of "data controller" in the personal data processing activities for which it determines the purposes and means, and announces to the public the obligations it has acquired due to this policy and the title of data controller.

3. DEFINITIONS

The important definitions in the KVK Policy and the legislation are given in the table below with their meanings:

Personal Data	Any information relating to an identified or identifiable natural person
Private Personal Data	Data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data
Data Owner	Specific or identifiable natural person whose personal data is processed (Relevant person)
Open Consent	Consent on a specific 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 it with other data.
Processing of Personal Data	All kinds of operations performed on data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data.
Data Responsible	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 Processor	A natural or legal person outside the organization that processes personal data on behalf of the data controller, based on the authority given by the data controller.
KVK Law (Law)	Published in the Official Gazette dated 7 April 2016 and numbered 29677, Law on Protection of Personal Data dated March 24, 2016 and numbered 6698
KVK Board	Personal Data Protection Board

KVK Institution (Institution)	Personal Data Protection Authority
VERBİS	Data Controllers Registry, which is kept open to the public in the Presidency of the Personal Data Protection Authority, under the supervision of the KVK Board

Data Controller (Company)	Erensoy Gıda ve Ambalaj Mak. San. ve Tic. Ltd. Şti.
Data Controller Work partners	Persons with whom the Data Controller cooperates due to commercial relations
Data Controller KVK Storage and Disposal Policy	The policy issued by the Data Controller, which regulates the processes of storage, deletion, destruction and anonymization of the personal data it contains.
Data Controller suppliers	Third parties providing services to the Data Controller on a contract basis
Data Controller Data Owner Application Form	The application form to be used by data owners when using their applications regarding their rights in Article 11 of the KVK Law.
Data Controller KVK Policy	Data Controller Personal Data Processing and Protection Policy
Group Companies	Group companies within the body of Data Controller
Personal Data Processing inventory	Personal data processing activities carried out by data controllers depending on their business processes; The inventory they have created by associating with the personal data processing purposes and legal reason, the data category, the transferred recipient group and the data subject group, explaining the maximum storage period required for the purposes for which the personal data is processed, the personal data to be transferred to foreign countries, and the measures taken regarding data security.
Data Controllers About the Registry regulation	Regulation on Data Controllers Registry, which entered into force on 1 January 2018, published in the Official Gazette dated 30 December 2017 and numbered 30286
Data security board	The Board, which will provide the necessary coordination within the Company within the scope of ensuring, maintaining and maintaining compliance with the personal data protection legislation by the Data Controller.

4. DATA SECURITY BOARD

Data Security Board; It is the unit responsible for the protection of the personal data processed within the body of the Data Controller and the monitoring of the compliance process with the personal data protection legislation. It consists of representatives of Finance and Human Resources departments.

Necessary meetings are held when deemed necessary by the Board or upon request. The revision of the policies and their compliance with the legislation are controlled by the Data Security Board. In this context, the following activities and other compliance processes are carried out by the Data Security Board:

a) Carrying out the necessary roles and assignments in the field of personal data protection,

b) To take and enforce the necessary measures in order to prevent the illegal transfer, access, disclosure of personal data and other issues that may create a lack of security, in accordance with the Law and Board decisions,

c) Performing audits regarding the implementation of measures and administrative decisions regarding data security,

d) If necessary, implementation of additional measures regarding the protection of sensitive personal data,

e) Organizing trainings, if necessary, in order to ensure a data protection culture within the company,

f) Ensuring the implementation of the relevant documents in terms of compliance with the legislation and carrying out the necessary audits,

g) Monitoring whether the group companies fulfill their obligations arising from the legislation,

h) Following up the relations with the KVK Institution and the KVK Board.

4.1. ROLE AND TASKS

For the communication to be established with the Institution, the decision regarding the replacement of the "Contact person" who will perform the VERBIS registration and information entry operations is made by the Data Security Board and the Board of Directors.

According to the “Personal Data Owner Relations Manual”, …….. “Data Controller Representative” Data Security Board decision or Board of Directors decision, who will perform the duties of 'controlling the data owner relations and the functionality of the relevant mechanisms'. assigned with.

In addition to the above-mentioned minimum duties, some additional duties and responsibilities may be assigned to the officials to be appointed due to the needs to be felt for ensuring compliance with personal data privacy.

4.2. PREPARATION OF POLICY, PROCEDURE, GUIDELINES AND GUIDELINES

By the Data Security Board in order to ensure compliance with the personal data protection legislation; On behalf of the Data Controller, the revision of the documents written below is provided in the capacity of the data controller.

1. Personal Data Protection Policy
2. Personal Data Retention and Disposal Policy
3. Personal Data Breach Procedure
4. Policy on Protection and Processing of Personal Data of Employees
5. Other texts required by law

6. POLICY PRINCIPLES

5.1. BASIC PRINCIPLES

The following basic principles are adopted by the Data Controller during the processing of personal data.

5.1.1. Processing personal data in accordance with the law and honesty rules

The Data Controller carries out personal data processing activities, in particular the Constitution of the Republic of Turkey and the KVK Law, in accordance with the data privacy legislation and the rule of good faith.

5.1.2. Ensuring the accuracy and up-to-dateness of the personal data processed

The Data Controller ensures the accuracy and up-to-dateness of the personal data he processes, and takes the necessary administrative and technical measures within this framework and continues the process follow-up.

5.1.3. Processing personal data in a limited and measured way in connection with the purpose

Data Controller; processes personal data in connection with the data processing conditions and as necessary for the performance of these services. In this context; The purpose of processing personal data is determined before starting the personal data processing activity. In other words, personal data is not processed only with the assumption that it can be used in the future (preserving personal data is also a data processing activity). In this context, the Data Controller takes into account the fundamental rights of data owners and their own legitimate interests.

5.1.4. Keeping personal data for as long as required by the relevant legislation or for the purpose for which they are processed

Data Controller; processes personal data for a period of time that will comply with this period, if a period is stipulated in the relevant legislation. If there is no regulation in this direction in the legislation, it keeps the data limited to the period required by the data processing purpose. Data Controller; It destroys personal data by deletion, destruction or anonymization methods in case the period stipulated in the legislation expires or the reasons requiring the processing of personal data disappear. In this context, the Personal Data Retention and Disposal Policy of the Data Controller, which has been created, is complied with.

5.2. LEGAL PROCESSING ACTIVITY

Data Controller; while engaging in the processing of personal data; It acts in accordance with the data processing conditions determined in Articles 5 and 6 of the KVK Law, provided that it also complies with the basic principles.

Data Controller, the law of personal data It establishes the necessary mechanisms in its internal systems to process it in accordance with the law. In addition, it carries out the continuity of the process sensitively by providing personnel awareness on data privacy through in-house trainings.

Data Controller; Within the scope of the processing of personal data, it operates in parallel with the rules set forth in the Constitution of the Republic of Turkey, the Turkish Penal Code No. 5237, the KVK Law and other legislation, and the Data Controller KVK Policy.

5.2.1. Data Processing Terms

Personal data is processed in accordance with the legislation and Board decisions, provided that the explicit consent of the Data Owner is obtained. If at least one of the following conditions is met, data processing activities can be carried out without seeking explicit consent:

– Explicit consent: Data processing as a result of obtaining consent of the personal data owner with free will, in accordance with the law, on a specific subject, based on information.

– Envisioned/obligatory in the law: Data processing if there is a clear provision in the legislation regarding the processing of personal data or if it is an obligation within the scope of the legal obligations of the Data Processor.

– Failure to obtain explicit consent due to actual impossibility: Processing the relevant data if the data owner is unable to give explicit consent due to actual impossibility or if his consent cannot be validated, and if it is necessary for the protection of the life or physical integrity of the data owner or a third party.

– Connection with the contract: Processing of the personal data of the parties, if necessary and directly related to the establishment or performance of a contract.

– Publication of personal data by the data owner: In case the data is made public directly by the Data Owner, data processing limited to the scope of publicization.

– Processing personal data if data processing is necessary for the establishment, exercise or protection of a right.

