EMIRSON GLOBAL FOREIGN TRADE LIMITED COMPANY PERSONAL DATA STORAGE AND DISPOSAL POLICY

1. PURPOSE OF THE POLICY

This Personal Data Retention and Destruction Policy ("**Policy**"), Personal Data Protection Law No. 6698 ("**KVKK**" or "**Law**") and the Regulation on the Deletion, Destruction or Anonymization of Personal Data ("**Regulation**"), in accordance with the relevant legislation, **Emirson Global Foreign Trade Limited Company** ("**Company**"), procedures, principles, It has been prepared to determine the storage, deletion and destruction periods.

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.

2. DEFINITIONS AND EXPLANATIONS

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.
Employee/Trainee	Company employees or interns.
Electronic Media	Environments where personal data can be created, read, changed and written by electronic devices.
Non-Electronic Media	All written, printed, visual etc. other than electronic media. Other environments.
Related Person	The real person whose personal data is processed.
Related User	People 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.
Recording Media	Any environment where personal data is processed wholly or partially automatically or non-automatically, provided that it is a part of any data recording system.

Personal Data	Any information relating to an identified or identifiable natural person.
Processing of Personal Data	Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or using personal data completely or partially by automatic or non-automatic means provided that it is a part of any data recording system. Any operation performed on the data, such as blocking.
Board	Personal Data Protection Board
Organization	Personal Data Protection Authority
KVKK, Law	Law No. 6698 on the Protection of Personal Data
Special Qualified Personal Data	Data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, dress, 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, which 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
Deletion	Making personal data inaccessible and unusable for the relevant users in any way.
Company	**Emirson Global Foreign Trade Limited Company**
Data Processor	A natural or legal person who processes personal data on behalf of the data controller, based on the authority given by the data controller.
Data Recording System	The registry system, directory, where personal data is processed and structured according to certain criteria.
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.
Annihilation	Making personal data inaccessible, irretrievable and reusable by anyone in any way.

Regulation	Regulation on the Deletion, Destruction or Anonymization of Personal Data published in the Official Gazette on October 28, 2017

3. REGULATED RECORDING MEDIA

Personal data stored within the company are sensitively stored in the following recording media in accordance with the nature of the data and legal obligations.

Electronic Media:

- Servers (domain, backup, email, database, web, file sharing)
- Software (office software, portal, etc.)
- MS office files
- Personal computers (desktop, laptop)
- Company computers (desktop, laptop)
- Network devices
- Mobile devices and their storage areas (phone, tablet, etc.)
- Shared/non-shared disk drives used for data storage on the network
- Printer
- Camera
- Browser
- Copier
- Peripherals such as fingerprint reader
- Optical discs (CD, DVD, etc.)
- Removable disks (USB, memory card, etc.)
- File server
- Dhcp
- DC

- Accounting operation system (micro)
- SQL database
- MySQL database

Non-electronic Media:

- Unit cabinets
- Unit archive
- Institution archive
- Archive
- Accounting unit
- Paper
- Written, printed, visual media
- Manual data recording systems (survey forms, guest book, candidate evaluation forms)

4. EXPLANATIONS RELATING TO THE REASONS REQUESTING THE STORAGE AND DISPOSAL OF PERSONAL DATA

Personal data within the company providing the company's services, uninterrupted operations, planning and executing human resources processes, planning employee rights and benefits, planning and executing procurement and business partner processes, ensuring effective communication, fulfilling legal obligations as required or mandated by legal regulations. fulfillment of sector-specific obligations, fulfillment of necessary quality and standard audit processes, informing public institutions and organizations, ensuring corporate communication, ensuring security, statistical studies, analysis studies, reporting studies, performance of the obligations imposed by the signed contracts and protocols. to be used as evidence in legal disputes that may arise in the future or to fulfill the burden of proof, to work in written, printed and electronic journals and bulletins is stored securely and sensitively in electronic or non-electronic media specified in this Policy, within the data processing conditions set forth below, for the purposes of operating archive processes and executing the supply chain.

Personal data within the company are destroyed ex officio or upon the request of the person concerned, if the data processing conditions listed below are no longer valid.

