EMIRSON GLOBAL FOREIGN TRADE LIMITED COMPANY
POLICY ON THE PROTECTION AND PROCESSING OF PERSONAL DATA

1. INTRODUTION

1.1. Generally

Ensuring the confidentiality and security of personal data and compliance with the relevant legal regulations are among the most important priorities of Emirson Global Foreign Trade Limited Company (“Company”), and utmost care is taken in this regard. In this context, the process and targeted purpose managed by this Personal Data Protection and Processing Policy (“Policy”) and other written policies within the Company regarding the processing and protection of personal data; informing our employees, employee candidates, visitors, guests and other third parties ("Related Persons") about the processing, storage and protection of personal data in accordance with the law and reflecting our corporate culture.

In the preparation of this Policy; We see the provisions in the relevant legal norms regarding the protection and processing of personal data, especially the regulations in the Constitution of the Republic of Turkey and the Law on the Protection of Personal Data No. 6698 ("KVKK") and in the decisions of the Personal Data Protection Board as a guide for our Company.

In this Policy, explanations will be made regarding the following basic principles adopted by our Company for the processing of personal data:

- Processing personal data in accordance with the law and honesty rules
- Keeping personal data accurate and up-to-date when necessary
- Processing personal data for specific, explicit and legitimate purposes,
- The personal data are linked, limited and measured for the purpose for which they are processed,
- Keeping personal data for as long as required by the relevant legislation or for the purpose for which they are processed,
- Clarification of relevant persons,
- Establishing the necessary processes for the relevant persons to exercise their rights,
- Taking the necessary measures in the processing and preservation of personal data,
- Transferring personal data to third-parties in line with the requirements of the processing purpose,
- Showing the necessary sensitivity in the processing and protection of personal data of special nature,
- Deletion, destruction or anonymization of personal data whose purpose of processing is lost.

1.2 Purpose of the Policy

The main purpose of this Policy is to make explanations about the personal data processing activity carried out by our **Company** in accordance with the law and the procedures adopted for the protection of personal data and to provide transparency by informing the **Relevant People** within this scope. In addition, this KVK Policy and other written policies aim to make our principle of compliance with

KVKK and other relevant legal regulations regarding personal data security sustainable.

1.3. Scope of the Policy

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

1.4 Implementation of the Policy and Related Legislation

This Policy has been embodied and arranged within the framework of the principles set forth by the relevant legislation. Our company undertakes and accepts that in case of inconsistency between the legislation in force and this Policy, the applicable legislation will find an area of application.

1.5 Enforcement of the Policy

This policy enters into force after being approved by our Company's board of directors, is published on the website (www.emirson.com.tr) and is made available to Relevant Persons in this way.

2 DEFINITIONS AND ABBREVIATIONS

Open Consent	Consent on a particular subject, based on the information and expressed with free will
Making Anonymous Fetch/Anonymize	Making personal data incapable of being associated with an identified or identifiable natural person in any way, even by matching with other data
Employee	Company employees
Employee Candidate	Real persons who have applied for a job or submitted their CV and related information to our Company for review by any means.
Related person	A real person whose personal data is processed
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 in whole or in part by automatic or non-automatic means provided that it is a part of any data recording system. All kinds of operations performed on data, such as blocking
Committee	Personal Data Protection Committee

Board	Personal Data Protection Board
Organisation	Personal Data Protection Authority
KVK Policy	Personal Data Protection and Processing Policy
KVKK	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 trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data
Periodic Disposal Process	In the event that all of the personal data processing conditions in the Law are eliminated, the deletion, destruction or anonymization process is to be carried out ex officio at repetitive intervals and specified in the personal data storage and destruction policy.
Policy	KVK Policy
Potential Customer	Persons who have requested to use our services or who have been evaluated in accordance with the rules of commercial practice and honesty
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	Registry system, directory, where personal data are 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
Data Controller Application Form	The application form that the Relevant Persons will benefit from when using their applications regarding their rights in Article 11 of the KVKK
Deleting Data	Making personal data inaccessible and unusable for the relevant users in any way
Destroying Data	Making personal data inaccessible, irretrievable and reusable by anyone in any way