– Legitimate interests of the data controller: Data processing when required by the legitimate interests of the Data Controller, provided that the fundamental rights and freedoms of the Data Owner are preserved.

5.2.2. Special Qualified Personal Data Processing Conditions

Special categories of personal data, if the following conditions are met; can be processed within the framework of express consent in accordance with Article 6 of the Law in accordance with the relevant legislation, Board decisions and the policies implemented by the Data Owner.

5.2.3 Special Cases Subject to Data Processing Activity

– Providing fringe rights and benefits arising from the Labor Law,

– Ensuring equality of opportunity,

– Preventing illegal violations,

– Giving references,

Processing in company mergers and acquisitions and other transactions that change the company structure,

– Processing your personal data in disciplinary investigations and audit processes

– Separate storage of health data and persons authorized to process health data

– Alcohol and drug tests

– Processing of personal data regarding the use of electronic communication tools

– Processing of personal data related to the security camera application

– Processing of personal data regarding internet use

– Processing of personal data regarding vehicles allocated by the company

– Processing personal data within the scope of requesting information about employees from third parties

5.3. LEGAL DATA TRANSFER

By the Data Controller; In the sharing of personal data with group companies and third parties or sharing personal data with third parties, the personal data transfer conditions regulated in Articles 8 and 9 of the KVK Law are complied with. All necessary precautions and inspections are made to the third parties to whom the data is transferred, to ensure the security of the personal data in question.

5.3.1. Transfer of Personal Data

Personal data can be transferred upon the explicit consent of the Data Owner, or without the explicit consent of the data subject, provided that the necessary protective measures are applied in accordance with the legislation and the Data Owner's policies, in the presence of the following conditions:

– Explicit consent: Data transfer as a result of obtaining consent of the personal data owner with free will, in accordance with the law, on a specific subject, based on information.

– Envisioned/obligatory in the law: Data transfer if there is a clear provision in the legislation regarding the processing of personal data or if it is an obligation within the scope of the fulfillment of the legal obligations of the Data Controller.

– Failure to obtain explicit consent due to actual impossibility: Transfer of the relevant data if the data owner is unable to give explicit consent due to actual impossibility or if his consent cannot be validated, if it is necessary for the protection of the life or physical integrity of the data owner or a third party.

– Connection with the contract: The transfer of personal data of the parties, if necessary and directly related to the establishment or performance of a contract.

– On the side of the data owner of the personal data n publicisation: In case the data is made public directly by the Data Owner, data transfer limited to the scope of publicisation.

– Transfer of personal data if data processing is necessary for the establishment, exercise or protection of a right,

– Legitimate interests of the data controller: Data transfer when required by the legitimate interests of the Data Controller, provided that the fundamental rights and freedoms of the Data Owner are preserved.

5.3.2. Transfer of Private Personal Data

Provided that adequate technical and administrative security measures are established and the following conditions are met, special categories of personal data can be transferred:

– Special categories of personal data other than health and sexual life can be transferred without obtaining the explicit consent of the Data Owner, provided that it is expressly regulated in the law. If there is no regulation in this direction in the law, data can be transferred provided that the relevant person has express consent.

In case of the existence of the specified data transfer conditions, the relevant personal data is sent to the countries with adequate protection/safe as determined and announced by the Board, or in the absence of sufficient protection, to ensure adequate protection of the data controllers in Turkey and in the relevant foreign country in line with the data transfer conditions determined by the relevant legislation and the Board regulations. It can be transferred to foreign countries where the written commitment is obtained and the permission of the Board is obtained; Provided that the limitations and

conditions determined by the Board are complied with, it can be transferred abroad if the application of the Binding Company Rules is applied.

7. OBLIGATIONS

Employees are informed by the Company regarding the purposes for which Personal Data will be processed, to whom the data can be transferred, for what purposes data can be processed and transferred, and data collection methods. Within the scope of this information, employees are also informed about the rights they have regarding their data and how they will be used.

Data Controller; It complies with the obligations stipulated by the KVK Law for data controllers. In this context, the main issues that the Data Controller is obliged to comply with in this policy are listed below:

6.1. Obligation to Fulfill the Decisions Made by the KVK Board

Data Controller; It immediately implements the decisions notified by the KVK Board, which is the executive body of the KVK Institution, which regulates the personal data protection activities and is the administrative authority of our country in this field, in case of a complaint or as a result of the ex officio examination. It also adopts the policy decisions established by the KVK Board as data privacy rules.

6.2. Data Owner Relations Obligation

Data Controller; In its capacity as data controller, pursuant to Article 13 of the KVK Law, it concludes the requests of data owners regarding their personal data as soon as possible and within thirty (30) days at the latest, depending on the nature of the request.

In accordance with Article 11 of the KVK Law, Data Owners can use the following rights by applying to the Data Controller via the website address:

1. To learn whether personal data is processed or not,

2. To request information on personal data if it has been processed,

3. To learn the purpose of processing personal data and whether they are used in accordance with the purpose,

4. To know the third parties to whom personal data is transferred in the country or abroad,

5. Requesting correction of personal data in case of incomplete or incorrect processing and requesting notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,

6. To request the deletion or destruction of personal data in the event that the reasons requiring its processing disappear, although it has been processed in accordance with the provisions of the KVK Law and other relevant laws, and to request the notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,

7. Objecting to the emergence of a result against the person himself by analyzing the processed data exclusively through automated systems,

8. To request the removal of the damage in case of loss due to unlawful processing of personal data.

6.3. Obligation to Register and Notify the Data Controllers Registry

Data Controller; If it meets the criteria mentioned in the Regulation on the Data Controllers Registry, it is registered in the Data Controllers Registry in accordance with Article 16 of the KVK Law and the procedures and principles of the regulation.

6.4. Obligation to Inform the Data Owner

Data Controller; In accordance with Article 10 of the KVK Law and the Communiqué on the Procedures and Principles to be Complied with in Fulfilling the Obligation of Clarification, it carries out the necessary processes to ensure that the data owners are informed by the authorized persons during the acquisition of personal data. You can review the KVK Clarification Text published on the website for the purpose of fulfilling the lighting obligation.

6.5. Power of Personal Data Obligation to ensure safety

Conscious of the importance of ensuring the security of personal data and observing the fundamental rights and freedoms of data subjects, in accordance with Article 12 of the KVK Law, by the Data Controller;

1. To prevent the unlawful processing of personal data,

2. To prevent unlawful access to personal data and

3. To ensure the protection of personal data

All necessary technical and administrative measures are taken to ensure the appropriate level of security for its purposes. In addition, necessary audits are implemented within the scope of the operation of mechanisms to ensure data security.

8. ENSURING THE SECURITY OF PERSONAL DATA

The Data Controller takes all necessary measures, within the possibilities, according to the nature of the data to be protected, in order to prevent the unlawful processing of personal data, illegal access to personal data, or security deficiencies that may occur in other ways, and to ensure the safe keeping of personal data.

7.1. ADMINISTRATIVE MEASURES

– By the Data Controller; Personal Data Processing Inventory is created, which includes personal data categories, data owners, processing purposes and security measures taken.

– Necessary institutional policies and procedures regarding the protection of personal data are established and their functionality and continuity are ensured.

– Confidentiality agreements are signed with the employees.

– Awareness training and meetings are held to create awareness of data protection within the organization.

– In cases where personal data is subject to transfer, necessary measures are taken by group companies or third party companies.

– Legal provisions are added to employment contracts and disciplinary regulations.

– In case the conditions are met, the registration and information entry processes in the Data Controllers Registry Information System VERBIS are completed.

– Data Security provisions are added to the contracts signed with data processors.

7.2. TECHNICAL MEASURES

– By the Data Controller; The security of physical and electronic media containing personal data is ensured.

– Against malicious software, personal data is regularly backed up and the security of the backed up personal data is ensured.

– In order to ensure cyber security, preventive systems and software are established for information networks.

– Data Controller employees' access to personal data is created by constantly ensuring their duties and authority controls.

– Data security trainings are planned.

– Data penetration test standards are determined.

