Personal Data Processing and Protection Policy

1- Objective

This Personal Data Processing and Protection Policy ("Policy") regulates the principles that our company has specified in order to ensure compliance with the applicable legislation regarding personal data processing activities and protection and destruction of this data.

2- Definitions

Terms beginning with a capital letter used in this Policy and not defined in the Policy will have the meanings ascribed below.

Explicit Consent	It expresses the informed consent on a particular subject, expressed with free will.
Anonymization	It refers to the process of making Personal Data unrelated to a certain or identifiable natural person, which cannot be associated under any circumstances even by matching with other data.
Secondary Legislation	Any regulation, circular, communiqué, principle decision or similar administrative decision or general opinion issued or taken by the Personal Data Protection Authority under the law.
Related Users	It refers to the persons who process personal data within the organization of the Data Controller or in accordance with the authorization and instruction received from the Data Controller except the person or unit responsible for the technical storage, protection and backup of the data.
Law	Refers to the Law No. 6698 on the Protection of Personal Data.
Personal Data	It refers to all kinds of information about a specific or identifiable natural person.
Processing of Personal Data	It refers to any operation performed on data such as obtaining, recording, storing, preserving, modifying, reorganizing, disclosing, transferring, taking over, making available, classifying or preventing its use by non-automated means provided that Personal Data is a part of a fully or partially automated data recording system or any data recording system
Board	Refers to the Personal Data Protection Board.
Authority	Refers to the Personal Data Protection Authority.
Sensitive Personal Data	Biometric and genetic data about people's race, ethnic origin, political thought, philosophical belief, religion, sect or other beliefs, disguise and outfit, association, foundation or union membership, health, sexual life, data related to criminal conviction and security measures, and biometric and genetic data.
Registry	It refers to Data Controllers Registry, which is a recording system in which data officers have to register and declare information about data processing activities.
Deletion	It refers to making personal data inaccessible and unusable for Related Users in any way.
Deletion and Destruction Policy	It refers to the policy that the Company has prepared, within the framework of the Regulation on the Deletion, Destruction or Anonymization of Personal Data, which regulates the procedures and principles regarding deletion and destruction.
Company	It refers to KOCHENDÖRFER HYDRO ELEKTROMEKANİK SAN. ve TİC. A.Ş..
Data Processor	It refers to the natural or legal person who processes Personal Data on behalf of the Data Controller, based on the authority granted by him/her.
Data Protection Commission	It refers to the Company's Personal Data Protection Commission.

Data Owner	Data Owner, defined as "Relevant Person" in the Law, refers to the natural person whose Personal Data is processed. Data Owners include customers, internet users, individuals in the communication, electronic mail and marketing database lists, employees, contracted parties and suppliers.
Data Controller	It refers to the natural or legal person who determines the purposes and means of Personal Data processing and is responsible for the establishment and management of the data recording system.
Draft Regulation on Data Controllers Registry	Draft Regulation on Data Controllers Registry has been prepared in accordance with Article 16 of the Law. It has not come into force yet.
Destruction	It refers to making personal data inaccessible, irreversible and non-reusable by anyone and anyway.

3- Scope

The Company commits to comply with the privacy and security requirements of the Personal Data available under the Law, therefore, the Company has adopted this Policy in order to form the basis of the approach, policies and procedures regarding the protection and processing of Personal Data.

This Policy applies to all full and part-time employees of the Company who have access to the Personal Data collected and processed by the Company, provide information to the Company or receive Personal Data from the Company, subcontractor employees, the employees of the Company's Affiliated Companies, joint venture employees and all suppliers and vendors. In addition, all provisions included in this Policy are subject to the Law and Secondary Legislation. In cases where the provisions of the relevant Law contradict or conflict with the provisions of this Policy, the provisions of the Law will be taken as basis and will be applied.

4- Rules

4.1 Principles to be followed in the Processing of Personal Data

4.1.1 Personal Data are Processed only in accordance with the Law and the Rules of Integrity.

The Company acts in accordance with the law and rules of integrity in the processing of Personal Data. In this context, the Company processes Personal Data in accordance with the rules brought by the Law. In addition, the Company follows the Secondary Legislation that will be published by the Board from time to time and the regulations to be introduced regarding data processing activities and performs/endeavors to perform reorganization and improvements in its applications, if necessary, within the framework of these legal regulations.

4.2.2 Personal Data Should Be Accurate and up-to-date When Necessary.

The company takes the necessary measures to ensure that the Personal Data it processes are accurate and up-to-date when necessary.

