

Personal Data Processing and Protection Policy

1- Purpose

This Personal Data Processing and Protection Policy (“Policy”) regulates the principles that our company has determined to ensure compliance with the applicable legislation on the processing of personal data and the protection and destruction of this data.

2- Definitions

Capitalized terms used in this Policy that are not defined in the Policy will have the meanings ascribed to them below.

Explicit Consent	It means the consent that is based on information and expressed with free will on a particular subject.
Anonymization means making the incapable of being	Personal Data associated with an identified or identifiable natural person under any circumstances, even by matching with other data.
Secondary Legislation	means any regulation, circular, communiqué, policy decision or similar administrative decision or general opinion issued or taken by the Personal Data Protection Authority pursuant to the Law.
Relevant Users:	Persons who process personal data within the organization of the data controller or in line with the authorization and instruction received from the data controller, excluding the person or unit responsible for the technical storage, protection and backup of the data.
The	Law refers to the Personal Data Protection Law No. 6698.
Personal Data/s	means any information relating to an identified or identifiable natural person.
Processing of	Personal Data Obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available Personal Data by fully or partially automatic or non-automatic means provided that it is a part of any data recording system means all kinds of operations performed on data such as classification or prevention of use.
Board means the	Personal Data Protection Board.
Institution means the	Personal Data Protection Authority.
Sensitive Personal Data Data about the	race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, disguise and dress, membership to associations, foundations or unions, health, sexual life, criminal convictions and security measures,

	and biometric and genetic data.
Registry	Refers to the Data Controllers Registry, which is a registration system where data controllers have to register and declare information about data processing activities.
Deletion means making	personal data inaccessible and non-reusable for Relevant Users in any way.
Deletion and Destruction Policy	refers to the policy that the Company has prepared within the framework of the Regulation on the Deletion, Destruction or Anonymization of Personal Data, regulating the procedures and principles regarding deletion and destruction.
Company	KOCHENDÖRFER HYDRO ELEKTROMEKANİK SAN. and TİC. Inc. Y represents.
Data Processor	means the natural or legal person who processes Personal Data on behalf of the Data Controller based on the authority given by him.
Data Protection Commission means the	Company's Personal Data Protection Commission.
Data OwnerData Owner	, defined as “Relevant Person” in the Law, refers to the natural person whose Personal Data is processed. Data Subjects also include customers, internet users, individuals in communication, e-mail and marketing database lists, employees, contract parties and suppliers.
Data Controller	means the natural or legal person who determines the purposes and means of processing Personal Data and is responsible for the establishment and management of the data recording system.
Draft Regulation on theDraft Regulation on the	Data Controllers Registry TheData Controllers Registry has been prepared in accordance with Article 16 of the Law. It has not yet entered into force.
Destruction It means making	personal data inaccessible, irretrievable and unusable by anyone in any way.

3- Scope The

Company undertakes to comply with the confidentiality and security requirements of Personal Data existing under the Law, therefore the Company has adopted this Policy in order to establish the principles of understanding, policies and procedures regarding the protection and processing of Personal Data.

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

4- Principles Principles to be accordance with the

4.1 Followed in the Processing of Personal Data Personal Data is processed

4.1.1 only in Law and the Rules of Integrity.

The Company acts in accordance with the law and the rule of honesty in the processing of Personal Data. In this context, the Company processes Personal Data in accordance with the rules introduced by the Law. In addition, the Company also monitors the Secondary Legislation to be published by the Board from time to time and the regulations to be brought about data processing activities, and makes/will try to make improvements in its practices if necessary within the framework of these legal regulations.

4.2.2 Personal Data Must 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 Must Be Processed for Specific, Explicit and Legitimate Purposes.

The company clearly and precisely determines the purpose of data processing and processes Personal Data only for legitimate purposes. What is meant by this is that the data processed by the Company is related to and necessary for the work it has done or the service it has provided.

The Company clearly announces these purposes to the Data Owners before their Personal Data is obtained.

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

4.2.5 Personal Data Should Be Retained For The Period Envisaged In The Relevant Legislation Or Required For The Purpose For Which They Are Processed.

The 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, 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, the Company takes as a basis the maximum retention periods for the protection of the data in a way that will not cause the loss of rights of its employees and customers, especially considering the statute of limitations for personal data, which may be required to be protected, subject to different legislation. If a period is not determined in the legislation or there is no legal reason to keep the data for a longer period, the Company keeps the Personal Data for the period necessary for the purpose for which they are processed.

