

**CAF MEKANİK SAN.İNŞ.LTD.ŞTİ**

**PERSONAL DATA PROTECTION POLICIES**

**Document Date: 14.08.2020**

**CONTENTS**

**PERSONAL DATA PROTECTION POLICIES ..... ..**

**1. DATA PRIVACY COMMITMENT ..... ..**

**2. PURPOSE OF THE POLICY ..... ..**

**3. SCOPE OF THE POLICY ..... ..**

**4. DEFINITIONS ..... ..**

**5. PRINCIPLES OF PERSONAL DATA PROCESSING ..... ..**

**6. PROCESSING OF PERSONAL DATA ..... ..**

**7. PROCESSING OF SPECIAL QUALITY PERSONAL DATA ..... ..**

**8. DELETING, DESTRUCTION AND ANONYMIZING OF PERSONAL DATA ..... ..**

**9. TRANSFER OF PERSONAL DATA AND PROCESSING OF PERSONAL DATA BY THIRD PARTIES**

**10. COMPANY'S LIGHTING OBLIGATION AND RIGHTS OF DATA OWNER ..... ..**

**11. MEASURES TAKEN FOR DATA MANAGEMENT, SECURITY AND PROTECTION OF PERSONAL DATA**

**12. EDUCATION ..... ..**

**13. AUDIT ..... ..**

**14. VIOLATIONS ..... ..**

**15. RESPONSIBILITIES ..... ..**

**16. CHANGES TO THE POLICY ..... ..**

**17. EFFECTIVE DATE OF THE POLICY ..... ..**

## **PERSONAL DATA PROTECTION POLICY**

### **1. DATA PRIVACY COMMITMENT**

CAF MEKANİK SAN.İNŞ.LTD.ŞTİ ("Company") undertakes to act in accordance with this Policy and the procedures to be applied depending on the Policy in terms of Personal Data within its structure.

### **2. PURPOSE OF THE POLICY**

The purpose of this policy is to determine the principles regarding the methods and processes for the protection of personal data within the scope of the Law on the Protection of Personal Data No.6698 ("KVKK") regarding Company activities.

### **3. SCOPE OF THE POLICY**

This Policy covers all activities for Personal Data that the Company carries out all kinds of processing activities in order to continue its activities and is applied to the said activities.

This Policy may be amended from time to time if required by the KVK Regulations or in cases deemed necessary by the Company's Data Responsible Representative or management, provided that legal obligations are observed.

### **4. DEFINITIONS**

The definitions in this Policy have the following meanings;

"*Explicit Consent*" refers to the consent of the Personal Data Owners freely declared on the basis of their information about the processing of their data and without any conditions.

"*Anonymization*" refers to making Personal Data that cannot be associated with an identified or identifiable natural person under any circumstances, even if they are matched with other data.

"*Anonymized Data*" refers to data that cannot be associated with a natural person in any way.

"*Personal Data*" refers to all kinds of information pertaining to an identified or identifiable natural person.

"*Processing of Personal Data*" Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available to Personal Data fully or partially automatically or by non-automatic means provided that it is a part of any data recording system. refers to all kinds of operations on data such as classification or prevention of use.

"*Board*" refers to the Personal Data Protection Board.

"*Institution*" refers to the Personal Data Protection Authority.

"*KVKK*" refers to the Personal Data Protection Law No. 6698.

"*KVK Regulations / Provisions*" Law No. 6698 on the Protection of Personal Data and other relevant legislation on the protection of Personal Data, binding decisions, resolutions, provisions, provisions, instructions issued by regulatory and supervisory authorities, courts and other official authorities and applicable international agreements on data protection. and refers to any other legislation.

"*KVK Procedures*" refers to the procedures that determine the obligations that the Company, employees and Data Responsible Representative must comply with under this Policy.

"*Special Qualified Personal Data*" With data on the race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress, association, foundation or union membership, health, sexual life, criminal conviction and security measures express biometric and genetic data.

"*Deletion*" is the process of making Personal Data inaccessible and unusable for the relevant users in any way.

"*Personal Data Inventory*" processes and methods of Personal Data Processing for the Company's Personal Data Processing activities, Personal Data Processing purposes, data category, third parties to whom Personal Data is transferred, etc. Refers to the inventory containing the information.

"*Data Processor*" refers to the natural or legal person who processes Personal Data on behalf of the Data Controller, with the authorization of the Data Controller.

"*Data Owner*" refers to the real person to whom Personal Data belongs.

"*Data Controller*" refers to the natural or legal person who processes Personal Data by specifying the purposes and ways of processing, and who is responsible for the establishment and management of the data recording system.