• Existence of explicit consent,

• Existence of a provision of law,

• Failure to obtain explicit consent due to actual impossibility,

• It is necessary to process the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of the contract,

• It is mandatory for the data controller to fulfill its legal obligation,

• The personal data of the person concerned has been made public by him,

• Data processing is mandatory for the establishment, exercise or protection of a right,

• Data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject.

5. TECHNICAL AND ADMINISTRATIVE MEASURES TO STORAGE PERSONAL DATA SECURELY AND TO PREVENT THEIR UNLAWFUL PROCESSING AND ACCESS

• Network security and application security are provided.

• Closed system network is used for personal data transfers via network.

• Security measures are taken within the scope of procurement, development and maintenance of information technology systems.

• There are disciplinary regulations that include data security provisions for employees.

• Training and awareness activities are carried out periodically for employees on data security.

• An authorization matrix has been created for the employees.

• Access logs are kept regularly.

• Institutional policies on access, information security, use, storage and destruction have been prepared and started to be implemented.

• Confidentiality commitments are made.

• 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.

• Signed contracts include data security provisions.

• Personal data security policies and procedures have been determined.

• Personal data security issues are reported quickly.

• Personal data security is monitored.

• 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 reduced as much as possible.

• Personal data is backed up and the security of the backed up personal data is also ensured.

• User account management and authorization control system is implemented, and these are also followed.

• In-house periodic and/or random audits are conducted and made.

• Log records are kept without user intervention.

• Existing risks and threats have been identified.

• Protocols and procedures for special quality personal data security have been determined and implemented.

• If sensitive personal data is to be sent via e-mail, it must be sent in encrypted form and using Registered E-mail Address or corporate e-mail account.

• Secure encryption / cryptographic keys are used for sensitive personal data and are managed by different units.

• Intrusion detection and prevention systems are used.

• Cyber security measures have been taken and their implementation is constantly monitored.

• Data processing service providers are periodically audited on data security.

• Awareness of data processing service providers on data security is ensured.

6. TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN FOR LAWFUL DISPOSAL OF PERSONAL DATA

The practices within the Company to destroy (delete, destroy and anonymize) personal data are as follows:

Deletion of Personal Data

• Personal data physically in paper, file, folder; It is stored in the archive/storage/storage areas or the relevant parts of these areas, where the relevant users (all employees other than the archive/storage officer) cannot access or review. What is important here is that the relevant users will not be able to enter these storage areas and cannot take any action on the personal data inside. In certain parts of the storage/storage/archive areas, deletion can be performed by keeping them in locked areas that cannot be accessed by anyone other than the archive/storage officers.

• Office files located on the central server are performed by deleting the file with the delete command in the operating system or by removing the access rights of the relevant user on the file or the directory where the file is located.

• Personal data in portable media (for example, data in flash-based storage media) should be stored encrypted and deleted using software suitable for these media.

• Personal data in databases are deleted with database commands (DELETE, etc.) of the relevant rows/columns or cells in the table.

Destruction of Personal Data

• The destruction of personal data on local systems is achieved by de-magnetization (exposing the media to a high magnetic field by passing through a special device), physical destruction (melting, burning, using shredders of media and magnetic media) and overwriting.

• Destruction of personal data on environmental systems; Network devices (switch, router etc.), Flash-based media/hard disks (ATA “SATA, PATA etc.”, SCSI “SCSI Express etc.”), Magnetic tape, Magnetic disk units, Mobile phones (Sim card and fixed memory) If the data recording media is removable or fixed, peripherals such as printer and fingerprint door access system, If the peripheral recording systems that we can specify as optical discs are digital media, if it is supported as a product feature, using the destroy command such as <block erase> is the product feature of the digital media. not supported by the manufacturer, using the manufacturer's recommended destruction method, or using one or more of the appropriate methods specified as "demagnetizing, physical destruction, overwriting", and finally "demagnetizing, physical destruction, overwriting" if not digital media. must be destroyed by using one or more of the appropriate "writing" methods.

• Since the personal data in the paper and microfiche media is permanently and physically written on the media, the main media containing these data is destroyed.