Visitor	Real persons who have entered the physical campuses owned by the institution for various purposes or visited the websites

3 PRINCIPLES OF PROCESSING PERSONAL DATA

3.1 Processing of Personal Data in Compliance with the Principles Established in the Legislation

3.1.1. Legal and Integrity Processing

Our company has adopted the principle of complying with the law and honesty rules in all transactions to be carried out on personal data. In this context, by adopting the principle of transparency, it informs the **Related People** about the purpose of use of the personal data collected through this Policy and other texts.

3.1.2. Ensuring Personal Data Are Accurate and Up-to-Date When Necessary

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

3.1.3. Processing for Specific, Explicit, and Legitimate Purposes

Our company clearly determines the purpose of processing personal data within legitimate and legal limits and presents it to the Information of **Relevant People** through this Policy and other texts before the personal data processing activity begins.

3.1.4. Relating to the Purposes for which they are Processed, Limited and Measured

Our company processes personal data within the scope of the necessary purposes for the execution of the activity in a way that is related and proportional to the field of activity. In this context, while carrying out data processing activities, it carefully refrains from processing personal data that is not related to the realization of the purpose and is not needed at present/in the future.

3.1.5. Retention for as Long as Required for the Purpose of Processing or Envisioned in the Relevant Legislation

Our company retains personal data only for the period specified in the relevant legislation or for the period required for the purpose for which they are processed. In this context, first of all, it is determined whether a period is determined in the relevant legislation for the storage of personal data, if a period is determined, action is taken in accordance with this period.

In this context, **our Company** prepares and implements the policy and directive regarding the deletion, destruction or anonymization of personal data.

3.2 Processing of Personal Data in Compliance with and Limited to the Personal Data Processing Conditions specified in Article 5 of the KVKK

Our company processes personal data only on the basis of the explicit consent of the **Relevant Person** or in cases where explicit consent is not required in the PDPL, without explicit consent, in a limited manner to these circumstances and conditions.

3.2.1. Open Consent

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

3.2.2. Circumstances Where Explicit Consent is Not Required

KVKK m. 5/2 regulates the processing of personal data in some cases without the explicit consent of the **Relevant Person**. Since obtaining explicit consent from the data subject in the presence of one of the specified conditions will be considered as misleading the **Relevant Person**, **our Company** does not apply for explicit consent in cases where data processing conditions are present.

3.3 Processing of Private Personal Data

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

By **our company**; Special categories of personal data can be processed in the following cases, provided that adequate measures to be determined by the Board are taken, if the person concerned does not have express consent.

a) Private personal data other than the health and sexual life of the person concerned, in cases stipulated by the laws,

b) Private personal data regarding the health and sexual life of the person concerned, but only for the purposes of protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing, or persons or authorized institutions under the obligation to keep confidential. It can be processed by organizations without seeking the explicit consent of the person concerned.

Our Company has determined additional measures and processes regarding the processing of personal data of special nature and access to this data. In this framework, the environments where sensitive personal data are stored are protected with secondary locks and secondary passwords and are only processed by authorized persons within the framework of the authorization matrix.

3.4 Transfer of Personal Data

Personal data, in order to fulfill the purposes specified in this Policy, to supervisory institutions within the framework of audit activities, to our shareholders, legally authorized public institutions and organizations, domestic and / or foreign suppliers and organizations due to reasons arising from auditing and partnership rights in accordance with the relevant legal regulations. to our business partners, natural persons to whom services are supplied or third parties to whom services are rendered.

It can be transferred within the framework of the personal data processing conditions and purposes specified in Article 8 and Article 9 of the KVKK.