7.3. PERSONAL DATA VIOLATION

Data Controller; In case the processed personal data is obtained unlawfully by unauthorized persons, it notifies the KVK Board and the relevant data owners within 72 hours. For this reason, the Data Controller Data Breach Procedure (link) has been created; Within the scope of this procedure, all breach drills within the body of the Data Controller are set up by the Data Security Board.

9. DISPOSAL OF PERSONAL DATA

Data Controller; Pursuant to Article 7 of the KVK Law, it has created all necessary internal systems for the destruction of personal data in accordance with the Personal Data Retention and Destruction Policy, which it has created for the deletion, anonymization or destruction of personal data that has been processed in accordance with the law.

10. REVISION

This Policy enters into force from the moment it is approved by the Data Security Board. Except for the repeal of this Policy, the Data Security Board is authorized for the changes to be made in the Policy and how it will be put into effect.

The KVK Policy was published on the website by the Data Controller and presented to the public. In any case, this Policy is reviewed once a year, and if necessary changes are made, it is updated by submitting it to the Data Security Board for approval. In case of conflict between the applicable legislation, especially the KVK Law, and the regulations included in this Policy, the provisions of the legislation shall apply.

The Data Controller reserves the right to make changes in the KVK Policy in line with the legal regulations to be made by the KVK Institution, which is the administrative authority.

Revisions that may occur in this policy or legislation will be added to the policy by specifying the date and subject, and will be considered an integral part of the policy after the necessary announcements are made. The current version of the KVK Policy will be published on the website of the Data Controller.

PERSONAL DATA STORAGE AND DISPOSAL POLICY

1. OBJECTIVE AND SCOPE

Erensoy Food and Packaging Mak. Singing. ve Tic. Ltd. Sti. (hereinafter referred to as the "Data Controller"), has a high sensitivity to comply with legal regulations in accordance with the ethical values that support its commercial assets and successes, and establishes all kinds of necessary structures within the framework of compliance with the legislation on the protection of personal data.

Through the Personal Data Retention and Destruction Policy, the principles and principles adopted in the processes of keeping and destroying the personal data processed by the Data Controller are regulated.

The provisions of this Policy will be applied upon the disappearance of the reasons requiring the processing of the personal data processed in accordance with the law by the Data Controller or the request of the data owner for destruction.

2. BASIS

Personal Data Disposal Policy; Published in accordance with the KVK Law and the Regulation on the Deletion, Destruction or Anonymization of Personal Data; It has been prepared by influencing the Personal Data Protection and Processing Policy and the publications and guides published by the Personal Data Protection Authority.

3. DATA SPEAKER

Data Controller, who determines the purposes and means of processing personal data processed under his legal personality and is responsible for data processing; He is the data controller in accordance with the KVK Law.

In accordance with this policy; The Data Security Board is authorized in the destruction processes of personal data processed within the Data Controller.

4. DEFINITIONS

Data Controller's Personal Data Retention and Disposal Policy and important definitions in the legislation are given in the table below with their meanings:

Personal Data	Any information relating to an identified or identifiable natural person
Private Personal Data	Data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data
Data Owner	Specific or identifiable natural person whose personal data is processed (Relevant person)
Destruction of Personal Data	Deletion, destruction or anonymization of personal data

Processing of Personal Data	All kinds of operations performed on data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data.
Data Responsible	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
Periodic Destruction	When the personal data processing and storage period expires, the destruction process to be carried out by the Data Controller at repetitive intervals and Ex officio
KVK Law	Published in the Official Gazette dated 7 April 2016 and numbered 29677, Law on Protection of Personal Data dated March 24, 2016 and numbered 6698
Data Security Board	The Board, which will provide the necessary coordination within the Company within the scope of ensuring, maintaining and maintaining compliance with the personal data protection legislation by the Data Controller.
KVK Institution	Personal Data Protection Authority
Data Breach	In the law of protection of personal data; Unlawful access to the personal data processed by third parties

5. STORAGE OF PERSONAL DATA

Personal data stored with the Data Controller are kept in a recording environment in accordance with the nature of the relevant data and our legal obligations. Data Controller; takes the necessary administrative and technical measures in order to keep personal data safe and not be exposed to unlawful interventions. The Policy on the Protection and Processing of Personal Data is complied with regarding the measures taken regarding data security and the reasons for data retention.

The recording media used for the storage of personal data are generally listed below. However, some data may be kept in a different environment than the ones shown below due to their different qualities or due to the legal obligations of the Data Controller.

Physical environments	Personal data stored by paper and similar physical means
Electronic environments	Personal data within the body of the Data Controller and stored only on the server and external disks that the Data Controller has access to
Cloudy environments	Personal data stored using internet-based systems encrypted using cryptographic methods

6. DISPOSAL OF PERSONAL DATA

Destruction of personal data; It refers to the processes of deletion, destruction or anonymization of personal data that has lost the purpose of processing or requested by the data owner. If the existence of personal data is related to possible claims arising in accordance with contractual, commercial, legal and administrative transactions, the data is retained during the statute of limitations regarding the said transaction.

Personal data processed within the Data Controller; Upon the request of the person concerned, or if the reasons for data processing listed in Articles 5 and 6 of the KVK Law and the Data Controller Personal Data Protection and Processing Policy disappear, they are deleted, destroyed or anonymized ex officio in accordance with this Policy.

Data Security Board; It performs periodic destruction at 6-month intervals for all personal data being processed by the Data Controller.

7. DELETING PERSONAL DATA

Deletion of personal data; It is the process of making personal data inaccessible and unusable for the relevant users in any way. Deleted data cannot be accessed by relevant users other than the data controller.

If there is a conflict between the request and the company policy in this regard, a written application is made to the Personal Data Protection Authority in order to eliminate the conflict and action is taken in line with the policy decision.

By using an access authorization and control matrix or a similar system, the relevant users are determined for each personal data, and the authorizations and methods of the users such as access, retrieval, reuse are determined, and then the access, retrieval, reuse authorization and re-use of the personal data of the relevant users are determined. Procedures for closing and eliminating methods are carried out.

7.1. DELETING TECHNIQUES

7.1.1. BLACKOUT

It is the technique of making the personal data on the relevant document in the paper environment invisible to the users by cutting it where possible, otherwise using ink.

7.1.2. SECURE ERASE FROM DIGITAL MEDIA

Personal data on central servers and in the cloud are securely deleted with the delete command in the operating system.

8. DESTRUCTION OF PERSONAL DATA

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way. Destruction of personal data, unlike deletion, means that the data controller cannot access the said data after the destruction process.

8.1. EXTERMINATION TECHNIQUES

8.1.1. DE-MAGNETIZED

Magnetic media is passed through a demagnetizing device, corrupting the data in an unreadable way. De-magnetized device is provided by the Data Controller if needed.

8.1.2. PHYSICAL DESTRUCTION

Optical media and magnetic media are physically destroyed by melting, incinerating or pulverizing.

8.1.3. OVERWRITING

By writing random data consisting of 0s and 1s on magnetic media rewritable optical media at least seven times, recovery of old data is prevented. If necessary, software is provided by the company for this purpose.

8.1.4. SAFELY DISPOSAL FROM DIGITAL MEDIA

Personal data on central servers are irreversibly destroyed by the destroy command in the operating system.

9. ANNOUNCEMENT OF PERSONAL DATA

Anonymization of personal data; It is the process of making personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching it with other data. Data Controller; takes all kinds of security measures related to the anonymization of personal data.

9.1. TECHNIQUES OF ANNOUNCEMENT

In anonymizing personal data; There are techniques such as grouping, masking, derivation, generalization, and randomization. Data Controller; When choosing the anonymization method, the nature and size of the personal data, the structure and variety of the personal data in physical environments, the desired benefit / purpose of processing from the data, the frequency of processing the data, the reliability of the third parties to whom the personal data will be transferred, the meaningful effort required for anonymization, the deterioration of the anonymity of personal data. It takes into account the size of the damage that may arise in the event, the area of influence, the distribution / centrality rate of the data, the access authorization control of the users to the relevant data and the possibility of an attack that will disrupt the anonymity.