• Personal data in the cloud environment is encrypted and stored and when the destruction time comes, the destruction command is applied.

Anonymization of Personal Data

• Anonymization is carried out by removing the basic identifying information (eg name, surname, Republic of Turkey ID number) that enables the identification of the data owner with the masking method.

• With the aggregation method, personal data is extracted in a way that cannot be associated with any person (eg, more job applications from people between the ages of 25 and 30), and anonymization is carried out.

• With the Data Derivation method, anonymization is carried out by creating a more general content from the content of personal data and in a way that the personal data cannot be associated with a person in any way (eg writing age instead of birth dates).

Anonymization Methods That Do Not Provide Value Irregularities

No change, addition or subtraction is applied to the values of the data, instead, all of the rows or columns in the set are anonymized by making changes. Thus, while there is a change in the data in general, the values in the fields are kept in their original state.

- **Removing Variables**: It is an anonymization method provided by removing one or more of the variables from the table by completely deleting them.
- **Removing Records**: By removing a row containing singularity from the dataset, anonymization is strengthened and the probability of generating assumptions about the dataset is reduced.
- **Regional Obfuscation**: In order to make the dataset more secure and reduce the risk of predictability, the value is changed to "unknown" if the combination of values for a particular record is likely to make it distinguishable.
- **Generalization**: It is the process of converting the relevant personal data from a specific value to a more general value. The new values obtained by this method show the total values or statistics belonging to a group that makes it impossible to reach a real person.
- **Lower and Upper Bound Coding**: Generally, the low or high values of a certain variable are collected together, and these values are obtained by making a new definition.
- **Global Coding**: It is an anonymization method in the form of grouping used in data sets that do not contain numeric values or have values that cannot be numerically sorted, where lower and upper bound coding is not possible.
- **Sampling**: A subset from the set is described or shared instead of the entire dataset. Thus, the risk of producing accurate predictions about people is reduced.

Anonymization Methods That Provide Value Irregularity

It is anonymized by changing the existing values, creating distortion in the values of the data set. Even if the values in the data set are changing, it is still possible to benefit from the data by ensuring that the total statistics are not corrupted.

• **Micro-Association**: All records in the dataset are first arranged in a meaningful order and then the whole set is divided into subsets a certain number of times. Then, by taking the average of the value of each subset of the determined variable, the value of that variable of the subset is replaced with the mean value. Thus, the average value of that variable for the entire data set will not change.

• **Data Exchange**: Record changes obtained by exchanging values of a subset of variables between pairs selected from the records. This method is mainly used for categorizable variables, and the main idea is to anonymize the database by changing the values of the variables among the records belonging to individuals.

• **Adding Noise**: It is anonymized by adding and subtracting in order to provide distortions to a determined extent in a selected variable. This method is mostly applied on datasets containing numeric values. Distortion applies equally to each value.

Statistical Methods to Strengthen Anonymization

As a result of the combination of some values in the records with singular scenarios in

anonymized data sets, the possibility of determining the identities of the people in the records or deriving assumptions about their personal data may arise. For this reason, anonymity can be strengthened by minimizing the singularity of the records in the dataset by using various statistical methods in anonymized datasets. The main purpose of these methods is to keep the benefit to be gained from the data set at a certain level while minimizing the risk of anonymity deterioration.

- **K-Anonymity**: It is an anonymization statistical method developed to prevent the disclosure of information specific to individuals with singular characteristics in certain combinations by enabling the identification of more than one person with certain fields.
- **L-Diversity**: It has been formed through studies carried out on the deficiencies of K-Anonymity. This method takes into account the diversity of sensitive variables corresponding to the same variable combinations. For example, although K-anonymity has been applied by anonymizing the name, surname or identity number of the people, there is a possibility that they can be identified because the zip code, age and ethnic origin information are shared. By anonymizing this information with the masking method, it has reduced the guessing power of the user with external information.
- **T-Proximity**: Although the L-diversity method provides diversity in personal data, there are cases where it does not provide sufficient protection since the said method does not deal with the content and sensitivity of personal data. In this state, the process of calculating the degree of closeness of personal data and values among themselves and anonymizing the dataset by subclassing it according to these degrees of closeness is called T-proximity method.
- In this context, the decision of the institutions to anonymize as a result of their own discretion, whether there is a risk of reversing the anonymized personal data with various interventions and transforming the anonymized data into re-identifying and distinguishing real persons should be investigated and action should be taken accordingly.

