PERSONAL DATA PROTECTION AND PRIVACY POLICY

THE IMPORTANCE OF PROTECTING PERSONAL DATA

Protection of personal data is a constitutional right and is within the scope of our Company's priorities. As a matter of fact, for this purpose, it is aimed to establish a system that is constantly updated in our Company and this policy has been established.

Within the scope of the Law on Protection of Personal Data No. 6698, **MAVİMOR DANIŞMANLIK VE YÖNETİM HİZMETLERİ** A.Ş. "Hereinafter referred to as **the COMPANY** ", this Policy is made in order to fulfill the Disclosure Obligation and to determine the basic principles of our Company's personal data processing rules, and in this context, our current customers, potential customers, employees, employee candidates, supplier/subcontractor employees and officials. The basic principles regarding the protection of personal data of our company shareholders and company partners, business partners, visitors and third parties whose data we process are regulated.

PURPOSE OF THE POLICY

The main purpose of this Policy is to set forth the principles regarding the personal data processing activity carried out by the **COMPANY in accordance with the law and the protection of personal data, in this context, to ensure transparency by enlightening and informing the persons whose personal data are processed by our company.**

SCOPE

This Policy; Automatic or any data recording of the persons we have categorized under the headings of “existing customers, potential customers, employees, employee candidates, supplier/subcontractor employees and officials, company shareholders and company partners, business partnerships, visitors and other third parties whose data we process” It includes information regarding all personal data we process by non-automatic means, provided that they are part of the system.

IMPLEMENTATION OF POLICY AND RELEVANT LEGISLATION

Relevant legal regulations in force on the processing and protection of personal data will find application first. In case of inconsistency between the current legislation and the Policy, **the COMPANY** accepts that the applicable legislation will find an area of application.

ACCESS AND UPDATE

Policy Our company's websites are on **mavimor.com.tr** and **vvino.com.tr** It is published and made available to the relevant persons upon the request of the personal data owners and updated when necessary.

PROCESSING PERSONAL DATA

- Our company, in accordance with Article 20 of the Constitution and Article 4 of the KVK Law, regarding the processing of personal data; in accordance with the law and the rules of honesty, accurate and up-to-date when necessary; for specific, explicit and legitimate purposes; engages

in personal data processing activities in a connected, limited and measured manner for this purpose.

- Our company keeps personal data for as long as required by law or for the purpose of processing personal data.
- Our company processes personal data in accordance with Article 20 of the Constitution and Article 5 of the KVK Law, based on one or more of the conditions in Article 5 of the KVK Law regarding the processing of personal data.
- Our company processes the personal data of employees and employee candidates based on the purposes of work inclination and performance of the employment contract, in accordance with Article 419 of the Code of Obligations, without prejudice to the KVK Law No. 6698.
- Our company processes the personal data of the flat owners and tenants it provides services for, based on the purposes of the service contract, in accordance with the Property Ownership Law, without prejudice to the Personal Data Protection Law No. 6698.
- In accordance with Article 20 of the Constitution and Article 10 of the Personal Data Protection Law, our company informs the personal data owners and provides the necessary information in case personal data owners request information and apply to exercise their rights arising from the law, and responds to the applications within the legal time limit. .
- Our company acts in accordance with the regulations stipulated for the processing of personal data of special nature in accordance with Article 6 of the Personal Data Protection Law.
- Our company complies with the rules stipulated in the law regarding the transfer of personal data in accordance with Articles 8 and 9 of the Personal Data Protection Law, and takes into account the decisions taken by the KVK Board and the communiqués published and the safe country lists.

PROCESSING PERSONAL DATA IN ACCORDANCE WITH THE PRINCIPLES AND RULES OFFERED IN THE LEGISLATION

Principles of Processing Personal Data

Processing in Compliance with Law and Integrity;

Our company; acts in accordance with the principles brought by legal regulations and the rule of honesty in the processing of personal data. In this context, our Company determines the legal grounds that will require the processing of personal data, takes action, takes into account the proportionality requirements, does not use personal data other than what is required for the purpose, and does not perform any processing activities without the knowledge of individuals.

Ensuring Personal Data Is Accurate and Up-to-Date When Necessary

The COMPANY processes by taking into account the fundamental rights of personal data owners and its own legitimate interests, ensures that personal data is accurate and up-to-date, and takes the necessary measures in this direction. In this context, we try to keep the data on all categories of people up to date. In particular, customer and potential customer data are carefully updated, and marketing and promotional e-mails and offers are not sent to individuals against their consent.

Processing for Specific, Explicit, and Legitimate Purposes

Our company clearly and precisely determines the purpose of processing personal data, which is legitimate and lawful. Our company processes personal data as much as is necessary for and in connection with the service it provides. The purpose for which personal data will be processed by our company is determined before the processing activity and is also recorded in the "Personal Data Inventory".

Being Related to the Purpose for which they are Processed, Limited and Measured

Our company processes personal data in a way that is suitable for the realization of the determined purposes and avoids the processing of personal data that is not related to the realization of the purpose or that is not needed. In this context, processes are constantly reviewed and the Principle of Reducing Personal Data is tried to be implemented.

Retention for the Time Required for the Purpose of Processing or Envisioned in the Relevant Legislation

Our company retains personal data only for as long as required by the relevant legislation or for the purpose for which they are processed. In this context, our Company first determines whether a period is foreseen for the storage of personal data in the relevant legislation, if a period is determined, it acts in accordance with this period. In the event that the period expires or the reasons requiring its processing disappear, personal data is deleted, destroyed or anonymized in accordance with our Company's "Personal Data Retention and Destruction" policy.

Processing of General Personal Data

Protection of personal data is a constitutional right, and in accordance with the third paragraph of Article 20 of the Constitution, personal data can only be processed in cases stipulated by law or with the explicit consent of the person. Our company processes personal data without seeking the explicit consent of the person concerned, only if the following conditions are met;

1. clearly stipulated in the law,
2. It is compulsory for the protection of the life or physical integrity of the person or another person, who is unable to express his or her consent due to actual impossibility or whose consent is not legally valid.
3. Provided that it is directly related to the establishment or performance of a contract, it is necessary to process the personal data of the parties to the contract,
4. It is mandatory for the data controller to fulfill its legal obligation,
5. The person concerned has been made public by himself,
6. Data processing is mandatory for the establishment, exercise or protection of a right,
7. 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.

In the absence of the above conditions, our Company applies the explicit, free will and informed consent of the person concerned.