The storage reasons and durations of the personal data categories processed by the Data Controller are given in the table below. Every data that has expired is destroyed in the first subsequent periodic destruction period. This period may vary if necessary within the scope of the performance of legal and contractual obligations, and it is destroyed in the first periodic destruction period following the elimination of the relevant obligation.

Data Category	Storage Time	Reason for Hiding Reason for Hiding
Personnel Data	According to Law No. 5510, the document retention period is 10 years, starting from the beginning of the year following the relevant year of the document.	Fulfillment of obligations arising from employment contracts and legislation for employees
Health Information	According to the provisions of Occupational Health and Safety, the health files of the employees are kept for 10 years.	Ensuring occupational health and safety obligations
Professional experience	The CV information of the employee candidates is kept for 3 months.	Execution of the application processes of employee candidates
Identity and Contact Data	The contact information received regarding the customer and the prospective customer is stored for 10 years.	Conducting communication activities
Legal action	It is stored for 10 years from the date of transaction.	Responding to requests submitted by competent judicial / administrative institutions and authorities

Customer Transaction	TBK. It is stored for 10 years in accordance with the relevant provisions.	Execution of goods / services purchasing and sales processes and ensuring customer satisfaction
Finance and Accounting Data	TTK. art. According to 82, it is stored for 10 years.	Execution of finance and accounting works
Marketing Data	It is stored for 10 years from its acquisition.	Execution of marketing activities and studies
Criminal Conviction and Security Measures	It is stored for 10 years in accordance with the provisions of occupational health and safety.	Follow-up of Occupational Health / Safety and Legal affairs
Physical Space Security	Security camera recordings are kept for a period of 3 months.	Ensuring physical space security
Transaction Security	It is stored for 10 years.	Execution of information security processes
Other	It is stored for 10 years.	Continuity of company activities

10. DATA OWNER DISPOSAL REQUESTS

In case the destruction request is sent to the Data Controller by the data owner; The situation is reported to the Data Security Board within 24 hours. In the process of responding to the request, the Data Controller Data Owner Relations Manual is complied with.

In the event that the data subject application submitted to the Data Controller contains findings regarding the possibility of a data breach, the Data Controller Data Breach Procedure is put into practice. The possibility of violation is reported to the Data Security Board immediately and within 24 hours at the latest.

11. VIOLATIONS and SANCTIONS

If the policies and procedures regarding personal data published by the data controller are violated by the employees; In accordance with the Employment Contract and the Labor Law No. 4857, the defense

of the employee is taken and disciplinary action is taken in accordance with the act. If the act also constitutes a crime under the Turkish Penal Code No. 5237 or other laws, the necessary judicial authorities are notified.

12. REVISION

This Policy enters into force from the moment it is approved by the Data Security Board. Except for the repeal of this Policy, the Data Security Board is again authorized for the changes to be made in the Policy and how it will be put into effect.

In any case, the Data Controller's Personal Data Retention and Disposal Policy is reviewed once a year, if necessary, it is updated by submitting it to the Data Security Board for approval. In case of conflict between the applicable legislation, especially the KVK Law, and the regulations included in this Policy, the provisions of the legislation shall apply.

The Data Controller reserves the right to make changes to the Data Controller's Personal Data Retention and Disposal Policy in line with the legal regulations to be made by the KVK Institution, which is the administrative authority. Revisions that may occur in this procedure or legislation will be added to the procedure by specifying the date and subject, and will be considered as an integral part of the procedure after the necessary announcements are made.

CUSTOMER PERSONAL DATA PROTECTION LIGHTING TEXT

Erensoy Gıda ve Ambalaj Mak. Singing. ve Tic. Ltd. Sti. (hereinafter referred to as the "Company"); It will be processed in accordance with the Law on the Protection of Personal Data No. 6698 (hereinafter referred to as the "Law"). You have the opportunity to access the policies regarding the processing, storage and transfer of your personal data via www…….com.tr.

Collection of Personal Data, Legal Reason

Your personal data is your personal data in accordance with our company's security and protection activities, service performance and post-performance services, complaints and requests, customer satisfaction studies, face-to-face, telephone, e-mail, website, call center, channels or channels you have contacted with our company. It is collected in accordance with Articles 5 and 6 of the law.

Our company;

A-) In order to fulfill our legal obligations, in cases expressly stipulated in the laws,

B-) For the purposes of establishing and performing the contracts to which we are a party,

C-) Establishment, protection and use of a right

D-) In order not to harm fundamental rights and freedoms, in order to protect the legitimate interests of our company that will be legally accepted;

Pursuant to Articles 5 and 6 of the Law, it will operate in accordance with the Law and other legislation.

Personal data collected by our company will be processed by the Company for the following purposes.

I. Ensuring the continuity of company activities and operations (sales, marketing, finance, production, R&D, transaction security), (A,B,C,D)

ii. Performance of sales and after-sales services,

iii. Continuity of global company activities in which the company is involved, (A, B, C, D)

iv. Customer satisfaction, survey effectiveness, demand and complaint management (A,B,C,D)

v. Making a call to you with advertisement, promotion, survey, campaign content via electronic message, sms and call center, (A, B, C, D)

The reasons and purposes of the processing arising from the Law regarding your personal data above are presented for your information in parentheses.

Purpose of Processing Personal Data and Your Data

Collected personal data is regulated by the Law II. In the section; It is processed for the purposes stated above in accordance with the provisions of Articles 4,5,6,7,8 and 9. During the site visit you have made, the place visited and your license plate information, name and surname are recorded and these collected data are stored for 10 years. Your collected personal data may be transferred to our business partners, suppliers, legally authorized public institutions in line with the realization of the above-mentioned purposes.

Rights of Personal Data Owner

We would like to remind you that you have the following rights as a data owner in accordance with Article 11 of the Law.

I. Learning whether your personal data is processed,

ii. Requesting information if your personal data has been processed,

iii. Personal data

Learning the purpose of processing the data and whether they are used in accordance with its purpose,

iv. Knowing the third parties to whom personal data is transferred at home or abroad,

v. Requesting correction of personal data in case of incomplete or incorrect processing, requesting notification of the situation to third parties to whom the data has been transferred

vi. Demanding the deletion or destruction of your personal data in the event that the reasons requiring the processing of personal data disappear, requesting the notification of the situation to the third parties to whom the data has been transferred

vii. Objecting to the emergence of a result against you by analyzing the processed data exclusively through automated systems,

viii. To request the compensation of the damage in case of loss due to unlawful processing of personal data,

Based on the explanations explained to you above, you can submit your requests regarding your rights in Article 11 of the Law to the Company by filling out the Data Owner Application Form published on our website with the extension www.……..com.tr. Your requests will be met as soon as possible (30 days at the latest), and if meeting your request requires a cost, you will be charged a fee according to the tariff published by the Personal Data Protection Board.

I have read and understood
Name-Surname :
Signature :
Date :

CAMERA RECORDING SYSTEMS LIGHTING TEXT

This Clarification Text is written by Erensoy Gıda ve Ambalaj Mak. Singing. ve Tic. Ltd. Sti. (hereinafter referred to as the "Company") for the purpose of clarification regarding the processing of personal data recorded by closed system security cameras in the company campus in accordance with the Law on Protection of Personal Data No. 6698.

Purpose of Processing Personal Data

As a company, closed system security cameras have been installed in common areas within our company, within the framework of our corporate structure, occupational health/safety and the principle of ensuring the safety of our employees and visitors. The security cameras, the number of which varies in order to ensure the security of our buildings and facilities, have been placed at various points, floor corridors and entry/exit points of our company in your current location for the purpose of taking images.

Collection of Personal Data, Legal Reason

Your personal data is part of the Law II. In the section; In accordance with the provisions of Articles 4,5,6,7,8 and 9, it is collected and processed electronically during your visits to our company via cameras for the purposes stated below.

Transfer of Personal Data

Your personal data obtained electronically through closed-circuit camera recording systems may be transferred to our suppliers, legally authorized public institutions and legally authorized private persons in accordance with the data processing conditions and purposes specified in Articles 8 and 9 of the Law on the Protection of Personal Data No. 6698.