4.2.3 Personal Data Should Be Processed for Specific, Explicit and Legitimate Purposes.

The company clearly and precisely determines its data processing purpose and processes Personal Data only for legitimate purposes. This means that the data processed by the Company should be related to and required by the business or service it provides.

The Company explicitly announces these purposes before taking the Personal Data from the Data Owners.

If the Company's Personal Data processing purposes change, this Policy will be updated as necessary. In addition, efforts will be made to announce the changes in data processing purposes to Data Owners through different channels as much as possible.

4.2.5 Personal Data Should Be Kept for the Period Specified in the Relevant Legislation or Required for the Purpose or Processing.

The Company keeps the Personal Data only for the period required for the processing purpose or as specified in the relevant legislation. In this context, if a period is stipulated in the relevant legislation for the storage of Personal Data, the Company keeps the Personal Data limited to these periods.

However, considering that it may be necessary for the Company to keep Personal Data subject to different regulations,

especially the duration of the nonclaim statute, the Company predicate maximum preservation periods on keeping the data, without causing loss of rights for its employees and customers. If a period has not been stipulated in the legislation or there is no legal reason for keeping the data longer, the Company keeps Personal Data for the time required for the purpose for which it was processed.

In addition, the Company complies with the rules and procedures for data preservation specified in the Company Destruction Policy.

4.3 Processing Terms

4.3.1 Processing of Personal Data

Personal Data is processed by the Company based on one or more of the legal processing terms specified in the Law. Our Company processes Personal Data in accordance with the regulations introduced by the Law.

In this context:

4.3.1.1 Personal Data can be processed upon the Explicit Consent of the Data Owner.

4.3.1.2 It is possible to process Personal Data without seeking the Explicit Consent of the Data Owner in case of any of the followings:

1. Explicitly prescribed by law;

2. Is compulsory to protect the person's or anyone else's life or body integrity, for the person who is unable to disclose his/her consent due to actual impossibility or whose consent lacks legal validity;

3. The processing of Personal Data belonging to the parties of the contract is necessary, provided that it is directly related to the establishment or execution of a contract;

4. It is mandatory for the Data Controller to fulfill his/her legal obligation;

5. It is publicized by the Data Owner himself/herself;

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 damage the fundamental rights and freedoms of the Data Owner.

4.3.2 Data Protection Commission

Within the framework of the compliance program of the company, it has been decided to conduct and supervise the personal data processing activities by the Data Protection Commission.

The duties of the Data Protection Commission are as follows:

a) To determine the procedures and standard contractual provisions for the compliance of this Policy with the sellers, suppliers and third parties to whom Personal Data is transferred from the Company, those who have access to the Personal Data collected and processed by the Company and those who provide data to the Company,

b) To specify regular audit mechanisms, procedures and applicable rules to comply with this Policy,

c) To specify, maintain and operate the system that will provide a fast and appropriate response to the requests of the Data Owner when using his/her rights arising from the Law,

d) To ensure that the compliance program of the Company is up to date,

e) To inform the senior executives, administrators and managers of the Company about potential corporate and individual, administrative or criminal liabilities that may be directed against the Company and/or its employees due to violations of the current legislation, and to carry out the necessary actions,

f) To manage and execute the Company's relations with the Authority, the Board and the Registry,

g) To ensure that all necessary records are recorded to the Registry in accordance with the relevant legislation and Board decisions and to supervise the registration procedures,

h) To manage and implement the activities for the implementation of Board decisions.

4.3.3 Processing of Sensitive Personal Data

Personal Data are processed by the Company in accordance with the terms stipulated in the Law. In addition, special measures may be introduced by the Board for the processing of Sensitive Personal Data. If such measures are brought by the Board at any time following the date of the publication of this Policy, the Company will make the necessary arrangements to comply with these measures.

In this context:

4.3.3.1 Sensitive Personal Data can be processed upon the Explicit Consent of the Data Owner

4.3.3.2 Sensitive Personal Data other than the Data Owner's health and sexual life (about race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, disguise and dress, association, foundation or union membership, data related to criminal conviction and security measures and biometric and genetic data) can be processed without seeking the relevant person's Explicit Consent in cases stipulated by law.

4.3.3.3 Personal Data related to health and sexual life, on the other hand, can be processed without seeking Explicit Consent of the owner by the person who has the obligation of keeping confidentiality or authorized institutions and organizations, only for the purpose of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and its financing.