In addition to these, the Company also complies with the rules and procedures stipulated in the Company's Disposal Policy regarding data protection.

4.3 Processing Conditions Processing of

4.3.1 Personal Data

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

In this context:

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

4.3.1.2 In the presence of one of the following conditions, the Open Data Owner Consent can be processed regardless of the Personal Data:

1. clearly provided for in the Act;
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 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 his legal obligation; 5. Being made public by the Data Owner 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 Owner.

4.3.2. Data Protection Commission

Within the framework of the Company's compliance program, it has been decided that the personal data processing activities will be carried out and supervised by the Data Protection Commission.

The duties of the Data Protection Commission are as follows:

- a) Sellers, suppliers and third parties to whom Personal Data is transferred from the Company, those who have access to Personal Data obtained and processed by the Company, and those who provide data to the Company are required to comply with this Policy. To determine the procedures and standard contractual provisions, to determine
- b) the regular audit mechanisms, applied procedures and valid rules in order to comply with this Policy
- c) , to determine and maintain the system that will provide a fast and appropriate response to the requests of the Data Owner to the Company while exercising their rights arising from the Law. and to carry it out,
- d) to ensure that the compliance program of the Company is up-to-date, to
- e) inform the Company's senior executives, executives and managers about potential corporate and individual, administrative or criminal liabilities that may be directed against the Company and/or its employees due to the violation of the applicable legislation, and to take necessary actions. to carry out, the
- f) Company's Institution, Board and the Registry,
- g) ensuring that all necessary records are made to the Registry in accordance with the relevant legislation and Board decisions, and supervising the registry records,
- h) managing and putting into practice the activities to implement the Board's decisions.

4.3.3. Processing of Special Quality Personal Data

Personal Data is processed by the Company in accordance with the conditions specified in the Law. In addition, special measures may be introduced by the Board for the processing of Sensitive Personal Data. If measures are taken by the Board at any time after the publication of this Policy, the Company will make the necessary arrangements to comply with these measures.

In this context:

4.3.3.1 Special Quality Personal Data can be processed with the Explicit Consent of the Data Owner.

4.3.3.2 Private Personal Data of the Data Owner other than his/her health and sexual life (related to race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, dress, association, foundation or union membership, criminal conviction and security measures) data and biometric and genetic data) can be processed without seeking the explicit consent of the person in cases stipulated by the laws.

4.3.3.3 Personal Data related to health and sexual life, on the other hand, can only be used for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing, by persons under the obligation of keeping secrets or by authorized institutions and organizations without seeking the explicit consent of the person. can be processed.

4.3.3.4 In particular, the Personal Data of the employees related to health can be processed directly or indirectly in order to carry out the processes within the scope of the employer-employee relationship (permit, advance, insurance process, creation of the personnel file, etc.). In such cases, explicit consent is obtained from the employees and personal data related to health can only be processed and accessed by the persons or departments that are required to process this data. These personal data may be processed without explicit consent, if determined within the framework of the current legislation and the decision of the Institution/Board, which do not require consent.

4.4 Consent To be

4.4.1 valid, consent must be based on information, be explicit, and be expressed with free will.

4.4.2.1 The Data Owner must be informed in a clear and understandable manner on all matters related to the processing. This information should be understandable and easily accessible in a language that the average individual can understand.

4.4.2.2 Explicit Consent should be understood as a declaration of consent that is clear without hesitation and is limited to that transaction only. An open-ended consent cannot be considered an Open Consent. As a rule, it is sufficient to obtain the Explicit Consent of the Data Owner once for different transactions to be performed by the Data Controller. However, if the data in question is requested to be processed for purposes other than its original purpose, a separate consent will be required.

4.4.2.3 Explicit Consent should be given freely, without any pressure, and is valid only if the Data Subject is able to demonstrate a genuine choice.

4.4.2.4 As long as these conditions are met, the way of obtaining consent can be freely determined. These can be in the form of clauses in employment contracts, checkboxes on application or purchase forms, and boxes in online forms where Personal Data is entered.

4.4.3 Where consent is obtained through other written representations, the request for consent must be made prominently.

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

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

4.5 Transfer of Personal Data

4.5.1 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 for the required level of data protection.