4 PRINCIPLES ON THE PROTECTION OF PERSONAL DATA

4.1 Technical and Administrative Measures Taken by Our Company Regarding the Security of Personal Data

4.1.1 Technical Measures

The main technical measures taken by **our company** to ensure that personal data are processed in accordance with the law and to prevent unlawful access to personal data are as follows:

- Personal data processing activities carried out within **our company** are audited by established technical systems.
- Knowledgeable and experienced personnel in technical matters are employed.
- Relevant departments on technical issues have been established.
- The technical measures taken are periodically reported to the authorized unit/person as required by the internal audit mechanism.
- A backup program is used in accordance with the law to ensure that personal data is kept securely.
- New technological developments are followed and technical measures are taken on systems, especially in the field of cyber security, and the measures taken are periodically updated and renewed.
- Access and authorization technical measures are used within the framework of legal compliance requirements determined for each department within **our company**.
- Access authorizations are limited, authorizations are regularly reviewed, and accounts of former employees are closed.
- Software and hardware including virus protection systems and firewalls are used.
- The use of counterfeit software and hardware is strongly avoided. All of the products we use are original and licensed.

In this framework, our Company carries out continuous and sustainable studies on the following technical measures determined by the Board:

- Authority Matrix
- Authorization Control
- Access Logs
- User Account Management
- Network Security
- Application Security
- Encryption
- Intrusion Detection and Prevention Systems
- Log Records
- Backup
- Firewalls

• Current Anti-Virus Systems
• Delete, Destroy or Anonymize
• Key Management

4.1.2. Administrative Measures

The main administrative measures taken by **our company** to ensure that personal data are processed in accordance with the law and to prevent unlawful access to personal data are as follows:

• Our personnel are informed and trained on the law of protection of personal data and the processing of personal data in accordance with the law.

• Personal data processing activities carried out by **our company's** business units; The requirements to be fulfilled in order to ensure that these activities comply with the data processing conditions specified in the KVKK are examined for each business unit and the activity carried out.

• With the contracts and documents governing the legal relationship between **our Company** and employees, the Company's instructions and the obligations of not processing, disclosing or using personal data, except for the exceptions made by law, the awareness of employees is increased.

• In order to meet the legal compliance requirements determined on the basis of our business units, awareness is created specific to the relevant business units and implemented. Necessary administrative measures are implemented with in-house policies and training to ensure the supervision of these issues and the continuity of the implementation.

• Access to personal data and authorization processes are designed and implemented within **our Company** in accordance with activity-based legal compliance requirements.

• It is followed by the Personal Data Protection Committee, which was established for convenience and compliance in the follow-up of works and transactions related to KVKK and other relevant regulations.

• Provisions are added to the contracts concluded by **our company** with third-parties to whom personal data are transferred in accordance with the law, that necessary security measures will be taken to protect the transferred personal data and that these measures will be complied within their own establishments.

In this framework, regarding the administrative measures determined by the Board and listed below, **our company** carries out continuous and sustainable studies:

• Preparation of Personal Data Processing Inventory
• Corporate Policies (Access, Information Security, Use, Storage and Disposal etc.)
• Contracts (Between Data Controller - Data Controller, Data Controller - Data Processor)
• Confidentiality Commitments
• In-house Periodic and/or Random Audits
• Risk Analysis
• Employment Contract, Disciplinary Regulation (Adding Legal Provisions)
• Corporate Communication (Crisis Management, Informing the Board and Relevant Person, Reputation Management, etc.)
• Training and Awareness Activities (Information Security and Law)
• Notification to Data Controllers Registry Information System

4.2 Raising Awareness and Supervision of Our Employees on the Protection of Personal Data

Our company ensures that necessary training and meetings are held in order to raise awareness to prevent unlawful processing of personal data, to prevent illegal access to data, and to ensure the safekeeping of data.

In order to increase the awareness of the current employees of **our company** on the protection of personal data, we work with professional people if needed.

4.3 Protection of Private Personal Data

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

4.4 Process to Follow in Case of Unauthorized Disclosure of Personal Data

Our company will notify the relevant person and the Board within 72 hours, in the event that the personal data it processes is obtained by others unlawfully.