4.3.3.4 The Personal Data of the employees can be processed directly or indirectly in order to carry out the processes especially within the scope of the employer-employee relationship (leave, advance payment, social security process, creation of the personal file, etc.). In such cases, Explicit Consent is obtained from employees and personal data related to health can only be processed and accessed by the people or departments who are required to process this data. These personal data can be processed without explicit consent, in cases specified as the cases that do not require consent within the framework of the current legislation and Authority/Board decision.

4.4 Consent

4.4.1 In order for it to be valid, the consent must be based on information, be explicit and must be disclosed with free will.

4.4.2.1 Data Owner should be informed explicitly and comprehensively in all matters related to processing. This clarification should be understandable by an average individual and easily accessible.

4.4.2.2 Explicit Consent should be understood as a statement of approval clear enough, leaving no room for hesitation and issued limited to that transaction. An open-ended consent cannot be considered an Explicit Consent. As a rule, it is sufficient to take the Explicit Consent of the Data Owner once for different operations to be performed by the Data Controller. However, if the data in question is desired to be processed for purposes other than its original purpose, a separate consent will be required.

4.4.2.3 Explicit Consent should be freely given without any pressure and is valid only if the Data Owner can make a real choice.

4.4.2.4 As long as these conditions are met, the way of taking consent can be specified freely. These can be in the form of provisions on employment contracts, check boxes on application or purchase forms, and boxes on online forms in which Personal Data is entered.

4.4.3 If the consent is acquired by other written statements, the request for consent must be made explicitly.

4.4.4 The Consent can always be withdrawn by the Data Owner.

4.4.5 Data Protection Commission, together with the relevant departments, will establish systems for taking and documenting Data Owner’s Explicit Consent for Personal Data processing.

4.5 Transfer of Personal Data

4.5.1 Transfer of Personal Data to Third Parties

4.5.1.1 Personal Data should not be transferred to another institution, country or region without taking reasonable and appropriate measures according to the required level of data protection.

4.5.1.2 Personal Data may be transferred to third parties only for reasons consistent with their intended purpose or for other purposes permitted by the Law.

4.5.1.3 Necessary security measures should be taken for all Sensitive Personal Data transferred by the Company or should be protected against unauthorized access using encryption to the extent possible.

4.5.1.4 Transfer of Personal Data for third party data processing activities will be subject to written agreements. The Company will develop standard terms and conditions that can be used for this purpose with the Data Protection Commission.

4.5.1.5 Personal Data may be transferred where any of the following applies:

a) Data Owner gives Explicit Consent to that transfer,

b) The transfer is explicitly stipulated by laws,

c) The transfer is compulsory to protect the person’s or anyone else's life or body integrity, for the person who is unable to disclose his/her consent due to actual impossibility or whose consent lacks legal validity

d) The processing of Personal Data belonging to the parties of the contract is necessary, provided that the transfer is directly related to the establishment or execution of the contract;

e) Transfer is mandatory for the Data Controller to fulfill his/her legal obligation

f) The transfer of the data publicized by the Data Owner him/herself;

g) The transfer is mandatory for the establishment, exercise or protection of a right,

h) The transfer is mandatory for the legitimate interests of the Data Controller, provided that it does not damage the fundamental rights and freedoms of the Data Owner.

i) Personal Data other than the Data Owner's health and sexual life can be transferred without seeking the relevant person's Explicit Consent in cases stipulated by law. Personal Data related to health and sexual life, on the other hand, can be processed without seeking Explicit Consent of the owner by the person who has the obligation of keeping confidentiality or authorized institutions and organizations, only for the purpose of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and its financing.

4.5.2 Transfer of Personal Data Abroad

The data should not be transferred abroad. In case it should be transferred for a compulsory reason, the data owner should be informed, and his/her explicit consent should be obtained.

4.6 Monitoring of Visitor and Customer Activities

4.6.1 Closed Circuit Camera Recording

In order to ensure security, personal data processing activities are carried out by the Company through closed circuit camera surveillance in the stores and workplaces of the Company, monitoring the entrance and exit of people, such as customers, visitors and the shopping activities inside the store.

Personal data are processed in accordance with the Law and other relevant legislation through the use of cameras and recording of customer and guest entries and exits and their activities.

Monitoring can be done with closed-circuit cameras, especially to ensure the safety of the Company, visitors and others, and to protect the interests of customers regarding the service they receive. The Company duly discloses the objectives it has specified within this scope to the relevant people. In addition to the clarification it has made regarding general issues, the Company notifies with a different method that it deems appropriate regarding the closed-circuit camera surveillance activities.