4.5.1.2 Personal Data may be transferred to third parties only for reasons consistent with the purposes for which they were obtained 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 by using encryption to the extent possible.

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

4.5.1.5 Personal Data can be transferred in cases where any of the following are valid: The

a) Data Owner's Explicit Consent to the transfer in question, The

b) transfer is expressly stipulated in the law, The

c) life or physical integrity of the person or another person who is unable to express his consent due to the actual impossibility of the transfer or whose consent is not legally valid.that the

d) Provided transfer is directly related to the establishment or performance of a contract, the processing of the Personal Data belonging to the parties to the contract is necessary, the Data Controller

e) transfer is mandatory for the to fulfill its legal obligation

f) , The transfer of data is

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

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

i) Provided that adequate precautions are taken, personal data other than health and sexual life may be transferred without seeking the explicit consent of the person concerned, in cases stipulated by the laws. Personal Data related to health and sexual life, on the other hand, can only be collected by individuals or authorized institutions and organizations that are under the obligation of confidentiality, for the purpose of protecting public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and managing health services and financing. It can be processed without seeking his express consent.

4.5.2 Transfer of Personal Data Abroad

Data should not be transferred abroad. In cases where it is required to be transferred for a compulsory reason, the data owner should be informed and his explicit consent should be obtained.

4.6. Monitoring Visitor and Customer Activities

4.6.1. Taking Closed Circuit Camera Recording In

order to ensure security, the Company carries out personal data processing for monitoring the entrances and exits of people, such as customers and visitors, with closed circuit cameras at the stores and workplaces of the Company, and for monitoring the shopping activities in the store. .

Personal data is processed in accordance with the Law and other relevant legislation, by using cameras and recording customer and guest entries and exits and their activities.

In order to ensure the safety of the company, visitors and other persons and to protect the interests of the customers regarding the service they receive, monitoring can be done with closed circuit cameras. The company duly discloses the objectives it has determined in this context to the relevant persons.

In addition to the lighting it makes regarding general matters, the company also notifies with a different method it deems appropriate regarding the surveillance activity with closed circuit camera.

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

In addition, for security purposes, identity checks are made at the entrances to the company's headquarters 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, or through the texts posted in the Company or made available to the guests in other ways, the personal data owners in question are informed in this context. The data obtained for the purpose of tracking guest entry-exit is processed only for this purpose and the relevant personal data is recorded in the data recording system in the physical environment.

The Data Owner is informed by the Company in accordance with Article 10 of the Law.

In addition to the lighting it makes regarding general issues, the company can make notifications with more than one method regarding the camera monitoring activity. The Company aims to prevent harming the fundamental rights and freedoms of the personal data owner and to ensure transparency and enlightenment of the personal data owner.

For the camera monitoring activity by the company; A notification letter stating that monitoring will be made is posted at the entrances of the areas where monitoring is done. It is essential that only a limited number of Company employees have access to the footage. Access authorization is done by the Data Protection Commission. Those who have access to the records are also made to sign a confidentiality agreement.

4.6.2. Website Visitors On the

Company's website; to ensure that the visitors of the site perform their visits in accordance with the purposes of their visit; Internet movements within the site can be recorded by technical means (eg Cookies/Cookies) in order to show them customized content and to engage in online advertising activities.

If the company carries out such a processing activity, detailed explanations on the protection and processing of personal data are included in the text of the "Cookie Policy" on the company's website.

4.7. Clarification During the Obtaining of Personal Data It is

4.7.1 essential to inform the Data Owner appropriately at the moment when consent is requested from the Data Owner to process Personal Data or in any situation where Personal Data is obtained (whether consent is requested or not). In this context, including but not limited to the following, the

- name/title and address of the Data Controller and, if applicable, the name and address of therepresentative
- Data Controller'sPurpose(s) ofprocessing The purpose(s) of
- datadata transfer and to whom the data will be transferred,
- Data collection method and The legal reason,
- the rights ofthelisted in the Law, such as the right to access the data, get a copy of the data, delete and rectify the data, and the methods of exercising these rights, the
- Data

Ownertype of data processed

will be explained to the Data

Owner.

4.7.2 The lighting obligations above will not be applied in cases where the applicable laws make exceptions to the obligations stipulated for lighting.