Rules for the Processing of Private Personal Data

Our company complies with the regulations stipulated in the Personal Data Protection Law in the processing of personal data determined as "special quality" by the Personal Data Protection Law. In Article 6 of the Personal Data Protection Law, a number of personal data that carry the risk of causing victimization or discrimination when processed unlawfully have been determined as **"special quality"** and care and sensitivity should be shown in the processing of these data. These; Data related to race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, clothing, association, foundation or union membership, health, sexual life, criminal conviction and security measures, and biometric and genetic data.

By our Company in accordance with the Personal Data Protection Law; Special quality personal data is processed in the following cases, provided that the necessary precautions are taken: Special quality personal data other than the health and sexual life of the personal data owner, in cases stipulated by the laws or based on the explicit consent of the personal data owner, Special categories of personal data regarding the health of the personal data owner However, it is processed by persons or authorized institutions and organizations under the obligation of confidentiality, or with the explicit consent of the personal data owner, for the purpose of protecting public health, preventive medicine, medical diagnosis, providing treatment and care services, planning and management of health services and financing. Regardless of the reason, general data processing principles are always taken into account in the processing processes and compliance with these principles is ensured.

Clarification and Informing of Relevant Persons whose Data is Processed

Our company informs the personal data owners during the acquisition of personal data in accordance with Article 10 of the Personal Data Protection Law. In this context

- For what purpose the personal data will be processed for the data subject,
- To whom and for what purpose the processed personal data can be transferred,
- Method of personal data collection and legal reason
- of the person whose personal data is processed.

Again, in Article 11 of the Personal Data Protection Law, “Requesting Information” is also listed among the rights of the person whose personal data is processed, and in this context, our company does not collect personal data in accordance with Article 20 of the Constitution and Article 11 of the Law on Protection of Personal Data. If the person concerned requests information, necessary information is provided. At the same time, the obligation to inform has been published on our website www.mavimor.com.tr and information details are available.

TRANSFERRING PERSONAL DATA

Our company can transfer the personal data and sensitive personal data of the person whose personal data is processed to third parties by taking the necessary security measures in line with the personal data processing purposes in accordance with the law. Accordingly, our company acts in accordance with the regulations stipulated in Article 8 of the Personal Data Protection Law.

Principles of Transfer of Personal Data

In line with the legitimate and lawful personal data processing purposes, our company may transfer personal data to third parties based on one or more of the personal data processing conditions specified in Article 5 of the Law listed below and in a limited manner:

- Based on the explicit consent of the person whose personal data is processed, or
- If there is a clear regulation in the law regarding the transfer of personal data,
- If it is necessary for the protection of the life or physical integrity of the personal data owner or someone else, and the personal data owner is unable to express his consent due to actual impossibility or if his consent is not legally valid;
- If it is necessary to transfer the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract,
- If personal data transfer is mandatory for our company to fulfill its legal obligation,
- If the personal data has been made public by the person concerned,
- If personal data transfer is necessary for the establishment, exercise or protection of a right,
- Provided that it does not harm the fundamental rights and freedoms of the person whose personal data is processed, personal data is transferred if it is necessary for the legitimate interests of our Company.

Regardless of the reason, general data processing principles are always taken into account in the transfer processes and compliance with these principles is ensured.

Transfer of Private Personal Data

Our company, by showing due diligence, taking the necessary security measures and taking the adequate measures prescribed by the Personal Data Protection Board; In accordance with the legitimate and lawful personal data processing purposes, it can transfer the sensitive data of the person whose personal data is processed to third parties in the following cases. Contact person

- If there is explicit consent, based on this or if the person concerned does not have express consent;

- Sensitive personal data other than the health and sexual life of the personal data subject (race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, clothing, association, foundation or union membership, criminal conviction and data on security measures) and biometric and genetic data), in cases stipulated by law,

- Special categories of personal data related to the health of the data subject can only be processed by persons or authorized institutions and organizations under the obligation of confidentiality for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

Regardless of the reason, general data processing principles are always taken into account in the transfer processes and compliance with these principles is ensured.

Transfer of Personal Data Abroad

Our company can transfer the personal data and sensitive personal data it processes to third parties by taking the necessary security measures in line with the legal personal data processing purposes. Personal data by our company; To foreign countries declared to have adequate protection by the Personal Data Protection Board ("Foreign Country with Sufficient Protection") or in case of insufficient protection, where data controllers in Turkey and the relevant foreign country undertake in writing to provide adequate protection and the Personal Data Protection Board It is transferred to foreign countries where permission is granted ("Foreign Country of Data Controller Undertaking Adequate Protection").

Accordingly, our company acts in accordance with the regulations stipulated in Article 9 of the Personal Data Protection Law. In line with the legitimate and lawful personal data processing purposes, our company can transfer the personal data to Foreign Countries with Sufficient Protection or Where the Data Controller Undertakes Sufficient Protection, if there is explicit consent of the person whose personal data is processed or if there is no explicit consent of the person whose personal data is processed, in case of one of the following conditions: :

- If there is a clear regulation in the law regarding the transfer of personal data,
- If it is necessary for the protection of the life or physical integrity of the person or other person whose personal data is processed, and
- personal data is processed is unable to express his/her consent due to actual impossibility or if his/her consent is not legally valid;
- If it is necessary to transfer the personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract,
- If personal data transfer is mandatory for our company to fulfill its legal obligation,
- If the personal data has been made public by the person concerned,
- Personal data transfer is the establishment, exercise or use of a right.
- If it is necessary to protect
- If personal data transfer is necessary for our Company's legitimate interests, provided that it does not harm the fundamental rights and freedoms of the personal data owner.

Purposes of Transfer of Personal Data by Our Company and Categories of Persons Transferred to

Data Transfer Purposes

To ensure the fulfillment of our company's activities and establishment purposes, to ensure that the services that our company outsources from the supplier and that are necessary to carry out our company's commercial activities are provided to our company, to ensure the execution of our company's human resources and employment policies, to fulfill our company's obligations within the framework of occupational health and safety, and to take necessary measures. Data transfer is carried out for purposes such as ensuring the receipt of data.

Persons To whom Data is Transferred

In accordance with Articles 8 and 9 of the Personal Data Protection Law of our company, personal data may be transferred to the following categories of persons:

- Authorized Public Institutions : Public institutions and organizations authorized to receive information and documents from our company, in accordance with the provisions of the relevant legislation.
- To Authorized Private Legal Persons: To private legal persons authorized to receive information and documents from our company, limited to the purpose requested by the relevant private legal persons within their legal authority.
- Shareholder : To the shareholders of our company, limited to the design of strategies regarding our company's commercial activities and audit purposes.
- Supplier : On a limited basis, in order to provide our Company with the services necessary to carry out the commercial activities of our Company, which our Company outsources from the supplier and which the parties providing services to our company while carrying out the commercial activities of our company.
- To Our Business Partners : Parties with whom our company has established business partnerships for purposes such as the execution of commercial activities, limited to ensure that the objectives of the business partnership are fulfilled.