TITLES, UNITS AND JOB DEFINITIONS OF THOSE INVOLVED IN PERSONAL DATA STORAGE AND DISPOSAL

Employee	Unit	Job Description
Archive Manager	Human Resources	Destruction of personal data.
Lawyer	Law Office	Receiving the requests of the relevant persons, checking their compliance with the procedure and answering the request.
Computer Engineer	Information Technologies	Ensuring the compliance of the processes within its scope with the storage period, management of the periodical destruction process, performing the necessary inspections and controls in order to respond to the requests of the relevant persons, the destruction of personal data in the electronic environment.

Human Resources Staff	Human Resources	Managing the personal data destruction process in accordance with the periodical destruction period, ensuring the compliance of the processes within its scope with the retention period.
OHS Personnel	OHS	Managing the personal data destruction process in accordance with the periodical destruction period, ensuring the compliance of the processes within its scope with the retention period.

7. TABLE OF STORAGE AND DISPOSAL PROCESS AND TIME

Recommended storage times under this heading; The general statute of limitations has been specified by taking into account the duration of the legal relationship with the relevant persons, the period during which the legitimate interests of the company remain valid in accordance with the law and the rules of honesty, and the period during which the update of personal data can continue. The periods that are specific to the sector in which the company operates or that are accepted as customary in the sector should be evaluated separately.

Personal data within the company; If it is foreseen in the relevant legislation, it is stored for the period specified in this legislation.

If the purpose of processing personal data has ended and the storage period determined by the relevant legislation and the company has come to an end, personal data are stored in order to resolve possible legal disputes, to meet the lawful demands of authorized public institutions and organizations, or to assert the relevant right related to personal data.

The processed personal data are stored for the periods specified in this Policy, starting from the end of the activity or process.

Storage times are divided into deletion time and destruction time.

Deletion refers to the process of making personal data inaccessible and non-reusable for the relevant users.

Relevant user refers to the 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 means making personal data inaccessible, unrecoverable and unusable by anyone in any way. Stored/backed up personal data is destroyed after certain periods.

Anonymization means making personal data incapable of being associated with an identified or identifiable natural person under any circumstances, even by matching them with other data.

Deleted personal data, until the time of destruction;

- **Resolution of possible legal disputes,**
- **Meeting the legal demands of authorized public institutions and organizations,**
- **It is backed up for the purposes of asserting a right related to personal data. No access to the backed up personal data is provided for any other purpose.**

SAMPLE STORAGE AND DISPOSAL PROCESS

SAMPLE:

Process (Activity): Keeping personnel files Deletion time: 5 years from the expiry of the contract

Time of destruction: The first periodic destruction after the 15th year from the completion of the time of deletion

EXPLANATION ON EXAMPLE:

In the example above, the personal data of the personnel in the personnel file is stored for a total of 20 years from the end of the contract with the personnel.

In the first 5 years of the specified 20-year period, the Human Resources Unit can access this data. After 5 years, the Human Resources Unit cannot access this data.

At the end of 5 years, this data can be accessed by the person or unit responsible for technical storage, protection and backup of the data.

After 20 years, this data is destroyed in a way that no one can access.

Abbreviations:

TBK: Turkish Code of Obligations No. 6098 TTK: Turkish Commercial Code No. 6102 VUK: Tax Procedure Law No. 213 OHS: Occupational Health and Safety Legislation EIC: Execution and Bankruptcy Law No. 2004

TCK: Turkish Penal Code No. 5237

HMK: Civil Procedure Law No. 6100 HR: Labor Law No. 4857

Law No. 5651: Law No. 5651 on Arranging Broadcasts on the Internet and Combating Crimes Committed Through These Broadcasts