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

b) Processing of Personal Data made public by the Data Owner himself.

c) Personal Data processing is necessary for the execution of supervisory or regulation duties and for disciplinary investigation or prosecution by authorized and authorized public institutions and organizations and professional organizations in the nature of public institutions, based on the authority given by the Law.

d) The processing of Personal Data is necessary for the protection of the economic and financial interests of the state with regard to budget, tax and financial matters.

4.7.3 Clarification should be carried out as soon as possible and preferably at the first contact with the Data Owner. In the case of employees, lighting should be done separately. In addition, appropriate disclosures should be made in job application forms or in employee handbooks and workplace regulations. Explanations should be constructed and made in such a way as to attract the attention of those concerned.

4.7.4 Illumination can be made verbally, electronically, orally or in writing. Where disclosure is made orally, the person making the disclosures must use an appropriate written text or form approved in advance by the Company or the Data Protection Commission. The receipt or form should be kept with a concurrent record specifying the method, content, date and event of the disclosure.

4.7.5 If the initial explanation is insufficient, annotations 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, no new or expanded Personal and/or Special Quality Personal Data acquisition or processing activities will be carried out by the Company without the approval of the Data Protection Commission. They will try to work in harmony with all relevant departments and managers, the Data Protection Commission and other departments, and will avoid new activities that are not in compliance with the Law.

4.9 Data Owner's Rights

4.9.1 Through the Data Protection Commission, the Company establishes a system in line with its own policies and practices in order to enable the Data Owner to exercise their rights listed in Article 11 of the Law, to facilitate this and to inform the relevant persons about the inappropriate disclosure of Personal Data. will set up.

4.9.2 With a request made in accordance with the policies and procedures determined by the Data Owner, the Company and the Data Protection Commission, about their Personal Data: To

4.9.2.1 learn whether the Company processes Personal Data about the Data Owner, if so, to request information about this, to process the

4.9.2.2 Personal Data purpose and whether they are used in accordance with its purpose, whether the

4.9.2.3 has the right to learn the Personal Data is transferred domestically or abroad and to whom it is transferred.

4.9.3 The Data Owner also has the right to request the Company to correct inaccurate and incomplete Personal Data and to inform the recipients whose data has been or may have been transferred.

4.9.4 In accordance with Article 7 of the Law, the Data Owner may request the deletion and destruction of his data from the Company in case the reasons requiring the processing of his Personal Data disappear.

4.9.5 The Data Owner may object to the results of Personal Data analyzes created exclusively using an automated system, if these results are contrary to their 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 kvkk@kochendoerfer.com.tr filling out the request form submitted at. Applications can be submitted in person or through a notary public or by e-mail with a secure electronic signature.

In order for the requests of those acting to represent the Data Owner to be processed, they must submit to the Company a power of attorney (notarized) issued by the Data Owner, containing a special provision regarding the requests or actions regarding their Personal Data. Identity card and guardianship decision are requested from those who apply on behalf of their children or guardians.

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

4.9.8 The company will establish a system to record the requests mentioned herein when they are received and to determine the response dates.

Unless otherwise required by applicable laws and regulations, the Company responds to a request for information made as stated above within 30 days from the date of receipt of a written request from the Data Owner and the appropriate confirmation that the requester is the Data Owner or an authorized legal representative proving his identity. will give. Incomplete, incomprehensible or illegible requests will not be considered by the Company. In such a case, the Company will inform the applicant within 30 days of the application not being processed.

4.9.9 Even if the Company can not answer fully to the request within the specified time, the Data Protection Department said in any case must provide the following information to the Data Owner within 30 days:

- a receipt of the data owner's request for confirmation,
- until that time, all who gathered in response characteristics that directed the demand information about releases,
- Data owner to be quoted by requested by the Company regarding the information or any change or an explanation as to which can not be performed, Data owner to request the rejection reason (reasons), and if there is the decision of the appeal procedures within the company an explanation of
- in force laws and regulations Data owner Notification of the price to be paid, if any, or estimation of the price, by the Data Owner, unless it prevents the liability of the Data Owner in this regard.

4.9.10 If providing information to the requesting Data Owner would cause the disclosure of another person's Personal Data or risk violating their fundamental rights and freedoms, the business unit conducting the request should review the data and redact the data as necessary or appropriate to protect the rights of this person. or not disclose data.