Personal data processed within the scope of closed-circuit camera surveillance activity are kept for a maximum of [15 days].

In addition, identity check is made at the entrance to the headquarters of the company for security purposes and a guest book is kept. In this context, necessary measures are taken regarding the processing and security of personal data.

While obtaining the names and surnames of the persons who come to the company workplaces as guests, these personal data owners are informed by means of the texts hanged at the Company or made available to the guests in other ways. The data obtained for the purpose of monitoring guest entry-exit are processed only for this purpose and related personal data are recorded in the data recording system in physical environment.

In accordance with Article 10 of the Law, the Data Owner is informed by the Company.

In addition to the clarifications regarding general issues, the Company can notify about camera surveillance activities through multiple methods. The Company aims to prevent the damage to the fundamental rights and freedoms of the personal data owner and to ensure transparency and clarification of the personal data owner.

Regarding the camera surveillance activity by the company; a notification statement is hanged at the entrance of the surveillance areas. It is essential that only a limited number of Company employees have access to the camera recordings. Access authorization is given by the Data Protection Commission. Those who have access to the records also sign a confidentiality statement.

4.6.2 Website Visitors

Internet movements in the website can be recorded on the company's website by technical means (e.g. Cookie) in order to ensure that the website visitors perform their visits in a manner suitable for their visit purposes, to show them customized content and to perform online advertising activities.

In case that the Company carries out such a business activity, detailed explanations about the protection and processing of personal data are included in the "Cookie Policy" text on the Company's website.

4.7 Clarification During the Acquisition of Personal Data

4.7.1 When the consent of the Data Owner to process Personal Data is requested or in any case where Personal Data is collected (whether the consent is requested or not), it is essential that the Data Owner is properly informed. In this context, including but not limited to the followings will be declared to the data owner,

- Name/title and address of the Data Controller and, if applicable, the name and address of the representative of the Data Controller
- The purpose (s) of data processing
- The purpose of data transfer and to whom data will be transferred,
- Data collection method and legal reason,
- The rights of the Data Owner listed in the Law including the right to access data, to obtain a copy of the data, to delete and correct the data and the methods of using these rights.
- Type of the processed data

4.7.2 The above clarification obligations will not be applied where the applicable law exempts the obligations stipulated for clarification.

a) Personal Data processing is necessary for the prevention of a crime or for a criminal investigation.

b) Processing of Personal Data publicized by the Data Owner him/herself.

c) Based on the authority granted by the Law, the processing of Personal Data is required for the conduct of auditing or regulatory duties and for disciplinary investigation or prosecution by the assigned and authorized public institutions and organizations, and professional institutions that have the characteristics of public institutions.

d) Personal Data processing is necessary for the protection of the state's economic and financial interests in relation to budget, tax and financial matters.

4.7.3 The Data Owner should be informed as soon as possible and preferably at the first contact. In the case of employees, further clarification should be given. In addition, appropriate explanations should be given on job application forms or employee handbooks and workplace regulations. The explanations should be designed and made to attract the attention of those concerned.

4.7.4 The clarification can be done verbally, electronically, orally or in writing. In cases where the information is given verbally, the person making the statements must use a suitable written text or form pre-approved by the Company or the Data Protection Commission. The receipt document or form should be kept together with a simultaneous record that specifies the method, content, date and event of the explanation.

4.7.5 If the initial explanation is insufficient, additional explanations can be made later and the event, date, content and method of these annotations are recorded.

4.8 Avoiding New Activities That Are Not in Compliance with The Law

As a rule, new or expanded Personal and/or Sensitive Personal Data acquisition or processing activities will not be carried out by the Company without the approval of the Data Protection Commission. All relevant departments and managers will try to work in harmony with the Data Protection Commission and other departments and will avoid new activities that are not in compliance with the Law.

4.9. Rights of the Data Owner

4.9.1. The Company will establish a system compatible with its own policies and practices through the Data Protection Commission in order to enable Data Owner to exercise the rights specified in Article 11 of the Law, to facilitate this and to inform the relevant people in case of inappropriate disclosure of Personal Data.

4.9.2. The Data Owner has the following rights about his/her Personal Data with a request made in accordance with the policies and procedures set by the Company and the Data Protection Commission:

4.9.2.1. To find out whether the Company processes Personal Data about the Data Owner, and if so, to request information about it,

4.9.2.2. To learn the purpose of processing Personal Data and whether it is used in accordance with its purpose,

4.9.2.3. To find out whether Personal Data is transferred abroad or within the country and if so, to whom it was transferred.