In the transfers made by our company, we act in accordance with the principles and rules set out in this Policy.

CATEGORIES OF PERSONAL DATA RECEIVED

The persons whose data are processed in our company and the data processed in this context are categorized as follows.

Data Category	Personal Data Disclosure	Types of Personal Data Included in Relevant Personal Data
Credentials	Information contained in documents such as driver's license, identity card, residence, passport, attorney's ID, marriage certificate, which are clearly belonging to an identified or identifiable natural person and included in the data recording system	TCKN, passport no., identity card serial no, name-surname, photo, place of birth, date of birth, age, place of registration, identity card with proof example, signature
Communication information	Information that clearly belongs to an identified or identifiable natural person and is included in the data recording system, and is used for the purpose of communicating with the person.	Email address, phone number, mobile number, telephone, address etc.
Location Data	Data that are clearly belonging to an identified or identifiable natural person and are included in the data recording system, which are used to determine the location of the data owner.	Email address, phone number, mobile number, location data, address etc.
	Data that are clearly belonging to an identified or identifiable natural person and are included in the data recording system, which are used to determine the location of the data owner.	Location data obtained during the use of company vehicles
Family Members and Close Information	Information about the family members and relatives of the personal data owner, which is clearly belonging to an identified or identifiable natural person, is included in the data recording system, and is processed in order to protect the legal interests of the relevant company and the data owner.	Identity information, contact information and professional, educational information etc. about the children and spouses of the personal data owner
Customer information	Information belonging to customers who benefit from our products and services, clearly belonging to an identified or identifiable natural person and included in the data recording system.	Customer no, profession, etc.
Customer Transaction Information	Information regarding all kinds of transactions carried out by customers who benefit from our products and services, which are clearly belonging to an identified or identifiable natural person and are included in the data recording system.	Request and instructions, order and cart information, etc.
Physical Space Security Information	Information of the physical space at the entrance to the physical space, which is clearly belonging to an identified or identifiable natural person and is included in the data recording system.	Entry and exit logs, visit information, camera recordings, etc.
Transaction Security Information	Personal data clearly belonging to an identified or identifiable natural person and included in the data recording system, processed in order to ensure the technical, administrative, legal and commercial security of our Company and related parties	Information showing that the person is authorized to match the transaction associated with the personal data owner and to perform that transaction (eg, website password and password information)
Risk Management Information	Personal data clearly belonging to an identified or identifiable natural person and included in the data recording system, processed in order to manage the commercial, technical and administrative risks of our Company	IP address, Mac ID etc. records

Data Category	Personal Data Disclosure	Types of Personal Data Included in Relevant Personal Data
Financial Information	Personal data within the scope of information, documents and records that clearly belong to an identified or identifiable natural person and are included in the data recording system, showing all kinds of financial results created according to the type of legal relationship with the personal data owner.	Information showing the financial result of the transactions made by the data owner, credit card debt, loan amount, loan payments, interest amount and rate payable, debt balance, receivable balance, etc.
Personal Information	Personal data that is clearly belonging to an identified or identifiable natural person and is included in the data recording system, which forms the basis of the personal rights of the employees.	All kinds of information and documents that are legally required to be entered in the personnel file (eg salary amount, SSI premiums, payrolls, etc.)
Worker Candidate Information	Personal data used in the application evaluation process, belonging to data owners who share their information in order to apply for a job with our Company, which are clearly belonging to an identified or identifiable natural person and are included in the data recording system.	Curriculum vitae, interview notes, personality test results, etc.
Employee Process Information	Personal data related to all kinds of transactions carried out by employees or work, which are clearly belonging to an identified or identifiable natural person and are included in the data recording system.	Job entry-exit records, business trips, information about meetings attended, security inquiries, e-mail traffic monitoring information, vehicle usage information, company credit card spending information, etc.
Employee Performance and Career Development Information	Personal data clearly belonging to an identified or identifiable natural person and included in the data recording system, processed for the purpose of measuring the performance of employees and planning and carrying out their career development within the scope of human resources policies	Performance evaluation reports, interview results, career development trainings etc.
Benefits and Benefits Information	Personal data that is clearly belonging to an identified or identifiable natural person and is included in the data recording system, processed for the purpose of planning fringe benefits and benefits offered to employees and for employees to benefit from them.	Private health insurance, vehicle allocation, etc.
Marketing Information	Data that are clearly belonging to an identified or identifiable natural person and included in the data recording system, to be used by our Company in marketing activities	Reports and evaluations showing the habits and tastes of the person collected for marketing purposes , targeting information, cookie records, data enrichment activities, etc.
Legal Action and Compliance Information	Personal data clearly belonging to an identified or identifiable natural person and included in the data recording system, processed for the purpose of determining and monitoring legal receivables and rights, and fulfilling debts and legal obligations	Data contained in documents such as court and administrative authority decisions
Audit and Inspection Information	Personal data clearly belonging to an identified or identifiable natural person and included in the data recording system, processed within the scope of compliance with our Company's legal obligations and company policies	Audit and inspection reports, related interview records and similar records

Data Category	Personal Data Disclosure	Relating to Into Personal Data entering Personal Data Types
Special Qualified Personal Data	Race, ethnic origin, political thought, philosophical belief, religion, sect or other belief, dress and dress, membership of an association, foundation or trade union, which are clearly belonging to an identified or identifiable natural person and included in the data recording system, blood type, health, sexual life, criminal conviction and security measures, and biometric and genetic data	Race, ethnicity, political thought, philosophical belief, religion, sect or other belief, dress and dress, association, foundation or union membership information, health and sexual life data, criminal conviction and security measures, biometric data, genetic data
Request / Complaint Management information	Any and all information directed to our Company, which clearly belongs to an identified or identifiable natural person and is included in the data recording system. Personal data regarding the receipt and evaluation of any request or complaint	All kinds of requests and complaints against companies, related records and reports
Reputation Management Information	Personal data clearly belonging to an identified or identifiable natural person and included in the data recording system, which may affect the reputation of our Company's shareholders, employees, business partners or customers	Personal data etc. in negative news about the company on social media
Visual and Audio Data	Visual and audio recordings that are clearly belonging to an identified or identifiable natural person and are included in the data recording system and associated with the personal data owner.	Photos, video recordings and audio recordings

Data Categories

LEGAL BASIS AND PURPOSE OF PROCESSING PERSONAL DATA LEGAL BASIS OF PROCESSING PERSONAL DATA

General Principles: Although the legal bases for the processing of personal data by our company differ, we act in accordance with the general principles in Article 4 of the Law No. 6698 in all kinds of personal data processing activities. According to this; in any data processing

- Compliance with the law and the rules of honesty,
- Being accurate and up-to-date when necessary,
- Processing for specific, explicit and legitimate purposes,
- Being connected, limited and restrained with the purpose for which they are processed,
- The general principles of storage for the period required for the purpose for which they are processed or stipulated in the relevant legislation are taken into account.