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

4.5 Personal Data Inventory

Each unit of **our company** creates an up-to-date personal data processing inventory. The unit manager is responsible for the accuracy, timeliness and submission of this inventory to the contact person when necessary. Keeping inventories accurate, implementing the current Company policy on the protection of personal data, and current developments in the protection of personal data are always followed.

5. APPLICATION OF RELATED PERSONS TO DATA SUPPORTER, OUR COMMUNICATION CHANNELS AND EVALUATION PROCESSES OF THE APPLICATION

5.1 Subject of Application

Our company attaches great importance and value to the rights of **Related People** and provides them with the opportunity and opportunity to exercise these rights. An "Application Form for Data Controller", in which the relevant persons can easily submit their requests, has been prepared by **our company** and published on our website. However, **Relevant People** are not obligated to use this form. Every application made in accordance with the Communiqué on Application Procedures and Principles to the Data Controller will be evaluated.

Everyone has the right, by making an application to **our Company**;

a) Learning whether personal data is processed or not,

b) If personal data has been processed, requesting information about it,

c) To learn the purpose of processing personal data and whether they are used in accordance with its purpose,
d) To know 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,
f) Requesting the deletion or destruction of personal data within the framework of the conditions stipulated in Article 7 of the KVKK,
g) Requesting notification of the transactions made pursuant to subparagraphs (d) and (e) to third parties to whom personal data has been transferred,
h) Objecting to the emergence of a result against the person himself by analyzing the processed data exclusively through automated systems,
i) To request the compensation of the damage in case of loss due to unlawful processing of personal data.

5.2 Application Method and Address

Application Method	**Address to Apply**	**Application Subject Heading**
Manual application *(In case the applicant applies personally The document proving the identity must be available, and if the application is made by proxy, a notarized power of attorney must be available.)*	Kosuyolu Mah. Muhittin Ustuundag Cad. No:57 KADIKOY/ISTANBUL	"*Information Request Under the Law on Protection of Personal Data*" will be written on the envelope.
Notary public notice	Kosuyolu Mah. Muhittin Ustuundag Cad. No:57 KADIKOY/ISTANBUL	"*Information Request Under the Law on Protection of Personal Data*" will be written in the notification envelope.
Email Via E-Sign/Mobile Signature	info@emirson.com.tr	"*Information Request Under the Law on Protection of Personal Data*" will be written in the subject part of the e-mail.

Application via Registered Electronic Mail address	info@emirson.com.tr	"*Information Request Under the Law on Protection of Personal Data*" will be written in the subject part of the e-mail.
The e-mail address registered in our systems (Your e-mail address must match your identity in our systems before.)	info@emirson.com.tr	"Information Request Under the Law on Protection of Personal Data" will be written in the subject part of the e-mail.

5.3 Post Application Process

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

Related People; In cases where the application is rejected in accordance with Article 14 of the KVKK, the answer given is insufficient or the application is not answered in due time; Complaints can be made to the Board within thirty days from the date of **our company's** response, and in any case within sixty days from the date of application.

5.4 Application Fee

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

6. INFORMING AND INFORMING RELATED PERSONS

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

A Data Controller Application Form has been created and published on **our Company's** website in order for the Data Subject to exercise their rights specified in the KVKK more comfortably. The relevant section is explained in detail in the 5th heading.

7. PURPOSE OF PROCESSING AND STORAGE OF PERSONAL DATA

7.1 Purposes of Processing Personal Data

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

- The processing of personal data is clearly stipulated in the law for **our Company** to carry out relevant activities,
- The processing of personal data by **our Company** is directly related to and necessary for the establishment or performance of a contract,
- The processing of personal data is mandatory for **our Company** to fulfill its legal obligations,
- Provided that the personal data has been made public by the person concerned; processed by the **Company** in a limited manner for the purpose of publicizing,
- The processing of personal data by the **Company** is mandatory for the **Company** to establish, exercise or protect a right,
- It is compulsory to process personal data for the legitimate interests of the **Company**, provided that it does not harm the fundamental rights and freedoms of the persons concerned,
- The processing of personal data by **our company** is mandatory for the protection of the life or physical integrity of the relevant persons or someone else, and in this case, the persons concerned are unable to express their consent due to actual impossibility or legal invalidity,
- Special categories of personal data other than the health and sexual life of the persons concerned, in cases stipulated by the laws,
- Persons or authorized institutions and organizations that are under the obligation to keep confidential personal data related to the health and sexual life of the persons concerned, for the purpose of protecting public health, conducting preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and their financing. processed by.