"*Data Responsible Representative*" refers to the employee who carries out the relations of the Company with the Authority.

"*Destruction*" means the destruction of personal data, making it inaccessible, unavailable and unusable by anyone.

## **5. PERSONAL DATA PROCESSING PRINCIPLES**

### **5.1. Processing of Personal Data in Compliance with Law and Good Faith Rules**

Personal Data is processed by the Company in accordance with the law and honesty rules and on the basis of proportionality. What is meant by proportionality is to process as much personal data as necessary for company activities for the required period.

### **5.2. Taking Necessary Precautions To Keep Personal Data Accurate and Updated When Required**

The Company takes all necessary measures to ensure that the Personal Data is complete, accurate and up-to-date, and updates the Personal Data in case the Data Owner requests changes to the Personal Data.

### **5.3. Processing of Personal Data for Specific, Legitimate and Clear Purposes**

Before the Processing of Personal Data, the Company determines the purpose for which Personal Data will be processed. In this context, the Data Owner is enlightened within the scope of KVK Regulations and their Explicit Consent is obtained when necessary.

### **5.4. Being Connected, Limited and Measured for the Purpose of Processing Personal Data**

The Company processes Personal Data only in accordance with the purpose within the scope of the Explicit Consent received from the Data Owner and in accordance with the principle of proportionality in cases where explicit consent is not required within the scope of the KVK Regulations and / or in cases where explicit consent is required.

### **5.5. Keeping Personal Data as Required and Deleting Afterwards**

**5.5.1.** The Company maintains Personal Data as required for company activities in accordance with the purpose of processing. If the company wishes to retain Personal Data for a period longer than the duration stipulated in the KVK Regulations or required by the purpose of Personal Data Processing, the Company complies with the obligations specified in the KVK Regulations.

**5.5.2.** After the expiry of the period required by the purpose of Personal Data Processing, Personal Data are Deleted, Destroyed or Anonymized. In this case, it is ensured that third parties to whom the Company transfers Personal Data are also provided with Deletion, Destruction or Anonymization of Personal Data.

**5.5.3.** The Data Responsible Representative is responsible for the operation of the Deletion, Destruction and Anonymization processes. In this context, the necessary procedure is created by the Data Controller Representative.

## **6. PROCESSING OF PERSONAL DATA**

Within the scope of the Company's activities, personal data can be processed in order to carry commercial activity and to provide services, including but not limited to the purposes listed below;

- Carrying out activities,
- Providing services within the scope of the contract and within the framework of service standards and fulfilling the contract requirements,
- Fulfilling legal obligations as required or required by legislation
- Evaluation of job applications and employment. During the application process as an Employee Candidate, shared by any method, CV, diploma, etc. Personal data contained in other documents can be processed, stored and transferred within the scope of this Policy for job application evaluation. In case of employment, the personal data of the employees are processed, stored and transferred in accordance with the Labor Law No. 4857 and other legislative obligations,
- Establishing contact with people who have a business relationship with the company,
- Marketing,
- Receiving and giving advertisement,
- Legal and financial reporting,
- Billing.

Personal Data can only be processed by the Company within the scope of the procedures and principles stated below.

### **6.1. Open Consent**

In cases where explicit consent is required for the processing of Personal Data within the scope of KVK Regulations;

**6.1.1.** Personal Data are processed after the information to be made within the framework of fulfillment of the Disclosure Obligation to Data Owners and if the Data Owners give Explicit Consent.

**6.1.2.** Data Owners are informed of their rights before express consent is obtained within the framework of the Disclosure Obligation.

**6.1.3.** Explicit Consent of Data Owners is obtained through methods in accordance with KVK Regulations. Explicit Consent is retained by the Company for the period required within the scope of KVK Regulations in a provable manner.

**6.1.4.** The Data Responsible Representative ensures the fulfillment of the Disclosure Obligation in terms of all Personal Data Processing processes and obtaining and maintaining Open Consent when necessary. All department employees that process Personal Data are obliged to comply with the instructions of the Data Responsible Representative and this Policy.

### **6.2. Processing of Personal Data without Explicit Consent**

**6.2.1** In cases where the Processing of Personal Data without Explicit Consent is envisaged within the scope of the KVK Regulations (in cases enumerated in the laws including but not limited to Article 5.2 and Article 6.3 of the KVKK), the Company may process Personal Data without obtaining the Explicit Consent of the Data Owner. In the event that Personal Data is processed in this way, the Company processes Personal Data within the limits set by the KVK Regulations and in compliance with the Disclosure Obligation. In this context:

**6.2.1.1.** Personal Data may be processed by the Company without Explicit Consent in order to protect the life or body integrity of a person other than the Data Subject and / or a person other than the Data Subject who is unable to disclose his consent due to actual impossibility or whose consent is not legally valid.