Reasons for Compliance with Law

Finding the Explicit Consent of the Personal Data Owner

One of the conditions for the processing of personal data is the explicit consent of the owner. The explicit consent of the personal data owner should be disclosed on a specific subject, based on information and free will.

Explicitly Provided in Laws

The personal data of the data owner can be processed in accordance with the law, if it is expressly stipulated in the law. *For example, reporting the identities of our Employees to the competent authorities in accordance with the Identity Reporting Legislation.*

Failure to Obtain the Explicit Consent of the Person Related to the Cause of Actual Impossibility

The personal data of the data owner may be processed if it is necessary to process the personal data of the person who is unable to express his or her consent due to actual impossibility, or whose consent cannot be validated, in order to protect the life or physical integrity of himself or another person. *For example, sharing the blood group information of the unconscious employee with the physician.*

Direct Concern with the Establishment or Performance of the Contract

It is possible to process personal data if 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 a contract. *For example, obtaining a CV from the candidate for the establishment of an employment contract, obtaining an address for notification within the scope of the contract.*

Fulfilling the Company's Legal Obligation

Personal data of the data subject may be processed if the processing is necessary for our company to fulfill its legal obligations as a data controller. *For example, processing family information to benefit the Employee from the Minimum Living Allowance.*

Making Personal Data Public by Personal Data Owner

If the data owner has made his personal data public by himself, the relevant personal data may be processed. For example, if the customers of our Company present their complaints, requests or suggestions on a public platform on the internet, these customers will make their relevant information public. In this case, it is possible to process the data, limited to the purpose of responding to complaints, requests or suggestions, by the representative of our Company.

Mandatory Data Processing for the Establishment or Protection of a Right

If data processing is necessary for the establishment, exercise or protection of a right, the personal data of the data owner may be processed. *For example, the storage of evidential data and its use when necessary.*

Obligatory Data Processing for the Legitimate Interest of Our Company

Provided that it does not harm the fundamental rights and freedoms of the personal data owner, the personal data of the data owner may be processed if data processing is necessary for the legitimate interests of our Company. *For example, monitoring critical points with a security camera against theft or for occupational safety.*

Processing of Private Personal Data and Reasons for Compliance with Law

Special categories of personal data can be processed by our company only in cases stipulated by the laws, provided that adequate measures to be determined by the Personal Data Protection Board are taken, if the personal data owner does not have the express consent.

Persons or authorized institutions and organizations that are under the obligation to keep confidential, only for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing. can be processed by

Regardless of the reason, general data processing principles are always taken into account in the processing processes and compliance with these principles is ensured.

PURPOSE OF PROCESSING PERSONAL DATA

Our company processes personal data limited to the purposes and conditions specified in the personal data processing conditions specified in the 2nd paragraph of Article 5 of the Law on the Protection of Personal Data No. 6698 and the paragraph of the 6th Article.

In the data processing process, the above-mentioned legal bases are taken into account, and if there are no other legal compliance reasons, the consent of the person concerned is requested. Here, too, general principles control is carried out within the scope of Article 4, and above all, it is sought that the data processing activity is generally compatible with the principles of legality.

The consent of the person concerned is obtained "in an open, informed and free will" manner.

The purposes of processing personal data are also stated in the "Personal Data Inventory" of our Company. Personal data is processed in the units of our company, especially for the following purposes.

In order to fulfill the mutual obligations arising from the employment contract as the employer, the personal data of the employees must be processed. Personal data of employees; in accordance with the law and the rules of honesty, accurate and up-to-date when necessary; for specific, explicit and legitimate purposes; It is processed and stored in a limited and measured way in connection with the purpose. In this context, in line with the purposes necessary for the employees to be employed in accordance with the law, the establishment, performance and termination of the employment contract should be carried out in accordance with the law, provided that it is not contrary to fundamental rights and freedoms, the legitimate interests of the Company, the situations clearly envisaged in the law, the legal conditions related to employee employment.

In cases where data processing is obligatory for the fulfillment of obligations, establishment, use and protection of the right in legal proceedings, and in cases other than these, the explicit, informed consent that will be requested from the employees and that the employees will declare with their free will constitute the legal basis of personal data processing.

Within the scope of the activities required by the company's field of activity, the legitimate interests of the employer require the processing of personal data of the employees. As a matter of fact, it is possible to process personal data of employees for reasons such as preventing abuse, preventing theft, ensuring general safety or occupational health and safety. However, in this case, great care is taken not to harm the fundamental rights and freedoms of the employees. The majority of the personal data of the employees being processed is obtained from the information given to the Company by the employees. Again, in some cases, personal data of employees may come to the Company from internal sources such as Company managers or from the references of employees or from data in systems established by public institutions and organizations due to work life requirements.

Personal data of employees being processed, application forms and references of employees, employment contracts and changes, employee contact information, information required for payroll, family or close information such as people to be contacted in case of emergency, employee training records, performance evaluation records, disciplinary records, camera information such as records.

There are rules in many Company policies and procedures regarding the processing of personal information of employees. It is implemented by the Human Resources unit. Employee health information is also among the personal data processed. As a rule, information regarding the health and sexual lives of employees is processed by persons or authorized institutions and organizations under the obligation of keeping confidentiality, for the purpose of protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing. In this context, the health data of the employees and the details about them are available at the workplace doctor and the health unit as a rule. In the event that the employee becomes a member of a union after the status of "employee" (which is not requested in the employee candidacy category), union membership can also be processed in accordance with the clear provisions of the law in order to fulfill the requirements of the legal legislation. Apart from this, race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, costume and clothing, and biometric and genetic data of employees are not included in the processed personal data as a rule, unless clearly stipulated in the law. , requirements are carefully evaluated before personal data is processed. The company controls and supervises information and communication tools (telephone, mobile phones, computers and internet). Law No. 5651 and the legitimate interests of our Company constitute the legal basis of these practices. Vehicle tracking system can be applied in our company's vehicles for the reasons of "security, more effective management of vehicles and personnel". The said activity is based on the legitimate interests of our company and is carried out on the condition that it does not harm the fundamental rights and freedoms of the employees. In line with the aim of ensuring the execution of our company's human resources policies; Recruitment of suitable personnel for vacant positions in accordance with our company's human resources policies, execution of human resources operations in accordance with our company's human resources policies, selection of employee candidates, management of personnel affairs, determination of

training and career plans, fulfillment of obligations within the framework of occupational health and safety and taking necessary measures. constitutes the purposes of processing the data.