4.9.11 The Company will not charge any fee from employees for providing the above-mentioned information. In cases where the information request imposes additional costs on the Company, the Company to bebyBoard in order to respond to requests from Data Owners who are not employees

may charge a fee in the tariff determined. In such a case, the fees to be determined cannot be higher than the fees to be announced by the Board from time to time.

4.9.12 The Company and the Data Protection Commission may establish procedures to monitor and reject repetitive or annoyingly burdensome requests by or on behalf of the Data Subject.

4.10 Storage, Deletion, Destruction and Anonymization of Personal Data (“Storage and Disposal of Personal Data”)

Our company keeps the Personal Data that it processes in accordance with the principles in the Law for the period stipulated in the legislation. If the legislation does not provide for a certain period of time for the storage of the relevant Personal Data categories, the Personal Data is retained until the end of the purpose for which they are processed.

In the absence of a specific period for the storage of the relevant Personal Data categories in the legislation, storage periods are determined for each data processing purpose. In this context, retention periods are determined by taking into account the practices of our Company and the practices of commercial life.

Personal Data; Apart from the processing purpose, it can be stored in order to constitute evidence in possible legal disputes, to assert a right that can be proven with Personal Data, to establish defense and to respond to information requests from authorized public institutions. In the establishment of the periods herein, the statute of limitations for asserting the aforementioned right, the retention obligations arising from the legislation applicable to the Company's activities, the contracts to which it is a party and the international regulations to which it is subject are taken into account.

The Company takes the necessary actions to destroy the relevant Personal Data as reasonably possible and appropriately when the specified periods expire. In addition, the Company may delete, destroy or anonymize Personal Data, ex officio or as the case may be, upon the request of the Data Owner. The Company, through the Data Protection Commission, decides which of these methods is reasonable and applies that method. The Data Owner may request information about why the Company has chosen this method, by exercising its rights described in article 4.9.

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

4.11 Proportionality

In terms of the implementation of this Policy, the Company will pay attention to the principle of proportionality. Care will be taken to ensure that the expense and effort spent in terms of the Company's data processing activities and the protection of the relevant Personal Data are proportionate to the purpose of protecting the data.

5- Registration of the Company in the Registry for Processing Activities

The company will fulfill its registration obligation in accordance with the Regulation on the Registry of Data Controllers, if necessary.

6- Use of Third Party Data Processors

6.1. Obligations of the Third Party Data Processor

In cases where the Company receives services or other support from others to assist its processing activities, a Data Processor who 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 Agreements for Third Party Data Processors

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

6.3 Control of Third Party Data Processor

As part of the Company's internal data audit processes, the Company will conduct audits from time to time on data processing activities and, in particular, data security and measures by a third-party Data Processor, and will establish the necessary legal infrastructure to carry out these audits.

7- Data Security

7.1 Physical, Technical and Organizational Security Measures

7.1.1 In order to ensure the security of Personal Data, the Company takes into account the level of technological development, the nature of the data and the risk they are exposed to by human or physical or natural environmental effects, including changes, loss, damage, unauthorized processing or access, physical, technical or organizational measures.

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

7.2 Employee Confidentiality Agreements

Everyone involved in any stage of the processing of Personal Data must clearly make a confidentiality commitment and sign a confidentiality agreement, which 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 matter 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 in cases where 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 does so in writing at the end of the period. It should be directed to the Department of Conservation.

8.1.2 In cases where the problem cannot be resolved through the Data Protection Commission and the Data Protection Department, disputes should be resolved in accordance with the company's internal regulations and regulations and the provisions of the employment contract.

9- Compliance Check

9.1 Current Compliance Assessment

The company must set a schedule and conduct a data protection compliance audit for all business units through the Data Protection Commission. The company, in coordination with the business units, should produce a plan and program to rectify the identified deficiencies within a reasonable period of time.

9.2 Annual Data Protection Audit

Each business unit should evaluate data acquisition, processing and security practices. They should commit relevant findings to their data inventories.

9.2.1 Departments, which Personal Data is collected and planned to be collected by the department, the purpose of data collection and processing, any additional purposes allowed, the actual use of the data, the existence of the data subject's consent to these transactions and the scope of consent, the data collection and processing, any legal obligations, the scope, adequacy and implementation status of security measures will be determined.

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

9.2.3 Departments must identify the persons to whom Personal Data under their control or control is transferred. Department where the transferred persons are located.