7.2 Retention Periods of Personal Data

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

When 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, this personal data is deleted and backed up only to provide evidence in possible legal disputes or to assert the relevant right related to personal data. In this case, personal data is not accessed for any other purpose. Personal data is destroyed or anonymized after the periods specified in **our Company's** Personal Data Retention and Disposal Policy expire.

The processed personal data and personal data inventories are reviewed in 6-month periods and the personal data that needs to be deleted/destroyed are deleted/destroyed within these 6-month

periodic destruction periods and the transaction is recorded.

8. PERSONAL DATA PROCESSING ACTIVITIES IN WORK AREAS

8.1 Monitoring Activity with Camera at the Entrances and Inside of the Work Areas

By **our company**; In order to ensure the safety of the **Relevant People** and **our Company**, personal data processing activities are carried out for monitoring the entrance/exit and overtime monitoring, with security camera monitoring at the entrance and inside the work areas, where we provide services and carry out these services. In this context, as the **Company**, we act in accordance with the KVKK and other relevant legislation.

8.1.1 Informing about the Monitoring Activity with a Camera

Our company informs the relevant persons in accordance with Article 10 of the KVKK; thus, it is aimed to prevent harming the fundamental rights and freedoms of the persons concerned and to ensure transparency. For the camera monitoring activity, the Company's website is illuminated both with this Policy (online Policy) and with a notification letter stating that monitoring will be made at the entrances of the areas where monitoring is performed (on-site lighting/layered lighting).

8.1.2. Purpose of Surveillance with Cameras

As a **company**, we process personal data in accordance with the KVKK in connection with the purpose for which they are processed, limited and measured. The purpose of maintaining video camera recording and monitoring activities by the **company** is limited to the purposes listed in this Policy. In this direction, the monitoring areas, the number of security cameras and when they will be monitored are implemented in a limited manner and sufficient to achieve the security purpose.

8.1.3. Ensuring the Security of Data Obtained by Camera Monitoring Activity

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

8.1.4. Who Has Access to the Information Obtained as a Result of Monitoring and To Whom This Information is Transferred

Only authorized persons can access the information obtained as a result of monitoring and the storage environment. Live camera footage can be viewed by security personnel who are employees of the **Company** or outsourced services. A limited number of people who have access to the records declare that they will protect the confidentiality of the data they access with a confidentiality agreement.

8.2. Visitor Entry/Exit Tracking at the Entrances and Inside of the Work Areas

By the **company** and the outsourced company; Personal data processing is carried out in order to ensure security and for the purposes specified in this Policy, to monitor visitor entries and exits in the **Company's** work areas.

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

8.3. Recording the Information of Electronic Devices at the Entrances of the Work Areas

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

9. REVIEW

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

10. PERSONAL DATA PROTECTION COMMITTEE

The company has appointed a contact person within the framework of personal data protection law. A committee of 5 people was formed among the employees of the company units. The Personal Data Protection Committee (“Committee”) is chaired by the **Company** contact person.

The contact person acts with the opinions and recommendations of the Committee on administrative and technical measures. The principles determined by the Committee regarding administrative and technical measures are taken into account. The Committee makes every effort to comply with the **Company**'s personal data protection legislation. The contact person supervises the **Company** units for which he is responsible within the scope of personal data protection law. As a result of these audits, it warns the relevant units when necessary and informs the senior management of the situation.

The liaison person provides the coordination to respond to the related person applications made to the **Company** within the legal deadlines and in accordance with the procedure. The contact person manages the Company's relations with the Personal Data Protection Authority.

11. ENFORCEMENT

This Policy enters into force as of the date of acceptance and announcement by the company's board of directors/authorized bodies.