Rights of Personal Data Owner

We would like to remind you that you have the following rights as a data owner in accordance with Article 11 of the Law.

a) Learning whether your personal data is processed or not,

b) Requesting information if your personal data has been processed,

c) Learning the purpose of processing personal data and whether they are used in accordance with its purpose,

d) Knowing the third parties to whom personal data is transferred in the country or abroad,

e) Requesting correction of personal data in case of incomplete or incorrect processing, requesting notification of the situation to third parties to whom the data has been transferred.

f) Demanding the deletion or destruction of your personal data in case the reasons requiring the processing of personal data disappear, requesting the notification of the situation to the third parties to whom the data has been transferred

g) Objecting to the emergence of a result against you by analyzing the processed data exclusively through automated systems,

h) To request the compensation of the damage in case of loss due to unlawful processing of personal data,

Based on the explanations explained to you above, you can submit your requests regarding your rights in Article 11 of the Law to the Company by filling out the Data Owner Application Form published on our website with the extension www.……..com.tr. Your requests will be met as soon as possible

(30 days at the latest), and if meeting your request requires a cost, you will be charged a fee according to the tariff published by the Personal Data Protection Board.

Our company; The right to make changes in this disclosure statement is reserved due to changes in the law and new methods or regulations that may be determined by the Personal Data Protection Board.

PERSONAL DATA OWNER APPLICATION FORM

Based on your rights stated in article 11 of the Law on the Protection of Personal Data No. 6698; In accordance with the provisions of Article 11 of the law and the "Communiqué on the Procedures and Principles of Application to the Data Controller", you can send it to the authorized units of our Company through the following means.

APPLICATION METHODS

In writing

In accordance with the Personal Data Protection Law, you can send your information requests to … with a wet signature.

Registered Email

In accordance with the Personal Data Protection Law, you can forward your information requests to our company's … … KEP address.

E-Mail Address Not Registered in Our System

In accordance with the Personal Data Protection Law, you can forward your information requests to our company's mail address with the extension … … … with a mobile signature or e-signature.

Your E-Mail Address Registered in Our System

In accordance with the Personal Data Protection Law, you can forward your information requests to our company's e-mail address with the extension … ….

KİMLİK VE İLETİŞİM BİLGİLERİ

Name/Surname	
Id nO	
Foreign T.R. Identification number	
Passport Number / Nationality	
Domicile or Workplace Address Based on Notification	
Phone	
E-mail (KEP)	
Postal Address	
Fax	

DEMAND

In accordance with Article 11 of the Law and Article 5 of the "Communiqué on Application Procedures and Principles to the Data Controller", you must clearly share your requests and submit additional documents and information on the subject, if any, together with the application form.

In addition, in the content of the application, it is important that you state which of the paragraphs written in Article 11 of the Law No. 6698 is your request, and if you have a different request, you should state the reason and legal reason, and indicate which communication method you would like to receive a response to your request.

PLEASE INDICATE YOUR APPLICATION THROUGH WHICH CONTACT YOU WOULD LIKE TO RECEIVE ANSWERS.

The answer to your application; Within the framework of the Law No. 6698 and the Communiqués of the Personal Data Protection Board; According to the nature of the request, it will be taken as soon as

possible and within 30 days at the latest. If the transactions to be carried out within the scope of your application require cost, you may be charged a fee based on the tariff determined by the Personal Data Protection Board. At the time of application, our company reserves the right to request identification for the purpose of confirming identity information.

I request you to take action in line with my explanations above.

Applicant :

History :

Attachments :

Signature :

PERSONAL DATA CONSERVATION AND PROCESSING POLICY

2. INTRODUCTION

Erensoy Food and Packaging Mak. Singing. ve Tic. Ltd. Sti. (hereinafter referred to as the "Data Controller"), has a high sensitivity to comply with legal regulations in accordance with the ethical values that support its commercial assets and successes, and establishes all kinds of necessary structures within the framework of compliance with the legislation on the protection of personal data.

The Policy on the Protection and Processing of Personal Data (hereinafter referred to as the "Personal Data Protection and Processing Policy or Policy") and the principles and principles adopted in the processing of data belonging to real persons who have employment or contractual relations with the Data Controller, and within this scope, the personal data carried out by the Data Controller are regulated. In processing activities, legal security of data owners is ensured and transparency is ensured.

The Protection and Processing of Personal Data Policy is included in the Personal Data Protection Law No. 6698 (hereinafter referred to as the "KVK Law") regarding the activities carried out by the Data Controller regarding all personal data processed automatically or non-automatically, provided that it is a part of any data recording system. Within the scope of compliance with the regulations, the basic principles and the principles to be fulfilled by the Data Controller are determined.

Although this Policy has a parallel content with the relevant legislation, in case of conflict between the Policy and the applicable legislation, the provisions of the legislation will be applied.

2. DATA SPEAKER

Data Controller; Pursuant to the KVK Law, it has the title of "data controller" in the personal data processing activities for which it determines the purposes and means, and announces to the public the obligations it has acquired due to this policy and the title of data controller.

6. DEFINITIONS

The important definitions in the KVK Policy and the legislation are given in the table below with their meanings:

Personal Data

Any information relating to an identified or identifiable natural person

Private Personal Data

Data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data

Data Owner

Specific or identifiable natural person whose personal data is processed (Relevant person)

Open Consent

Consent on a particular subject, based on information and freely expressed

Anonymization

Making personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching it with other data.

Processing of Personal Data

All kinds of operations performed on data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data.

Data

Responsible

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 Processor

A natural or legal person outside the organization that processes personal data on behalf of the data controller, based on the authority given by the data controller.

KVK Law

(Law)

Published in the Official Gazette dated 7 April 2016 and numbered 29677,

Law on Protection of Personal Data dated March 24, 2016 and numbered 6698

KVK Board

Personal Data Protection Board

KVK Institution

(Institution)

Personal Data Protection Authority

VERBIS

Data Controllers Registry, which is kept open to the public in the Presidency of the Personal Data Protection Authority, under the supervision of the KVK Board

Data Controller

(Company)

Signature Garment …….

Data Controller

Work partners

Persons with whom the Data Controller cooperates due to commercial relations

Data Controller KVK Storage and Disposal Policy

The policy issued by the Data Controller, which regulates the processes of storage, deletion, destruction and anonymization of the personal data it contains.

Data Controller

Third parties whose suppliers provide services to the Data Controller on a contract basis

Data Controller Data Owner Application Form

The application form to be used by data owners when using their applications regarding their rights in Article 11 of the KVK Law.

Data Controller KVK Policy

Data Controller Personal Data Processing and Protection Policy

Group Companies

Group companies within the body of Data Controller

Personal Data Processing

inventory

Personal data processing activities carried out by data controllers depending on their business processes; The inventory they have created by associating with the personal data processing purposes and legal reason, the data category, the transferred recipient group and the data subject group, explaining the maximum storage period required for the purposes for which the personal data is

processed, the personal data to be transferred to foreign countries, and the measures taken regarding data security.

Data Controllers

About the Registry

regulation

Regulation on Data Controllers Registry, which entered into force on 1 January 2018, published in the Official Gazette dated 30 December 2017 and numbered 30286

Data security

board

The Board, which will provide the necessary coordination within the Company within the scope of ensuring, maintaining and maintaining compliance with the personal data protection legislation by the Data Controller.

7. DATA SECURITY BOARD

Data Security Board; It is the unit responsible for the protection of the personal data processed within the body of the Data Controller and the monitoring of the compliance process with the personal data protection legislation. It consists of representatives of Finance and IT and Legal departments.

Necessary meetings are held when deemed necessary by the Board or upon request. The revision of the policies and their compliance with the legislation are controlled by the Data Security Board. In this context, the following activities and other compliance processes are carried out by the Data Security Board:

i) Carrying out the necessary roles and assignments in the field of personal data protection,

j) To prevent the illegal transfer, access, disclosure of personal data in accordance with the Law and Board decisions, and to take and enforce the necessary measures on other issues that may create a lack of security,

k) Performing audits regarding the implementation of measures and administrative decisions regarding data security,

l) If necessary, implementation of additional measures regarding the protection of sensitive personal data,

m) Organizing trainings, if necessary, in order to ensure a data protection culture within the company,

n) Ensuring the implementation of the relevant documents in terms of compliance with the legislation and carrying out the necessary audits,

o) Monitoring whether the Group companies fulfill their obligations arising from the legislation,

p) Following up the relations with the KVK Institution and the KVK Board.