4.9.3. The Data Owner also has the right to request the Company to amend incorrect and incomplete Personal Data and to inform the recipients to whom the data has or may have been transferred.

4.9.4. Data Owner, pursuant to Article 7 of the Law, may request the deletion and destruction of the data from the Company if the reasons that require the processing of Personal Data faded.

4.9.5. The Data Owner may object to the results of Personal Data analyzes, which have been created exclusively using an automated system, if these results contradict his/her interests.

4.9.6. All requests to be made by the Data Owner to the Company for the exercise of the above rights must be made in writing by filling out the request form submitted at kvkk@kochendoerfer.com.tr. Applications can be submitted personally or through

a notary or via e-mail with a secure electronic signature.

In order to process the requests of those acting on behalf of the Data Owner, they must submit a power of attorney (notarized) issued by the Data Owner, including requests or actions related to Personal Data. Identity cards and guardianship orders are requested from those who apply on behalf of their children or the people they guard.

4.9.7. All business units that receive a request from the Data Owner to access Personal Data will report these requests to the Data Protection Commission.

4.9.8. The Company will establish a system to record the requests mentioned here when they are received and to specify response dates.

Unless the applicable laws and regulations require otherwise, the Company will respond to an information request made as above, within 30 days from the date it received the written request from the Data Owner and that it was properly confirmed that it was the Data Owner or an authorized legal representative. Incomplete, incomprehensible or unreadable requests will not be considered by the Company. In such a case, the Company will inform the applicant within 30 days of not processing the application.

4.9.9. Even if the company cannot fully respond to the request within the specified time, the Data Protection Department must in any case provide the following information to the Data Owner within the said 30-day period:

- A confirmation that the data owner's request has been received,
- An explanation about all the information gathered as a response to the request until that time,
- An explanation about the information or change requested by the Data Owner, which cannot be given or realized by the Company, the reason (s) of refusing Data Owner’s request, and an explanation about objection against decision within the Company, if any,
- Notification of the price to be paid, if any, or the estimate of the price to be paid by the Data Owner, unless the applicable laws and regulations hinder the obligations of Data Owner in this regard.

4.9.10 If providing information to the relevant Data Owner who is requesting information causes disclosure of another person's Personal Data or creates a risk of violating fundamental rights and freedoms, the business unit that executes the request should review the data and redact the data in a way that may be necessary or appropriate to protect that person's rights or should not disclose the data.

4.9.11 The company will not charge any fees to the employees for providing the above-mentioned information. In cases where the information request imposes an additional cost to the Company, the Company may request a fee in the tariff to be determined by the Board in order to respond to requests from Data Owners who are not employees. In such a case, the fees to be determined cannot be higher than those to be announced by the Board from time to time.

4.9.12 The Company and the Data Protection Commission may establish procedures to track and reject repetitive or disturbingly burdensome requests from or on behalf of the Data Owner.

4.10 Storing, Deleting, Destroying and Anonymizing of Personal Data ("Preservation and Destruction of Personal Data")

Our company keeps the Personal Data that it processes in accordance with the principles stated in the Law for the period specified in the legislation. If a specific period of time is not stipulated in the legislation for the preservation of relevant Personal Data categories, Personal Data is kept until the purpose for which they are processed ends.

If a specific period of time is not stipulated in the legislation for the storage of relevant Personal Data categories, preservation periods are set according to each data processing purpose. In this context preservation periods are determined by considering the applications of our Company and the practices of commercial life.

Apart from the purpose of processing, Personal Data may be kept in order to constitute evidence in possible legal disputes, to claim a right that can be proved with Personal Data, to establish defense and to respond to information requests from authorized public institutions. In the establishment of the periods herein, the nonclaim statute periods and the preservation obligations arising from the legislation applied to the Company's activities, as well as the contracts to which it takes part and the international regulations to which it is subject are taken into consideration.

When the specified periods expire, the Company carries out the necessary actions to properly destroy Personal Data in a reasonably possible and appropriate way. In addition, the Company may delete, destroy or anonymize Personal Data ex officio or upon request by the Data Owner. The company decides which of these methods is reasonable and applies that method through the Data Protection Commission. Data Owner may request information about why the Company has chosen this method by using the rights described in item 4.9.

In accordance with Article 28 of the Law; Anonymous Personal Data can be processed for purposes such as research, planning and statistics.