**6.2.1.2.** If the conditions to be directly related to the establishment, implementation, execution or termination of a contract are met, the Personal Data of the parties to the contract may be processed by the Company without the Data Owners' Explicit Consent. In this sense, service agreements, employment agreements, lease agreements etc. to which the Company is a party. Personal data collected within the scope of all contracts necessary for the continuation of its activities, such as, are processed, stored, deleted and destroyed within the framework of this Policy without express consent.

**6.2.1.3.** If the Processing of Personal Data is mandatory for the Company to fulfill its legal obligation, Personal Data may be processed by the Company without the Data Owners' Explicit Consent.

**6.2.1.4.** Personal Data made public by the Data Owner can be processed by the Company without express consent.

**6.2.1.5.** If the processing of Personal Data without express consent is the only possible way to establish, use or protect a right, the Personal Data may be processed by the Company within the knowledge of the Data Controller Representative without obtaining Explicit Consent.

**6.2.1.6.** Provided that it does not harm the fundamental rights and freedoms of the Data Owners, Personal Data may be processed by the Company without Explicit Consent if data processing is necessary for the legitimate interests of the Company.

## **7. PROCESSING OF PRIVATE PERSONAL DATA**

**7.1.** Private Personal Data can only be processed with the Explicit Consent of the Data Owner or if processing is explicitly required by the law for Private Personal Data other than sexual life and personal health data.

**7.2.** The company does not collect, store and process in any way special quality personal data, except for the Private Personal Data that are stipulated to be received as a legal requirement due to the employment contracts it is a party to or transferred to it.

**7.3.** Private Personal Data related to health and sexual life can only be processed without express consent for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing. Therefore, until otherwise stipulated in the KVK Regulations, personal health data and sexual life data

can only be processed within the scope of Open Consent or by the Company physician who is under the obligation of secrecy.

**7.4.** When processing Private Personal Data, the measures determined by the Board are taken.

**7.5.** In any case that requires the Processing of Private Personal Data, the Data Responsible Representative is informed by the relevant employee.

**7.6.** If it is not clear whether a data is Private Personal Data, the opinion of the Data Controller Representative is taken by the relevant department.

## **8. PERSONAL DATA STORAGE, DELETION, DESTRUCTION AND ANONYMOUSING**

**8.1.** When the legitimate purpose of the Processing of Personal Data disappears, the relevant Personal Data is Deleted, Destroyed or Anonymized. Situations where Personal Data needs to be Deletion, Destroyed or Anonymized are followed up by the Data Responsible Representative.

**8.2.** Resumes sent to the company by any means are deleted within 1 year at the latest, if there is no return.

**8.3.** Personal data shared to the Company on the contact screen specified on the [www.cafendustri.com](http://www.cafendustri.com) web sites are deleted within three months at the latest.

**8.4.** The personal data acquired by the Company due to the employment contracts to which it is a party are destroyed upon the termination of the storage obligation arising from the employment contract.

**8.5.** The Company does not store Personal Data solely for the possibility of future use. The above articles also apply to personal data that the company does not collect but is transferred to the company for similar purposes.

## **9. TRANSFER OF PERSONAL DATA AND PROCESSING OF PERSONAL DATA BY THIRD PARTIES**

The Company may transfer Personal Data to a third natural or legal person ("Contractor") in accordance with the KVK Regulations. In this case, the Company ensures that the third parties to whom Personal Data has been transferred comply with this Policy. In this context, necessary protective regulations are added to contracts concluded with third parties. The item to be added to the contracts concluded with third parties to whom any Personal Data transfer is made is provided from the Data Responsible Representative. Each employee is obliged to go through the process in this Policy in case of Personal Data transfer. In the event that the third party to whom the Personal Data is transferred requests a change in the item transmitted by the Data Controller Representative, the employee notifies the Data Controller Representative immediately.

Personal data, including but not limited to the following;

- Suppliers,
- Business partners and business contacts,
- Legally authorized public institutions and organizations,
- Legally authorized private legal persons,

- It can be transferred to the shareholders according to the principles and rules explained in this Policy.

### **9.1. Transfer of Personal Data to Third Parties Found in Turkey**

**9.1.1.** Personal Data KVK Provisions of the specified cases open without their consent, Outdoor consent is sought in cases where the Data Owner in Turkey with the requirement to get explicit consent by third parties to the Company of their activities more or liabilities transferred in order to be fulfilled.