4.1. ROLE AND TASKS

For the communication to be established with the Institution, the decision regarding the replacement of the "Contact person" who will perform the VERBIS registration and information entry operations is made by the Data Security Board and the Board of Directors.

According to the "Personal Data Owner Relationship Guide", ……. “Data Controller Representative” is appointed by the decision of the Data Security Board or the decision of the Board of Directors.

In addition to the above-mentioned minimum duties, some additional duties and responsibilities may be assigned to the officials to be appointed due to the needs to be felt for ensuring compliance with personal data privacy.

4.2. PREPARATION OF POLICY, PROCEDURE, GUIDELINES AND GUIDELINES

By the Data Security Board in order to ensure compliance with the personal data protection legislation; On behalf of the Data Controller, the revision of the documents written below is provided in the capacity of the data controller.

11. Personal Data Protection Policy

12. Personal Data Retention and Disposal Policy

13. Personal Data Breach Procedure

14. Other texts required by law

5. POLICY PRINCIPLES

5.1. BASIC PRINCIPLES

The following basic principles are adopted by the Data Controller during the processing of personal data.

5.1.1. Processing personal data in accordance with the law and honesty rules

The Data Controller carries out personal data processing activities, in particular the Constitution of the Republic of Turkey and the KVK Law, in accordance with the data privacy legislation and the rule of good faith.

5.1.2. Ensuring the accuracy and up-to-dateness of the personal data processed

The Data Controller ensures the accuracy and up-to-dateness of the personal data he processes, and takes the necessary administrative and technical measures within this framework and continues the process follow-up.

5.1.3. Processing personal data in a limited and measured way in connection with the purpose

Data Controller; processes personal data in connection with the data processing conditions and as necessary for the performance of these services. In this context; The purpose of processing personal data is determined before starting the personal data processing activity. In other words, personal data is not processed only with the assumption that it can be used in the future (preserving personal data is also a data processing activity). In this context, the Data Controller takes into account the fundamental rights of data owners and their own legitimate interests.

5.1.4. Keeping personal data for as long as required by the relevant legislation or for the purpose for which they are processed

Data Controller; processes personal data for a period of time that will comply with this period, if a period is stipulated in the relevant legislation. If there is no regulation in this direction in the legislation, it keeps the data limited to the period required by the data processing purpose. Data Controller; It destroys personal data by deletion, destruction or anonymization methods in case the period stipulated in the legislation expires or the reasons requiring the processing of personal data disappear. In this

context, the Personal Data Retention and Disposal Policy of the Data Controller, which has been created, is complied with.

5.2. LEGAL PROCESSING ACTIVITY

Data Controller; while engaging in the processing of personal data; It acts in accordance with the data processing conditions determined in Articles 5 and 6 of the KVK Law, provided that it also complies with the basic principles.

The Data Controller establishes the necessary mechanisms in its internal systems for the legal processing of personal data.

s. In addition, it carries out the continuity of the process sensitively by providing personnel awareness on data privacy through in-house trainings.

Data Controller; Within the scope of the processing of personal data, it operates in parallel with the rules set forth in the Constitution of the Republic of Turkey, the Turkish Penal Code No. 5237, the KVK Law and other legislation, and the Data Controller KVK Policy.

5.2.1. Data Processing Terms

Personal data is processed in accordance with the legislation and Board decisions, provided that the explicit consent of the Data Owner is obtained. If at least one of the following conditions is met, data processing activities can be carried out without seeking explicit consent:

– Explicit consent: Data processing as a result of obtaining consent of the personal data owner with free will, in accordance with the law, on a specific subject, based on information.

– Envisioned/obligatory in the law: Data processing if there is a clear provision in the legislation regarding the processing of personal data or if it is an obligation within the scope of the legal obligations of the Data Processor.

– Failure to obtain explicit consent due to actual impossibility: Processing the relevant data if the data owner is unable to give explicit consent due to actual impossibility or if his consent cannot be validated, and if it is necessary for the protection of the life or physical integrity of the data owner or a third party.

– Connection with the contract: Processing of the personal data of the parties, if necessary and directly related to the establishment or performance of a contract.

– Publication of personal data by the data owner: In case the data is made public directly by the Data Owner, data processing limited to the scope of publicization.

– Processing personal data if data processing is necessary for the establishment, exercise or protection of a right.

– Legitimate interests of the data controller: Data processing when required by the legitimate interests of the Data Controller, provided that the fundamental rights and freedoms of the Data Owner are preserved.

5.2.2. Special Qualified Personal Data Processing Conditions

Special categories of personal data, if the following conditions are met; can be processed within the framework of express consent in accordance with Article 6 of the Law in accordance with the relevant legislation, Board decisions and the policies implemented by the Data Owner.

5.2.3 Special Cases Subject to Data Processing Activity

– Providing fringe rights and benefits arising from the Labor Law,

– Ensuring equality of opportunity,

– Preventing illegal violations,

– Giving references,

Processing in company mergers and acquisitions and other transactions that change the company structure,

– Processing your personal data in disciplinary investigations and audit processes

– Separate storage of health data and persons authorized to process health data

– Alcohol and drug tests

– Processing of personal data regarding the use of electronic communication tools

– Processing of personal data related to the security camera application

– Processing of personal data regarding internet use

– Processing of personal data regarding vehicles allocated by the company

– Processing personal data within the scope of requesting information about employees from third parties

5.3. LEGAL DATA TRANSFER

By the Data Controller; In the sharing of personal data with group companies and third parties or sharing personal data with third parties, the personal data transfer conditions regulated in Articles 8 and 9 of the KVK Law are complied with. All necessary precautions and inspections are made to the third parties to whom the data is transferred, to ensure the security of the personal data in question.

5.3.1. Transfer of Personal Data

Personal data can be transferred upon the explicit consent of the Data Owner, or without the explicit consent of the data subject, provided that the necessary protective measures are applied in accordance with the legislation and the Data Owner's policies, in the presence of the following conditions:

– Explicit consent: Data transfer as a result of obtaining consent of the personal data owner with free will, in accordance with the law, on a specific subject, based on information.

– Envisioned/obligatory in the law: Data transfer if there is a clear provision in the legislation regarding the processing of personal data or if it is an obligation within the scope of the fulfillment of the legal obligations of the Data Controller.

– Failure to obtain explicit consent due to actual impossibility: Transfer of the relevant data if the data owner is unable to give explicit consent due to actual impossibility or if his consent cannot be validated, if it is necessary for the protection of the life or physical integrity of the data owner or a third party.

– Connection with the contract: The transfer of personal data of the parties, if necessary and directly related to the establishment or performance of a contract.

– Making personal data public by the data owner: Making the data public directly by the Data Owner

Data transfer limited to the scope of publicisation.

– Transfer of personal data if data processing is necessary for the establishment, exercise or protection of a right,

– Legitimate interests of the data controller: Data transfer when required by the legitimate interests of the Data Controller, provided that the fundamental rights and freedoms of the Data Owner are preserved.

5.3.2. Transfer of Private Personal Data

Provided that adequate technical and administrative security measures are established and the following conditions are met, special categories of personal data can be transferred:

– Special categories of personal data other than health and sexual life can be transferred without obtaining the explicit consent of the Data Owner, provided that it is expressly regulated in the law. If there is no regulation in this direction in the law, data can be transferred provided that the relevant person has express consent.

In case of the existence of the specified data transfer conditions, the relevant personal data is sent to the countries with adequate protection/safe as determined and announced by the Board, or in the absence of sufficient protection, to ensure adequate protection of the data controllers in Turkey and in the relevant foreign country in line with the data transfer conditions determined by the relevant legislation and the Board regulations. It can be transferred to foreign countries where the written commitment is obtained and the permission of the Board is obtained; Provided that the limitations and conditions determined by the Board are complied with, it can be transferred abroad if the application of the Binding Company Rules is applied.