AVK: Attorneyship Law No. 1136 BK: Municipal Law No. 5393

Process (Activity)	Legal Basis of Activity	Deletion Time	Legal Basis for Retention	Time to Destroy
Personnel candidate evaluation/ Interview	-	-	KVKK	If the candidate is hired, it is transferred to the personnel file. If the candidate is not hired, the application will be rejected. first periodic destruction following the expiry date destroyed in the process.
Personnel file of the personnel (Name Surname, TR Identity Number, Nationality Information, Mother's Name-Father Name, Place of Registration and Other Population Information, Maiden Surname, Place of Birth, Date of Birth, Gender, Marital Status, Photograph, Home Address, Tax Number , Sgk Number, Telephone Number, E-Mail Address, Educational Schools, Certificate Information, Driver's License, Criminal Record Record, Experience Information, Position Information, Institutions Worked Before, Foreign Language Knowledge, Certificate Information, Military Status, Health Report, Family Members (Spouse, Mother, Father, Child Name, tckn, D. Date and Age Information), Bank Account Information, Employee Financial and Salary Details, Payrolls,	HR TCoO	It is deleted after 10 years from the expiration of the contract.	HR TCoO KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.

Declarations, Premium Progress Payments, Premium Amounts, File Regarding Execution Files and Debt Information, Minimum Living Allowance Information, Private Health Insurance Amount Etc. Information, Health Data, rest reports, SSI Occupational Code, embezzlement forms, fringe benefits and acts, disciplinary records, permits, payrolls, PDKS, part-time work information, resume information, account information, social assistance information, license plate, vehicle, etc.)				

CV information (employee)	Its currency is questioned for 3-year periods, it is renewed or destroyed when it is out of date.			
Criminal record records	Parallel to the periods in the Judicial Registry Law No. 5352, its currency is questioned and the existence of explicit consent is investigated.			
Keeping the identity information of the personnel and the entry and exit information of the personnel	HR TCoO OHS	It is deleted after 15 years from the expiry of the contract.	HR TCoO OHS KVKK	It is destroyed in the first periodic destruction process following the 5-year period from the date of deletion.
Personnel payment/cut-off transactions (such as Job Advance, Salary, Premium, Bonus, In-kind Aid, Bank Promotions, BES, Severance, Notice, Termination, Affiliate, Allowance and Travel Payments)	HR TCoO	It is deleted after 10 years from the expiration of the contract.	HR KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.
Recruitment health examinations and periodic- outpatient health examinations, rest reports	OHS HR TCoO	It is deleted after 15 years from the expiry of the contract.	OHS HR TCoO KVKK	It is destroyed in the first periodic destruction process following the 5-year period from the date of deletion.
Work accident report, emergency registration form, work accident inspection and event records, result notification	OHS	If there is a contract with the person involved in the accident: It is deleted after 15 years from the expiry of the contract. If there is no contract with the person involved in the accident: It is deleted at the end of 15 years from the date of the accident.	OHS KVKK	It is destroyed in the first periodic destruction process following the 5-year period from the date of deletion.

Training records within the scope of Occupational Health and Safety	HR OHS	It is deleted after 15 years from the expiry of the contract.	HR OHS KVKK	It is destroyed in the first periodic destruction process following the 5-year period from the date of deletion.
Training records other than Occupational Health and Safety	HR TCoO	It is deleted after 10 years from the expiration of the contract.	HR TCoO	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.
OHS Board meeting	OHS	After 5 years from the meeting date, those that are out of date by being evaluated are deleted.	OHS	It is destroyed in the first periodic destruction process following the 35-year period from the date of deletion.
Circumstances requiring investigation under the Turkish Penal Code No. 5237	The penalty is kept for the statute of limitations, at the end of which it is destroyed in the first periodic destruction.			
Keeping litigation/execution/mediation files	AVK HMK İİK	It is deleted after 10 years from the finalization of the file.	AVK HMK İİK KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion. It is destroyed in the first periodical destruction process following the expiry of the criminal statute of limitations in matters requiring criminal investigation.