Personal data of supplier/subcontractor employees can also be processed by our company. As a matter of fact, in the Law No. 6331, the documents and information that should be checked regarding the employees coming from another workplace regarding occupational health and safety have been specified to the main employer. Likewise, in the Labor Law No. 4857 and the Social Insurance and General Health Insurance Law No. 5510, obligations regarding sub-employer workers and temporary workers have been introduced to the main employer, and the issues to be controlled within this scope have been specified. Accordingly, the processing of the personal data of the workers working in our workplace depending on the supplier and other employer is based on the legitimate interests of our business, especially the legal amendments in question.

Personal data of people who buy products or services can also be processed by our company. The data processing activity in question is based on the legitimate interests of our company, on the grounds of both the Law of Flat Owners and the management of the service provided more effectively, provided that the customers / service areas are not provided. It includes profile management, sales, advertising, marketing activities of customers/service users, carrying out integrated facility management within the scope of our company's field of activity, maintaining activities in project areas, maintaining contractual activities related to flat owners and tenants (collection of dues, reporting of fees collected, legal proceedings, independent Data processing activities can be carried out in order to ensure the security in the project areas and to fulfill the obligations arising from the law.

Personal data also;

- Execution of emergency management processes
- Execution of information security processes
- Conducting audit/ethics activities
- Conducting educational activities
- Execution of access authorizations
- Execution of activities in accordance with the legislation
- Execution of finance and accounting works
- Execution of company/product/service loyalty processes
- Ensuring physical space security
- Execution of assignment processes
- Follow-up and execution of legal affairs
- Carrying out internal audit/investigation/intelligence activities

- Conducting communication activities
- Execution of goods/services/production and operation processes
- Execution of customer relations processes
- Carrying out activities for customer satisfaction
- Organization and event management
- Execution of marketing analysis studies
- Execution of performance evaluation processes
- Execution of advertisement/campaign/promotion processes
- Execution of risk management processes
- Execution of storage and archiving activities
- Execution of contract processes
- Execution of strategic planning activities
- Follow-up of requests / complaints
- Ensuring the security of movable property and resources
- Execution of supply chain management processes
- Execution of marketing processes of products/services
- Ensuring the security of data controller operations
- Foreign personnel work and residence permit procedures
- Execution of investment processes
- Providing information to authorized persons, institutions and organizations
- Execution of management activities
- It is processed in our Relevant Units for the purpose of creating and tracking visitor records.

For the purposes of occupational health and safety, general security, product safety, camera monitoring at the workplace is carried out by taking into account the legitimate interests of the Company, provided that it does not harm the fundamental rights and freedoms of our visitors, the persons whose data is processed in this context, and especially the employees.

STORAGE, DELETING, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

Although our company has been processed in accordance with the provisions of the relevant law as regulated in article 138 of the Turkish Penal Code and article 7 of the KVKK Law, personal data is deleted, destroyed, or upon the request of the personal data owner, upon our company's own decision or upon the request of the personal data owner, in case the reasons requiring processing are eliminated. is made anonymous.

STORAGE AND STORAGE PERIOD OF PERSONAL DATA

Our company keeps personal data for the period specified in the relevant legislation, if it is stipulated in the relevant laws and legislation. If the legislation regarding how long the personal data should be kept is not regulated for a period of time, the personal data is processed for the period that requires it to be processed in accordance with the practices of our Company and the practices of the commercial life depending on the services provided by our company while processing that data, then it is deleted, destroyed or anonymized. If the purpose of processing personal data has ended and the storage periods determined by the relevant legislation and the company have come to an end; Personal data can only be stored to provide evidence in possible legal disputes or to assert the right related to personal data or to establish a defense. Although the statute of limitations and the statute of limitations for the right to assert the aforementioned right in the establishment of the periods herein have expired, the retention periods are determined on the basis of the examples in the previous requests made to our Company on the same issues. In this case, the stored personal data is not accessed for any other purpose, and only when necessary to use it in the relevant legal dispute, access to the relevant personal data is provided. Here, too, personal data is deleted, destroyed or anonymized after the aforementioned period expires. In this context;

Deletion of Personal Data

Deletion of Personal Data

Even though it has been processed in accordance with the provisions of the relevant law, our company may delete personal data upon its own decision or upon the request of the personal data owner, in the event that the reasons requiring processing are eliminated. Deletion of personal data is the process of making personal data inaccessible and non-reusable for relevant users. All necessary technical and administrative measures are taken by our company to make the deleted personal data inaccessible and reusable for the relevant users.

Deletion Process of Personal Data

The process to be followed in the deletion of personal data is as follows:

- Determining the personal data that will be the subject of the deletion process.
- Identifying relevant users for each personal data using an access authorization and control matrix or a similar system.
- Determining the authorizations and methods of the relevant users such as access, retrieval and reuse.

- Closing and eliminating the access, retrieval, reuse authorization and methods of the relevant users within the scope of personal data.

Methods of Deletion of Personal Data Since personal data can be stored in various recording media, they are deleted by methods suitable for recording media.

Destruction of Personal Data

Destruction of Personal Data

Even though it has been processed in accordance with the provisions of the relevant law, our company may destroy personal data at its own discretion or upon the request of the personal data owner, in the event that the reasons for processing are eliminated. Destruction of personal data is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way. Our company takes all necessary technical and administrative measures regarding the destruction of personal data.

Personal Data Destruction Methods

In order to destroy personal data, all copies of the data are detected and the systems with the data are destroyed.