4.11. Proportionality

The Company will pay attention to the principle of proportionality in terms of the implementation of this Policy. Attention will be paid to ensure that the expenditure and effort spent in terms of data processing activities of the Company and those spent for the protection of related Personal Data are proportional.

5- Registration of the Company to the Registry for Business Activities

If required, the company will fulfill its registration obligation in accordance with the Regulation on Data Controllers Registry.

6- Using Third Party Data Processor

6.1. Obligations of the Third-Party Data Processor

In cases where the Company receives service or other support from others to assist the processing activities, a Data Processor, which provides adequate security measures and takes reasonable steps to comply with these measures, will be selected in accordance with the Law, Secondary Legislation and Company policies.

6.2. Written Contracts for Third Party Data Processor

The Company will make a written contract with each Data Processor that requires compliance with the data privacy and security requirements that the Company is obliged to fulfill in accordance with the Law and Secondary Legislation.

6.3. Audit of Third-Party Data Processor

As part of the Company's internal data auditing processes, the Company will occasionally perform audits on data processing activities, and especially data security and measures carried out by third-party Data Processors and will establish the legal infrastructure required to carry out these audits.

7- Data security

7.1. Physical, Technical and Organizational Security Measures

7.1.1. The Company will take physical, technical or organizational measures to ensure the security of Personal Data taking into account the level of technological development, the nature of the data, and the risk they are exposed due to human or physical or natural environmental effects, including changes, losses, damage, unauthorized processing or access,

7.1.2. Security measures to be taken will be specified and implemented in accordance with the company's information security policies.

7.2. Employee’s Confidentiality Agreements

Anyone involved in any stage of the processing of Personal Data must explicitly make a commitment to confidentiality and sign a confidentiality agreement that must continue after the end of the business relationship.

8- Resolution of Disputes

8.1. Employees

8.1.1. Employees who have complaints and questions regarding the processing of their Personal Data should first discuss this with the Data Protection Commission. In cases where the Data Owner does not want to submit a question or complaint to the Data Protection Commission, or the Data Protection Commission cannot find a satisfactory solution to the Data Owner's questions or requests within 30 days from the date of request, the employee shall notify this situation in writing at the end of this period to the Data Protection Department.

8.1.2. In cases where the problem cannot be solved by the Data Protection Commission and the Data Protection Department, the dispute must be resolved according to the company's internal regulations and legislations and the terms of the employment contract.

9- Compliance Audit

9.1. Existing Compliance Evaluation

The company should specify a program through the Data Protection Commission and perform data protection compliance controls for all business units. The company should produce a plan and a program to correct the deficiencies identified in coordination with business units within a certain reasonable time.

9.2. Annual Data Protection Audit

Each business unit should evaluate data acquisition, processing and security practices. They should record relevant findings in their data inventory.

9.2.1. Departments will determine the state of the followings: which Personal Data is collected or planned to be collected by the department, the purpose of data collection and processing, any additional permitted purposes, the main use of the data, the presence of the relevant person's consent to these transactions and the scope of the consent, any legal obligations related to the collection and processing of such data, the scope, adequacy and implementation of security measures.

9.2.2. Departments will determine whether there is Personal Data processed by non-automated means provided that it is part of a data recording system.

9.2.3. Departments should determine the identity of the people to which the Personal Data under their domination or control is transferred. The department should determine the location of the people to whom the data was transferred, the purposes of the transfer, the availability of physical, technical systems and processes, at least to maintain the current level of data security.

9.2.4 The information obtained as a result of this annual evaluation should be reported to the Data Protection Commission to take appropriate measures, update company policies and procedures, and ensure the establishment of appropriate processes.

10- Implementation

10.1. Publication

This policy will be communicated to the employees by the Human Resources Department.

10.2. Effective date

This Policy takes effect as soon as it is published. All departments will collaboratively develop a timetable and process for the implementation of this policy. This implementation process will include resolution of conflicts between this Policy and other existing policies.

10.3. Revisions

Revisions can always be made to this Policy. The notifications of important revisions will be communicated to employees by the Company's Human Resources Department and to others through an appropriate mechanism selected by the Data Protection Commission.

11- Protector

Data Protection Commission is in charge of the protection of this Policy. Each department manager is responsible for the implementation of this Policy. Questions regarding the implementation of this Policy should be directed to the Data Protection Commission.

12- Divisibility

Each section of this policy will be interpreted to sustain that section in accordance with the applicable law, however, if any provision is prohibited or considered invalid, the invalidity of this provision will only be subject to that prohibition and invalidity, without affecting the rest of the provision or other remaining provisions of this Policy.