Promotional film and advertisement works/ Social – cultural organization and activities/ Special day events	-	In the relevant process, the need for personal data and up-to-dateness are taken into account, and the possible ones are deleted when the need and timeliness expire.	KVKK	Personal data that can be processed with the explicit consent of the data subject are destroyed when the data subject withdraws his/her explicit consent.
Announcements	-	It is deleted 1 month after the announcement is out of date.	KVKK	It is destroyed in the first periodic destruction process following the 1 year period from the date of deletion.
Service - goods - product purchases that are not spread over the process	TBK TTK	It is deleted after 10 years from the date of purchase.	TBK TTK	It is destroyed in the first periodic destruction process following the 5-year period from the date of deletion.
Service-goods-product purchases throughout the process (Tender/Offer)	TBK TTK	If the result of the Tender/Offer is positive, it is deleted at the end of the 5-year period from the end of the contractual or legal relationship. If the result of the Tender / Bid is negative, it is deleted at the end of the 5-year period from the date of the tender.	TBK TTK	First periodic destruction after 10 years from the date of deletion destroyed in the process. First periodic destruction after 5 years from the date of deletion destroyed in the process.
Incoming - outgoing cargo receiving and delivering	-	It is deleted after 1 week from the end of the process.	KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.

Incoming and outgoing call records	-	-	KVKK	It is destroyed by the loss of need and timeliness.
Visitor entry-exit records	-	It is deleted after 1 month from the date of visit.		It is destroyed in the first periodic destruction process following the 5-year period from the date of deletion.
Camera recordings	-	Overwritten for 1 month	KVKK HR TBK	Overwritten for 1 month
Log records	KVKK HR TBK	It is deleted after 2 years from the date of registration.	KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.
Log records (Law No. 5651) / Internet access	5651 no. Law	-	KVKK 5651 no. law.	It is destroyed after 2 years from the date of registration.
Board of Directors, General assembly, Executive board decision	TTK	It is deleted at the end of the 10-year period following the year of the decision.	TTK KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.
Audit documents	MK TTK VUK İK OHS and other law	The type of audit, its entourage, and the actions to be taken as a result of the audit are taken into account. In any case, it is deleted at the end of the 10-year period from the audit date.	MK TTK TBK VUK KV KK Ve sair kanun	Documents that do not need to be kept are destroyed on the date of deletion. The destruction period is determined by considering the needs of the company and the up-to-dateness of the documents that need to be kept.

Invoices (Process spread transactions)	VUK TTK	It is deleted at the end of the 5-year period following the end of the process.	VUK TTK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.
Invoices (Unprocessed transactions)	VUK TTK	It is deleted at the end of the 5-year period following the invoice year.	VUK TTK KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.
Processes and documents carried out with suppliers (Ex: supplier payments, payment receipt, waybill, policy, reconciliation, progress payment, execution letters, declarations, addendum, service and consultancy purchases, declarations, forms, signature circular, mail order)	TBK VUK TTK	-	TBK VUK TTK KVKK	It is destroyed at the end of 15 years from the end of the contractual or legal transaction with the supplier.
Processes carried out with the customer (sales processes)	TBK	It is deleted after 10 years from the expiration of the contract.	TBK	It is destroyed in the first periodic destruction process following the 5-year period from the date of deletion.
Letter of guarantee/ Check	TTK	It is deleted after 5 years from the end of the relationship.	TTK KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.

GSM expenses / Vehicle expenses	-	It is deleted at the end of 1 year following the year of the transaction.	TBK KVKK	It is destroyed in the first periodic destruction process following the 9-year period from the date of deletion.
Request, complaint and satisfaction process (contractual)	TBK	It is deleted when the request or complaint is resolved.	KVKK	It is destroyed in the first periodic destruction process following the 10-year period from the date of deletion.
Request, complaint and satisfaction process (non-contractual)	-	It is deleted when the request or complaint is resolved.	KVKK	It is destroyed in the first periodic destruction process following the 3-year period from the date of deletion.
Melbusat and PPE	OHS	-	OHS	It is destroyed in the next PPE supply period.
Organization chart	-	It is destroyed when it is out of date.		
Making emergency planning	OHS	It is deleted when it becomes out of date.	KVKK	It is destroyed in the first periodic destruction process following the 5-year period from the date of deletion.
Photographing and video creation of organized or attended corporate event	-	-	KVKK	It is destroyed in the first periodical destruction process following the withdrawal of explicit consent for those that are carried out with express consent and for those that can be destroyed.
Device (computer, mobile device and gsm line) debit form	TBK HR	It is deleted after 10 years from the expiration of the contract.	TBK HR KVKK	It is destroyed in the first periodic destruction after the 10-year period from the date of deletion.