Anonymization of Personal Data

Anonymization of Personal Data

Anonymization of personal data means that personal data cannot be associated with an identified or identifiable natural person under any circumstances, even by matching them with other data. Our company can anonymize personal data when the reasons that require the processing of personal data processed in accordance with the law are eliminated. Personal data is anonymized by making it impossible to associate with an identified or identifiable natural person, even by using appropriate techniques for the recording medium and the relevant field of activity, such as returning it by the data controller or recipient groups and/or matching the data with other data. Our company takes all necessary technical and administrative measures to anonymize personal data. Personal data that has been anonymized in accordance with Article 28 of the KVK Law may be processed for purposes such as research, planning and statistics. Such processing is outside the scope of the Personal Data Protection Law and the explicit consent of the personal data owner will not be sought.

Methods of Anonymization of Personal Data

Anonymization is the removal or alteration of all direct and/or indirect identifiers in a data set, preventing the identification of the data subject from being identified, or losing its distinctiveness in a group or crowd in a way that cannot be associated with a natural person. Data that does not point to a specific person as a result of blocking or losing these features is considered anonymized data. The purpose of anonymization is to break the link between the data and the person identified by this data. All of the bond breaking processes carried out by methods such as automatic or non-automatic grouping, masking, derivation, generalization, randomization applied to the records in the data recording system where personal data is kept are called anonymization methods. The data obtained as a result of the application of these methods should not be able to identify a specific person.

COOKIES AND SIMILAR TECHNOLOGIES

While accessing our company's websites, electronic platforms, applications or e-mail messages or advertisements sent by the Company, small data files can be placed on users' computers, mobile phones, tablets or other devices used to record and collect certain data. These data files placed on computers and other devices may be cookies, pixel tags, flashcookies and web beacons, as well as other technologies for data storage purposes.

In this Policy, the term "cookie" is used to express cookies and similar technologies that can be used by the Company. Although it is possible to collect personal data through cookies, any data collected through cookies may not be considered personal data. For this reason, it should be taken into account that the data obtained through cookies will only be considered within the scope of this Policy and Personal Data Protection Law to the extent that they constitute personal data within the framework of Turkish law.

TYPES OF COOKIES

Cookies can be classified in terms of duration or according to the domain name they belong to. Cookies are divided into two as session cookies and permanent cookies if they are classified in terms of duration. Session cookies refer to cookies that are deleted when the user closes the browser, while Persistent cookies are cookies that remain on the user's computer/device for a predetermined period of time. If the cookies are classified according to the domain name they belong to, they are divided into two as Related party cookies and Third party cookies. Cookies placed by the visited domain are called related party cookies, while cookies placed by a different domain visited are referred to as third party cookies. In the event that people outside the visited area place a cookie on the user's device through the visited area, a third party cookie is in question.

INTENDED USE OF COOKIES

The Company may benefit from the cookies it uses on its websites, platforms, applications, advertisements and messages for the following purposes.

Operational uses: We may use cookies that we deem necessary for the administration and security of the company's website, platform, applications and services. Examples of cookies used for operational purposes are technologies that allow the use of functions on websites, applications and platforms, and cookies used to detect irregular behavior in these channels.

Uses for functionality: The company may use cookies to facilitate the use of its website, platform, applications and services and to customize them for users. Technologies that enable us to remember user information and preferences are examples of cookies used for functionality.

Performance-oriented uses: The company may also use cookies to increase and measure the performance of its website, application, platform and services. Examples of cookies used for this purpose are technologies that allow us to understand how users use the Company's website, applications, platforms and services, and to analyze user behavior, and to understand whether the messages we send are interacted with.

Uses for advertising purposes: We may use related party cookies and third party cookies for the purpose of transmitting advertisements and similar content for the interests of users through the

websites, platforms and applications of the Company or third parties. Examples of uses for advertising purposes are cookies that measure the effectiveness of ads, and cookies that show whether a particular ad has been clicked or how many times the ad has been viewed.

REJECTING AND DELETING COOKIES

Although most browsers allow the use of cookies, users can refuse or delete cookies at any time by changing their browser settings. The method of changing the settings varies according to the browser used, and how to disable cookies should be learned from the service provider for the browser used. If cookies are disabled, some features of the Company's website, application, platform and services may not be available.

AUTHORIZED SERVICE PROVIDERS

We may obtain assistance from some of the service providers we have authorized to operate and promote the company's website, platform and applications, and services. These service providers will be able to place cookies and similar technologies (third party cookies) on users' computers/devices and collect information such as IP address, unique identifier and device identifier to identify the user's device.

THIRD PARTY SITE, PRODUCTS AND SERVICES

Company websites, platforms and applications may contain links to third party websites, products and services. The links in question are subject to the privacy policies of third parties, and it should be noted that third parties and websites belonging to third parties are independent of the Company and the Company is not responsible for the privacy practices of third parties. In case of visiting the linked websites, we recommend that you read the privacy policies of these websites.

THE RIGHTS OF RELATED PERSONS THE SCOPE OF THE RIGHTS OF RELATED PERSONS AND THE USE OF THESE RIGHTS

Rights of Relevant Persons

Persons whose personal data are processed by our company have the following rights:

- Learning whether personal data is processed or not,
- If personal data has been processed, requesting information about it,
- Learning the purpose of processing personal data and whether they are used in accordance with its purpose,
- Knowing the third parties to whom personal data is transferred at home or abroad,
- Requesting correction of personal data in case of incomplete or incorrect processing and requesting notification of the transaction made within this scope to the third parties to whom the personal data has been transferred,
- Requesting the deletion or destruction of personal data in the event that the reasons requiring its processing have disappeared, although it has been processed in accordance with the

provisions of the KVK Law and other relevant laws, and requesting that the transaction carried out within this scope be notified to the third parties to whom the personal data has been transferred,

- Objecting to the emergence of a result against the person himself by analyzing the processed data exclusively through automated systems,
- To request the compensation of the damage in case of loss due to unlawful processing of personal data.

Relevant Persons' Exercise of Their Rights

Relevant Persons are required to submit their requests regarding the exercise of the above-mentioned rights in accordance with paragraph 1 of Article 13 of the KVK Law to our company through the application form on our website and the methods shown there. Name-Surname and signature if the application is written, TR Identity Number for Turkish citizens, nationality, passport number or identification number, if any, place of residence or workplace address for notification, e-mail address, telephone and fax number, subject of request, if any, subject to notification, must be present. Information and documents related to the subject are added to the application. It is not possible to make a request by third parties on behalf of personal data owners. In order for a person other than the personal data owner to make a request, there must be a special power of attorney issued by the personal data owner on behalf of the person to apply. In the application containing your explanations regarding the right you have as the personal data owner and you will make and request to use the above-mentioned rights; The subject you request must be clear and understandable, the subject you request is related to yourself or if you are acting on behalf of someone else, you must be specifically authorized in this regard and document your authority, the application must contain your identity and address information, and documents confirming your identity must be attached to the application. The application form for the data owners is available at the websites of our Company at mavimor.com.tr and vino.com.tr.