**9.1.2.** The company, the transfer of personal data to third parties in Turkey is responsible for ensuring that the REIT Regulations.

### **9.2. Personal Data Transfer to Third Parties Abroad**

**9.2.1.** The company will be able to transfer personal data abroad within the framework of this Policy and the provisions of the legislation due to the mail system.

**9.2.2.** Personal Data may be transferred by the Company to third parties abroad, provided that the Explicit Consent of the Data Owner is obtained, without the express consent of the KVK provisions.

**9.2.3.** In the event that Personal Data is transferred without express consent in accordance with the KVK Regulations, one of the following conditions must be present in terms of the foreign country to which it will be transferred:

**9.2.3.1** The foreign country to which the Personal Data is transferred is in the status of countries with sufficient protection by the Board (please follow the current list of the Board for a list),

**9.2.3.2** In case the foreign country where the transfer will take place is not included in the Board's list of safe countries, the Company and the Data Controllers in the relevant country must obtain a written commitment from the Board to ensure adequate protection.

**9.2.4.** The Company is responsible for ensuring that the transfer of Personal Data abroad to third parties is in accordance with the KVK Regulations.

**9.2.5.** The company can get services from service providers such as Google, Hotmail, Outlook for electronic communication purposes. In this context, personal data that may be included in the electronic communications of the company are stored on the servers of the service providers, and are stored, transferred and processed within the scope of the data protection policies of the said companies.

## **10. COMPANY'S LICENSE OBLIGATION AND RIGHTS OF DATA OWNER**

**10.1.** The Company enlightens the Data Owners regarding the Processing of Personal Data in accordance with Article 10 of the KVKK. In this context, the Company fulfills the Disclosure Obligation with the Clarification Text prepared during the acquisition of Personal Data. The notification to be made to the Data Subjects within the scope of the Disclosure Obligation includes the following elements in order:

Identity of the Data Controller and, if any, its representative,

- The purpose for which Personal Data will be processed,



- To whom and for what purpose the processed Personal Data can be transferred,
- Method and legal reason for collecting Personal Data,

The relevant person can receive information on the following issues by filling the Application Form and sending it to the address kvkk @ ..... com.tr specified in the Company's Clarification Text;

- Learning whether personal data is processed,
- Requesting information if personal data has been processed,

Learning the purpose of processing personal data and whether they are used appropriately for their purpose,

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

Objecting to an unfavorable result arising from the analysis of the processed data exclusively through automated systems,

- To request the compensation of the damage in case of damage due to the unlawful processing of personal data

**10.2.** In the event that the Data Owner requests information regarding his / her personal data processed in accordance with the provisions of the KVK, it shall provide the necessary information within 30 (thirty) days at the latest after verifying the identity of the Data Owner. The Company reserves the right to reject the application, including but not limited to the reasons listed below;

- Failure to verify the identity of the person requesting information that he / she is the data owner,
- Processing personal data for purposes such as research, planning and statistics by anonymizing them with official statistics,
- Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression, provided that it does not violate the privacy of private life or personal rights or constitutes a crime,
- Processing of personal data made public by the Personal Data Owner,
- The application is not based on a just cause,
- The application contains a request contrary to the relevant legislation,
- Failure to comply with the application procedure is rejected by explaining the reason for rejection.

**10.3.** In case the application is rejected, the response given to the application is insufficient or the response is not given in time; the applicant has the right to complain to the KVK Board within 30 (thirty) days from the date of learning the answer and in any case within 60 (sixty) days from the date of application.

**10.4.** Before the Processing of Personal Data, the necessary Disclosure Obligation is fulfilled by the employee and the Data Responsible Representative who follows the relevant process.

**10.5.** In the event that the Data Processor is a third party other than the Company, it must be committed by the third party before the Personal Data Processing begins with a written agreement that the third party will comply with the above-mentioned obligations. In cases where third parties transfer Personal Data to the Company, the item to be added to the contracts is obtained from the Data Responsible Representative. Each employee is obliged to go through the process stated in this Policy in case of Personal Data transfer to the Company by a third party. In the event that the third party transferring the Personal Data requests a change in the item transmitted by the Data Controller Representative, the employee immediately notifies the Data Controller Representative.

## **11. MEASURES TAKEN FOR DATA MANAGEMENT, SECURITY AND PROTECTION OF PERSONAL DATA**

**11.1.** The Company appoints a Data Responsible Representative to fulfill its obligations under the KVK Regulations, to ensure and supervise the implementation of the KVK Procedures required for the implementation of this Policy, and to make suggestions for their functioning.

The company takes administrative and technical measures within the scope of the relevant guide of the KVK Institution in order to ensure personal data security.