Signature Circulars	TTK ve other law	It is determined according to timeliness and need.	TTK and other law	It is determined according to timeliness and need. Those that are out of date and not needed are destroyed.
Senior management reporting from the TTK	TTK	If a transaction is made as a result of the report, it is deleted at the end of 10 years from the end of the process in which the transaction continues. If no action is taken as a result of the report, it is deleted at the end of the 10-year period from the reporting date.	KVKK	It is destroyed after 10 years from the date of expiration of the legal entity.
Senior management reporting and notifications that do not originate from the TTK	-	It is determined according to timeliness and need.	KVKK	It is determined according to timeliness and need.
Destruction report	KVKK	It is deleted at the end of 3 years from the realization of the destruction.	KVKK	It is destroyed after 10 years from the date of expiration of the legal entity.
Follow-up of incoming and outgoing documents / correspondence and documents related to the operation of the company	Depending on the nature of the document, the periods in this table are applied.			
Personal data that can be processed with the explicit consent of the data subject are destroyed when the data subject withdraws his/her explicit consent.				
Email contents	Emails are reviewed at 6 monthly intervals. The periods in this table are applied by looking at the documents and records containing personal data in the e-mail.			

Matters not mentioned in the table	Storage and destruction periods for personal data belonging to processes not specified in this table; The period during which documents and records containing personal data must be kept, the periods accepted as customary in the sector in which the activity is carried out, the duration of the legal relationship with the relevant persons, the period during which the legitimate interest of the data controller will be valid in accordance with the law and honesty rules, the timeliness of the personal data should be taken into consideration. determined by using the table.
Operation of the storage and destruction process on the basis of units	While the storage and destruction processes are operating, personal data subject to storage and destruction or a document containing personal data is obtained from the relevant unit(s). Storage and destruction processes are operated in coordination with the relevant unit(s).
Postponement of destruction	When the storage, deletion, destruction and anonymization periods specified in this table are reached, an evaluation regarding storage and destruction is made. As a result of the evaluation, the actuality of the personal data (or the document containing personal data), the legal or contractual relationship and obligations The retention and destruction process is operated or postponed to a reasonable period by evaluating the continuation status, the objective need for the personal data or the relevant document. This transaction is recorded. The record is kept for at least 3 years.

PERIODIC DISPOSAL TIMES

The operation time intervals at which periodic destruction will take place should be determined by the Company officials. However, the interval between two periodic destruction processes can be at most 6 months.

In the first periodical destruction process following the date on which the obligation to destroy personal data arises, personal data is deleted, destroyed or anonymized. Periodic destruction is carried out for all personal data at **6-month intervals (at the end of the 3rd and 9th months of each year).**

The minutes of the transactions regarding the deleted, destroyed and anonymized data are kept for at least 3 years, excluding other legal obligations.

TABLE OF UPDATE CONTENT MADE TO THE CURRENT PERSONAL DATA RETENTION AND DISPOSAL POLICY

DATE OF UPDATE	BEFORE THE UPDATE	AFTER THE UPDATE

PROTOCOL

The above-mentioned deletion, destruction and anonymization processes; It is recorded with the report prepared with the triple signature of the relevant unit manager, chief and personnel who carry out the transactions.

REPORT ON DISPOSAL OF PERSONAL DATA THAT DOES NOT NEED TO BE STORED

Disposal Officer	
Disposal Unit	
Disposal Unit Officer	
Disposal Unit Personnel	
Destruction Date – Number	
Location of Personal Data	
Disposal Process	
Company / Person Carrying Out the Transport	
Plate of Loading Vehicles	
Place of Destruction	
The Way of Destruction	

Disposal Officer

Disposal Unit Personnel **Disposal Unit Personnel**

Names, Surnames, Titles and Signatures of Other Persons Involved in the Disposal Process:

Name and Surname	Title	Signature