Responding to Applications

If the personal data owner submits his request to our Company in accordance with the prescribed procedure, our Company will conclude the relevant request free of charge as soon as possible and within thirty days at the latest, depending on the nature of the request. However, if the transaction requires a separate cost, our Company will charge the applicant the fee in the tariff determined by the KVK Board. Our company may request information from the person concerned in order to determine whether the applicant is the owner of personal data. Our company may ask questions about the personal data owner's application in order to clarify the issues in the personal data owner's application.

ENSURING THE SECURITY OF PERSONAL DATA TECHNICAL AND ADMINISTRATIVE MEASURES TO ENSURE THE LEGAL PROCESSING OF PERSONAL DATA

Our company takes all necessary technical and administrative measures to ensure that personal data is processed in accordance with the law. In this context, a Data Inventory compatible with the VERBIS system is issued within the scope of our Company, and compliance with the law and purpose audits are carried out here.

"Clarification Texts" have been prepared for each relevant person group so that our company can fully and correctly fulfill the lighting obligation of the relevant persons.

Employees are informed about the law on the protection of personal data and the processing of personal data in accordance with the law.

All activities carried out by our company are analyzed in detail specific to all business units, and as a result of this analysis, personal data processing activities are revealed, specific to the activities carried out by the relevant business units.

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 personal data processing conditions sought by the Law No. 6698 are determined by each business unit and the detail activity it carries out.

Contracts and documents governing the legal relationship between our Company and employees, except for the Company's instructions and the exceptions brought by the law, include records that impose the obligation not to process, disclose or use personal data, raise awareness of employees and carry out audits.

Agreements and documents governing the legal relationship between our Company and the third parties that process the data for which our Company is responsible, except for the Company's instructions and the exceptions made by law, are subject to the obligation not to process, disclose or use personal data. Additional Confidentiality protocols are signed.

TECHNICAL AND ADMINISTRATIVE MEASURES TAKEN IN PROCESSING SPECIAL QUALITY DATA

With the Personal Data Protection Law, special importance has been attached to certain personal data due to the risk of causing victimization or discrimination when processed unlawfully. These data are; data related to race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, dress and clothing, membership to associations, foundations or trade unions, blood type, health, sexual life, criminal convictions and security measures, and biometric and genetic data. . Our company acts sensitively in the protection of special quality personal data, which is determined as "special quality" by the KVK Law and processed in accordance with the law. In this context, the technical and administrative measures taken by our Company for the protection of personal data are meticulously implemented in terms of special quality personal data and necessary audits are provided.

For employees involved in the processing of sensitive personal data, regular trainings are provided on the Law and related regulations, as well as on sensitive personal data security, confidentiality agreements are made, the scope and duration of authorization of users who have access to data are clearly defined, and authorization controls are carried out, The authorizations of employees who have a change of job or quit their job in this field are immediately revoked and the inventory allocated to them by the data controller is returned.

In case the data is accessed through a software, user authorizations for this software are made, the security tests of these software are carried out regularly, and the test results are recorded. If remote access to data is required, at least two-stage authentication system is provided.

If the physical environment where sensitive personal data is processed, stored and/or accessed, adequate security measures (against electrical leakage, fire, flood, theft, etc.) Unauthorized entries and exits are prevented.

If sensitive personal data is to be transferred, if the data needs to be transferred via e-mail, it is provided to be transferred with an encrypted corporate e-mail address or by using a Registered Electronic Mail (KEP) account. If private data is transferred between servers in different physical environments, data transfer is carried out by establishing a VPN or FTP method between servers. If private data needs to be transferred via paper media, necessary precautions are taken against risks such as theft, loss or viewing of the document by unauthorized persons, and the document is sent in the form of "confidential documents".

TECHNICAL AND ADMINISTRATIVE MEASURES TO PREVENT ILLEGAL ACCESS OF PERSONAL DATA

Our company takes technical and administrative measures to prevent the imprudent or unauthorized disclosure, access, transfer or any other unlawful access to personal data. Technical Measures Taken to Prevent Unlawful Access to Personal Data The main technical measures taken by our company to prevent unlawful access to personal data are listed below:

- ***Ensuring Cyber Security*** Cyber security products are primarily used to ensure personal data security, but the measures are not limited to this. Measures such as firewall and gateway are taken. Unused software and services are removed from devices. Cyber Attack Policy and Network Management Policy are implemented

- ***Software updates*** With patch management and software updates, it is ensured that the software and hardware work properly and that the security measures taken for the systems are checked regularly. Change management policy is implemented

- ***Access Restrictions*** Access to systems containing personal data is also restricted. In this context, employees are granted access to the extent necessary for their job and duty authorities and responsibilities, and access to the relevant systems is provided by using a user name and password. While creating the aforementioned passwords and passwords, it is ensured that combinations of upper and lower case letters, numbers and symbols are preferred instead of numbers or letter sequences associated with personal information that can be easily guessed. Accordingly, an access authorization and control matrix is created. Access is made in accordance with the authorization policy and the Network Access policy.

- ***Encryption*** In addition to the use of strong passwords and passwords, limiting the number of password attempts, ensuring that passwords and passwords are changed at regular intervals, opening the administrator account and administrative authority for use only when necessary, and deleting the account or closing the logins without wasting time for employees who have been dismissed from the data controller. access is restricted by such methods. In this context, Password Security Policy is implemented.

- ***Anti-Virus Software*** In order to be protected from malicious software, products such as anti-virus and antispam are used, which regularly scan the information system network and detect dangers. Moreover, these are kept up-to-date and the necessary files are scanned regularly. If personal data is to be obtained from different Internet sites and/or mobile application channels,

connections are made via SSL or a more secure way. Antivirus policy and Anti-Malware policy are implemented.

- ***Internet Access Authorization*** Improper use of the Internet may cause undesirable consequences in terms of legal obligations, capacity utilization and corporate image of the institution. Internet Access Policy is implemented in order not to cause such negativities intentionally or unintentionally and to ensure that the internet is used in accordance with the rules, ethics and laws.

- ***Monitoring Personal Data Security***

    1. Checking which software and services are running in information networks,
    2. Determining whether there is an infiltration or an action that should not be in the information networks, Keeping the transaction records of all users regularly (such as log records)
    3. Reporting security issues as quickly as possible,
    4. Incident violation procedure is established for employees to report security vulnerabilities in systems and services or threats using them.