### **11.1.1. Administrative Measures**

- The Company establishes Policies and procedures covering the entire data processing process, conducts periodic studies to identify existing risks and threats, and ensures transparency in the data processing process.
- Company employees are informed and trained for the protection and legal processing of Personal Data.
- Reduces processed and stored personal data as much as possible and uses the data anonymized whenever possible.
- Manages relations with real and legal persons who process personal data in accordance with the job description within the company or the business relationship with the Company. In this context, Company employees can access Personal Data only within the authority defined to them and in accordance with the relevant KVK Procedure. All kinds of access and processing performed by the employee beyond his / her authority are unlawful and it is the reason for the termination of the employment contract with a just cause. Each person assigned a Company device is responsible for the security of the devices allocated for his own use. Each Company employee or person working within the Company is responsible for the security of physical and electronic files / data within his / her area of responsibility. If a department within the company processes Special Quality Personal Data, this department is informed about the importance, security and confidentiality of the Personal Data they process, and they act in accordance with the relevant department's Data Supervisor Representative's instructions. Access to Special Qualified Personal Data is only given to limited employees, and their list and tracking are made by the Data Controller Representative. In case there are security measures requested or additionally requested for the security of Personal Data within the scope of KVK Regulations, all employees are obliged to comply with additional security measures and to ensure the continuity of these security measures. All employees involved in the relevant process are jointly responsible for the protection of Personal Data in accordance with this Policy and KVK Procedures at the rate of their defects. Company employees are informed that their obligations regarding the

security and confidentiality of Personal Data will continue after the termination of the business relationship, and commitments have been taken from the relevant employees of the Company to comply with these rules. confidentiality of the Personal Data they process, and they act in accordance with the relevant department's Data Supervisor Representative's instructions. Access to Special Qualified Personal Data is only given to limited employees, and their list and tracking are made by the Data Controller Representative. All employees must comply with additional security measures in case there are security measures requested or additionally requested for the security of Personal Data within the scope of KVK Regulations.

#### **11.1.2. Technical Measures**

- The company ensures the cyber security of all personal data it processes and stores. Information processing personnel who are knowledgeable in technical matters regarding Personal Data Processing activities are employed.
- The company monitors the cyber security of all personal data it processes and stores within its structure and carries out maintenance and inspection periodically. Personal Data Processing activities are audited by the company with technical systems according to technological possibilities and implementation costs.
- The company does not use a cloud storage system for all personal data it processes or stores.
- The company supplies information technology systems and receives development and maintenance from companies providing this service. In the company, software and hardware including virus protection systems and firewalls are installed in accordance with technological developments in order to keep Personal Data in secure environments. The company has a security policy that includes technical measures for the protection of Personal Data.
- In the company, backup programs are used to prevent the loss or damage of Personal Data and adequate security measures are taken.

### **12. EDUCATION**

The Company provides its employees with the necessary training on the protection of Personal Data within the scope of the Policy and KVK Regulations and keeps records of these trainings.

### **13. AUDIT**

The Company has the right to inspect regularly and ex officio that all employees, departments and contractors of the Company act in compliance with this Policy and KVK Regulations and perform the necessary routine inspections within this scope. The Data Controller Representative creates the KVK Procedure for these inspections and ensures the implementation of the mentioned procedure.

### **14. VIOLATIONS**

**14.1** Each employee of the company reports the work, transaction or action that he / she thinks is contrary to the procedures and principles specified in the KVK Regulations and within the scope of this Policy to the Data Responsible Representative. In this context, the Data Responsible Representative for the relevant violation creates an action plan in accordance with this Policy and KVK Procedures.

**14.2.** As a result of the information made, the Representative of the Data Controller prepares the notification to be made to the Data Owner or the Authority regarding the violation, taking into account the provisions of the applicable legislation, especially the KVK Regulations. The Data Controller Representative carries out the correspondence and communication with the Authority.

## **15. PROCESS MANAGEMENT**

Process management regarding the Protection of Personal Data within the company is provided by the employee, department, and Data Responsible Representative. In this context, the Representative of the Data Officer, who will ensure the implementation of the Policy and manage the Personal Data Protection process, is appointed with the decision of the Company management and changes within this scope are also made in the aforementioned way.

## **16. CHANGES TO THE POLICY**

The Company shares the updated Policy text so that the changes on the Policy can be reviewed with the Data Owners via e-mail and / or makes it accessible at the workplace and / or on a website that may be established in the future.

This Policy has been approved by the Board of Directors on 14.08.2020 and entered into force.

**CAF MEKANİK SAN.İNŞ.LTD.ŞTİ**