6. OBLIGATIONS

The Company informs the data owners about the purposes for which the Personal Data will be processed, to whom the data transfer can be made, for what purposes the data can be processed and transferred, and the data collection methods. Within the scope of this information, the rights of the data owner regarding their personal data and how they will be used are also clarified.

Data Controller; It complies with the obligations stipulated by the KVK Law for data controllers. In this context, the main issues that the Data Controller is obliged to comply with in this policy are listed below:

6.1. Obligation to Fulfill the Decisions Made by the KVK Board

Data Controller; It immediately implements the decisions notified by the KVK Board, which is the executive body of the KVK Institution, which regulates the personal data protection activities and is the administrative authority of our country in this field, in case of a complaint or as a result of the ex officio examination. It also adopts the policy decisions established by the KVK Board as data privacy rules.

6.2. Data Owner Relations Obligation

Data Controller; In its capacity as data controller, pursuant to Article 13 of the KVK Law, it concludes the requests of data owners regarding their personal data as soon as possible and within thirty (30) days at the latest, depending on the nature of the request.

In accordance with Article 11 of the KVK Law, Data Owners can use the following rights by applying to the Data Controller via the website address:

9. To learn whether personal data is processed or not,

10. If personal data has been processed, to request information about it,

11. To learn the purpose of processing personal data and whether they are used in accordance with their purpose,

12. To know the third parties to whom personal data is transferred in the country or abroad,

13. Requesting correction of personal data in case of incomplete or incorrect processing and requesting notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,

14. Requesting the deletion or destruction of personal data in the event that the reasons requiring processing are eliminated, although it has been processed in accordance with the provisions of the KVK Law and other relevant laws, and requesting the notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,

15. Objecting to the emergence of a result against the person himself by analyzing the processed data exclusively through automated systems,

16. To request the compensation of the damage in case of loss due to unlawful processing of personal data.

6.3. Obligation to Register and Notify the Data Controllers Registry

Data Controller; If it meets the criteria mentioned in the Regulation on the Data Controllers Registry, it is registered in the Data Controllers Registry in accordance with Article 16 of the KVK Law and the procedures and principles of the regulation.

6.4. Obligation to Inform the Data Owner

Data Controller; In accordance with Article 10 of the KVK Law and the Communiqué on the Procedures and Principles to be Complied with in Fulfilling the Obligation of Clarification, it carries out the necessary processes to ensure that the data owners are informed by the authorized persons during the acquisition of personal data. You can review the KVK Clarification Text published on the website for the purpose of fulfilling the lighting obligation.

6.5. Obligation to Ensure the Security of Personal Data

By the Data Controller, KVK Kan

Conscious of the importance of ensuring the security of personal data and observing the fundamental rights and freedoms of data subjects, in accordance with Article 12 of unu;

4. To prevent the unlawful processing of personal data,

5. To prevent unlawful access to personal data and

6. To ensure the protection of personal data

All necessary technical and administrative measures are taken to ensure the appropriate level of security for its purposes. In addition, necessary audits are implemented within the scope of the operation of mechanisms to ensure data security.

7. ENSURING THE SECURITY OF PERSONAL DATA

The Data Controller takes all necessary measures, within the possibilities, according to the nature of the data to be protected, in order to prevent the unlawful processing of personal data, illegal access to personal data, or security deficiencies that may occur in other ways, and to ensure the safe keeping of personal data.

7.1. ADMINISTRATIVE MEASURES

– By the Data Controller; Personal Data Processing Inventory is created, which includes personal data categories, data owners, processing purposes and security measures taken.

– Necessary institutional policies and procedures regarding the protection of personal data are established and their functionality and continuity are ensured.

– Confidentiality agreements are signed with the employees.

– Awareness training and meetings are held to create awareness of data protection within the organization.

– In cases where personal data is subject to transfer, necessary measures are taken by group companies or third party companies.

– Legal provisions are added to employment contracts and disciplinary regulations.

– In case the conditions are met, the registration and information entry processes in the Data Controllers Registry Information System VERBIS are completed.

– Data Security provisions are added to the contracts signed with data processors.

7.2. TECHNICAL MEASURES

– By the Data Controller; The security of physical and electronic media containing personal data is ensured.

– Against malicious software, personal data is regularly backed up and the security of the backed up personal data is ensured.

– In order to ensure cyber security, preventive systems and software are established for information networks.

– Data Controller employees' access to personal data is created by constantly ensuring their duties and authority controls.

– Data security trainings are planned.

– Data penetration test standards are determined.

7.3. PERSONAL DATA VIOLATION

Data Controller; In case the processed personal data is obtained unlawfully by unauthorized persons, it notifies the KVK Board and the relevant data owners within 72 hours. For this reason, the Data Controller Data Breach Procedure (link) has been created; Within the scope of this procedure, all breach drills within the body of the Data Controller are set up by the Data Security Board.

8. DISPOSAL OF PERSONAL DATA

Data Controller; Pursuant to Article 7 of the KVK Law, it has created all necessary internal systems for the destruction of personal data in accordance with the Personal Data Retention and Destruction Policy, which it has created for the deletion, anonymization or destruction of personal data that has been processed in accordance with the law.

9. REVISION

This Policy enters into force from the moment it is approved by the Data Security Board. Except for the repeal of this Policy, the Data Security Board is authorized for the changes to be made in the Policy and how it will be put into effect.

The KVK Policy was published on the website by the Data Controller and presented to the public. In any case, this Policy is reviewed once a year, and if necessary changes are made, it is updated by submitting it to the Data Security Board for approval. In case of conflict between the applicable legislation, especially the KVK Law, and the regulations included in this Policy, the provisions of the legislation shall apply.

The Data Controller reserves the right to make changes in the KVK Policy in line with the legal regulations to be made by the KVK Institution, which is the administrative authority.

Revisions that may occur in this policy or legislation will be added to the policy by specifying the date and subject, and will be considered an integral part of the policy after the necessary announcements are made. The current version of the KVK Policy will be published on the website of the Data Controller.

PERSONAL DATA

DELETING,

DESTRUCTION,

MAKING ANONYMOUS,

POLICY

PREFACE

Erensoy Food and Packaging Mak. Singing. ve Tic. Ltd. Sti. The (Company) may delete or destroy the personal data it maintains in accordance with the Law No. 6698 on the Protection of Personal Data and other legislation containing special provisions, when the conditions are met in accordance with the Law No. 6698, in accordance with the company policy or in accordance with the processes listed below, upon the request of the person concerned. or make it anonymous.

In case of deletion, destruction or anonymization of personal data, in case of conflict, first of all, the provisions of Law No. 6698 and the policy decisions of the Personal Data Protection Authority will be applied.

Revisions that may occur in this policy or legislation will be added to the policy by specifying the date and subject, and will be considered an integral part of the policy after the necessary announcements are made.

-RELEASE DATE 01/12/2019-

I-DELETING PERSONAL DATA

Deletion of personal data is the process of making personal data inaccessible and non-reusable for relevant users. Deleted data cannot be accessed and used by users other than the data controller.

A-PROCESS OF DELETING PERSONAL DATA

Personal data is deleted in accordance with the legislation and request, if the person concerned requests it and there is a legal obligation. In other cases, personal data may be retained for 10 years.

If the existence of personal data is related to possible claims arising in accordance with contractual, commercial, legal and administrative transactions, the data is retained during the statute of limitations regarding the said transaction. If there is a conflict between the request and the company policy in this regard, a written application is made to the Personal Data Protection Authority in order to eliminate the conflict and action is taken in line with the policy decision.

By using an access authorization and control matrix or a similar system, the relevant users are identified for each personal data, and the authorizations and methods of the users such as access, retrieval, reuse are determined, and then the access, retrieval, reuse authorization and The process of closing and eliminating the methods is carried out.

B- DATA DELETE METHODS

1-CLOUD SYSTEM

In the cloud system, the data will be deleted by issuing the delete command. The relevant user does not have the authority to restore the deleted data on the cloud system.