Evidence is collected and securely stored in undesirable events such as the crash of the information system, malicious software, denial-of-service attack, incomplete or incorrect data entry, violations of confidentiality and integrity, abuse of the information system.

Ensuring the Security of Environments Containing Personal Data

If personal data is stored on devices located in the campuses of data controllers or on paper media, physical security measures are taken against threats such as theft or loss of these devices and papers. Applications by our company are made in accordance with the Physical Environment Security policy.

If personal data is in electronic media, access can be restricted or separated between network components in order to prevent personal data security breach. Access Authorization policy is implemented.

The same level of precautions are also taken for paper media, electronic media and devices (laptop, mobile phone, flash memory) located outside the Company campus and containing personal data belonging to the Company . Personal data to be transferred to e-mail is sent carefully and by taking adequate precautions. E-Mail Policy is implemented in our company.

In case of loss or theft of devices containing personal data, access control authorization and/or encryption methods are used. In this context, the encryption key is stored in an environment that only authorized persons can access, and unauthorized access is prevented.

Documents in paper media containing personal data are stored in a locked way and in environments that can only be accessed by authorized persons, and unauthorized access to these documents is prevented. In addition, a clean desk and clean screen policy is applied in work areas that contain personal data.

Storage of Personal Data in the Cloud

Applications for storing personal data in the cloud can also be applied when necessary. In this case, the Company should evaluate whether the security measures taken by the cloud storage service provider are sufficient and appropriate. In this context, the measures specified in the guidelines and recommendations of the KVK Board are taken into account.

Information Technology Systems Procurement, Development and Maintenance

Security requirements are taken into account when determining the needs for the supply, development or improvement of existing systems by the company.

Backing Up Personal Data

In cases where personal data is damaged, destroyed, stolen or lost for any reason, the Company uses the backed up data to take action as soon as possible. Backed up personal data can only be accessed by the system administrator, and data set backups are kept out of the network.

Administrative Measures Taken to Prevent Unlawful Access to Personal Data

The main administrative measures taken by our company to prevent unlawful access to personal data are listed below:

- Employees are informed and trained about the technical measures to be taken to prevent unlawful access to personal data.
- Employees are informed that they cannot disclose the personal data they have learned to others in violation of the provisions of the KVK Law and cannot be used for purposes other than processing, and that this obligation will continue after they leave their job, and necessary commitments are taken from them in this direction.
- Personal Data Security Policies and Procedures are determined, within the scope of policies and procedures; controls are carried out on a regular basis, the controls are documented, and the issues that need improvement are determined. Again, risks that may arise for each category of personal data and how security breaches will be managed are also clearly defined.

Reducing Personal Data as Much as Possible

Personal data must be accurate and up-to-date, and must be kept for the period required by the relevant legislation or for the purpose for which they are processed. However, inaccurate, outdated

still a need for data that has been lost and does not serve any purpose, and personal data that is not needed is deleted, destroyed or anonymized with the personal data retention and destruction policy.

Management of Relations with Data Processors:

When the company receives services from data processors to meet its IT needs, when receiving services, transactions are made by making sure that the security level provided by the data

processors is at least provided by them. In this context, protective regulations regarding personal data are introduced into the contracts signed with the data processor .

STORING PERSONAL DATA IN SAFE ENVIRONMENTS

Our company takes the necessary technical and administrative measures according to the technological possibilities and implementation cost in order to store personal data in secure environments and to prevent their destruction, loss or alteration for unlawful purposes.

Technical Measures Taken for Storing Personal Data in Secure Environments

The main technical measures taken by our company to store personal data in secure environments are listed below:

1. Systems suitable for technological developments are used to store personal data in secure environments.
2. Technical security systems are established for the hiding places, the technical measures taken are periodically audited by the audit mechanism determined by our Company, the risky issues are re-evaluated and the necessary technological solution is produced.
3. All necessary infrastructures are used in accordance with the law to ensure that personal data is stored securely.

Administrative Measures to Keep Personal Data in Secure Environments

The main administrative measures taken by our company to store personal data in secure environments are listed below:

1. Employees are informed about ensuring that personal data is kept securely.
2. In the event that an external service is received by our company due to technical requirements regarding the storage of personal data, the contracts concluded with the relevant companies to which the personal data is transferred in accordance with the law; Provisions are included that the persons to whom personal data are transferred will take the necessary security measures for the protection of personal data and that these measures will be complied with in their own organizations.

EDUCATION

Our company provides its employees with the necessary training on the protection of Personal Data within the scope of the Policy and procedures within the scope of KVKK Regulations.

If the employee of our Company accesses Personal Data physically or on a computer, the relevant employee of our Company is given training on Information security policies for these accesses.

In addition, Orientation Trainings are provided in the recruitment processes.

AUDIT

Increasing Awareness and Supervision of Business Units on the Protection and Processing of Personal Data

Our company ensures that the necessary notifications are made to the business units in order to prevent the unlawful processing of personal data, to prevent illegal access to the data, and to raise awareness about data protection.

Increasing Awareness and Supervision of Business Partners and Suppliers on the Protection and Processing of Personal Data

In order to prevent the illegal processing of personal data, to prevent illegal access to data, and to increase awareness regarding data protection, our company is required to inform its business partners in accordance with the Clarification obligations. In addition, confidentiality commitments are taken in the contracts.

VIOLATIONS

Each employee of the company informs the relevant Contact person about the work, transaction or action that he or she considers to be contrary to the procedures and principles set forth in the KVKK Regulations and within the scope of this Policy. contact person,

The Incident takes action within the scope of the Incident violation procedure, according to the content of the violation. As a result of the notifications, the Contact Person prepares the notification to be made to the Authority regarding the violation, taking into account the provisions of the applicable legislation on the subject, especially the KVKK Regulations. And handles correspondence and communication.

RESPONSIBILITIES

Responsibilities within the company are respectively employee, department, contact person who is Data Officer Representative. In this context; The Contact Person responsible for the implementation of the policy is appointed by the company's board of directors with the decision of the board of directors, and changes in this context are also made in the aforementioned way.

CHANGES TO THE POLICY

This Policy may be changed by the Company from time to time with the approval of the Board of Directors. The Company shares the updated Policy text with its employees via e-mail so that the changes it has made on the Policy can be reviewed, or makes it available to the employees and Data Subjects via the web address below.

Related web addresses: mavimor.com.tr and vvino.com.tr

EFFECTIVE DATE OF THE POLICY This version of the Personal Data Protection and Processing Policy was approved by the Company's Board of Directors on 10.09.2021 and entered into force.