2-PERSONAL DATA FOUND ON PAPER

Personal data printed on paper will be deleted using the blackout method.

The blackening process is done by cutting the personal data on the relevant document when possible, and in cases where it is not possible, making it invisible to the relevant users by using fixed ink, which cannot be read with technological solutions.

3-OFFICE FILES ON THE CENTRAL SERVER

The file must be deleted with the delete command in the operating system or the access rights of the relevant user on the file or the directory where the file is located must be removed.

4-PERSONAL DATA IN PORTABLE MEDIA

Personal data in flash-based storage media should be stored encrypted and deleted using software suitable for these media.

5-DATABASES

Relevant lines containing personal data must be deleted with database commands (DELETE etc.).

II- DESTRUCTION OF PERSONAL DATA

Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way. Necessary technical measures are taken to destroy personal data.

METHODS OF DESTRUCTION OF PERSONAL DATA

A-LOCAL SYSTEMS

1-DE-MAGNETIZED

Magnetic media is passed through a demagnetizing device, corrupting the data in an unreadable way. De magnetized device will be provided if needed.

2-PHYSICAL DESTRUCTION

Optical media and magnetic media are physically destroyed by melting, incinerating or pulverizing.

3-Overwrite

By writing random data consisting of 0s and 1s on magnetic media rewritable optical media at least seven times, recovery of old data is prevented. If necessary, software is provided by the company for this purpose.

B- ENVIRONMENTAL SYSTEMS

NETWORK DEVICES - FLASH-BASED DEVICES - MAGNETIC TAPE AND DISKS - MOBILE PHONES - SIM CARDS - MEMORY CARDS - OPTICAL DISKS - PRINTER - FINGERPRINT READING DEVICES

If there is an annihilation command among the technical features of the devices listed under the heading of this article, the deletion is performed by using the destroy command, otherwise, by selecting the appropriate method of magnetization, physical destruction or overwriting.

C- PAPER AND MICRO PLUGS

Personal data stored as paper and microfiche are destroyed by paper shredding or clipping devices, horizontally and vertically, if possible, in a way that cannot be recovered and combined. paper andIf micro-plugs are scanned and transferred to electronic media, destruction is performed by selecting the appropriate method of magnetization, physical destruction or overwriting according to the electronic environment conditions in which they are located.

D-CLOUD ENVIRONMENT

If there is a destroy command among the cloud system features where personal data is stored, this command will destroy all copies of the encryption keys that otherwise enable access to the cloud system.

E-MAINTENANCE AND REPAIR PROCEDURES

In the event that the devices containing personal data are delivered to third parties or institutions for maintenance and repair purposes, the destruction process is carried out by choosing the appropriate method among the methods listed under the destruction title of this policy, if possible. If the destruction is not appropriate, the data storage medium of the device is removed or other technical measures preferred by the relevant department are taken.

III-THE ANNOUNCEMENT OF PERSONAL DATA

Anonymization of personal data is the process of making personal data impossible to associate with an identified or identifiable natural person under any circumstances, even if it is matched with different data. When personal data is anonymized, even if it is returned or matched, the data controller and the users to whom the data is transferred cannot be identified and associated with whom it belongs.

The circumstances under which personal data will be anonymized and which method will be chosen for the anonymization process are determined by the data controller according to the characteristics of the transaction, and necessary technical measures are taken accordingly.

When choosing the anonymization method; The nature of the data, the size of the data, the structure of the data in the physical environment, the diversity of the data, the desired benefit / purpose of processing from the data, the frequency of processing the data, the reliability of the party to which the data will be transferred, the meaningful effort to make the data anonymized, the magnitude of the damage that may arise if the anonymity of the data is broken , domain, Distribution/centralization ratio of the data, Access authorization control of the relevant data, The possibility of the effort to be spent to construct and implement an attack that will break anonymity is taken into account.

Announcement and execution of this policy will be carried out by the Human Resources Department.

Prepared by Reviewer Approved by

DOCUMENT HISTORY

Version Release Date Description of Change

DATA BREACH PROCEDURE

PREFACE

Erensoy Food and Packaging Mak. Singing. ve Tic. Ltd. Sti. Although the (Company) has created and published its policies regarding the personal data it maintains as a data controller in accordance with the Law No. 6698 on the Protection of Personal Data and other legislation containing special provisions, the precaution to be taken in case of violation of the aforementioned policies or processes regarding personal data, the first actions This procedure has been prepared in order to plan the processes that need to be operated, correspondence and operation.

Revisions that may occur in this procedure or legislation will be added to the procedure by specifying the date and subject, and will be considered as an integral part of the procedure after the necessary announcements are made.

DATA BREACH / RISK OF DATA VIOLATION

Pursuant to Law No. 6698, data defined as personal data or sensitive/private personal data is obtained, processed, shared with third parties in Turkey or abroad without the explicit consent of the data owner, or in violation of the published policies on the protection of personal data, despite the explicit consent being obtained. It will be considered as a risk of data breach or data breach.

ACTION PLAN

In case of detection of data breach, it is essential to operate the following processes. In the event of a data breach being detected, the data security board officials are not contacted verbally by the relevant

personnel within 60 minutes at the latest, and if these officials cannot be reached, the company general manager is informed about the situation. Upon hearing of the breach, the Data Security Board is required to convene within 24 hours and prepare a data breach report by operating the processes listed below. This period cannot exceed 24 hours.

DETECTION OF THE CAUSE OF DATA VIOLATION

 Sending personal data to wrong recipients

 Theft or loss of documents/devices

 Storing data in unsafe environments

 Malware

 Social engineering

 Sabotage

 Accident/ Neglect

 Other

DATA GROUPS AFFECTED BY THE VIOLATION

PERSONAL DATA

 Identity

 Contact

 Location

 Personal Legal

 Transaction Customer

 Operation

 Physical Space Security

 Transaction Security

 Risk Management

 Finance

 Professional Experience

 Marketing

 Audio and Audio Recordings

PRIVATE PERSONAL DATA

 Race and Ethnicity

 Political Thought

 Philosophical Faith,

 Religion, Sect and Other Beliefs

 Disguise and Outfit

 Association Membership

 Foundation Membership

 Union Membership

 Health Information

 Sexual Life

 Criminal Conviction and Security Measures

 Biometric Data

 Genetic Data

NUMBER OF PEOPLE AFFECTED BY THE VIOLATION

 Estimated Number of Persons :..... ...

 Estimated Number of Records :..... ...

GROUPS OF PERSONS AFFECTED BY THE VIOLATION

 Employees

 Users

 Subscribers/Members

 Customers and potential Customers

 Other

EFFECT OF VIOLATION ON PEOPLE

 Loss of control over personal data

 Identity theft

 Discrimination

 Restriction of rights

 Fraud

 Financial loss

 Loss of reputation

 Loss of security of personal data

 Other

MISCELLANEOUS RISKS DUE TO VIOLATION

EFFECT OF VIOLATION ON ORGANIZATION

 Unknown

 Low No loss of effectiveness

 Medium You have lost the ability to provide an important service to some of your users

 High You have lost the ability to provide any important service to all your users

TIME TO HEAL

 normal

 Supported

 Extended

 Irreversible

 Completed

INFLUENCE OF THE INFORMATION SYSTEM BY CYBER ATTACK

 Yes

 No

If the answer is “Yes”, a description of the explanation, recovery time and impact on the organization

DATA BREACH REPORTING

Following the completion of the report regarding the data breach, the report will be sent electronically and physically to the Personal Data Protection Board by the contact person, and the process will be followed up. The period for sharing the report with the Board will be carried out within 72 hours following the detection of the data breach.

1 VIOLATION and SANCTIONS

2 If the policies and instructions regarding personal data published by the data controller are violated by the employees; In accordance with the contract and the law numbered 4857, the defense of the employee is taken and disciplinary action is taken in accordance with the act. If the act also constitutes a crime under the Law No. 5237 or other laws, the necessary judicial authorities are notified.

Announcement and execution of this procedure will be carried out by the Human Resources Department.

DOCUMENT HISTORY

Version Release Date Description of Change

Prepared by Reviewer Approved by