	Policy	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 1 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

**CFN KIMYA SANAYI VE DIS TICARET
ANONIM SIRKETI
PERSONAL DATA PROTECTION AND PROCESSING POLICY**



	<h1>Policy</h1>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 2 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

TABLE OF CONTENTS

PART 1: INTRODUCTION.....	3
1.1 The Importance of Personal Data Protection.....	Error! Bookmark not defined.
1.2 The Purpose of the Policy.....	Error! Bookmark not defined.
1.3 Scope.....	Error! Bookmark not defined.
1.4 Definitions	Error! Bookmark not defined.
1.5 Implementation of the Policy and Relevant Legislation.....	Error! Bookmark not defined.
1.6 Access and Updating.....	Error! Bookmark not defined.
PART 2: PROCESSING OF PERSONAL DATA.....	5
2.1 Processing of Personal Data in Accordance with the Principles and Rules Stipulated in the Legislation.....	Error! Bookmark not defined.
2.2 Transfer of Personal Data.....	Error! Bookmark not defined.
2.3 Categorization of Personal Data by the Company	Error! Bookmark not defined.
PART 3: LEGAL BASIS AND PURPOSES OF PROCESSING PERSONAL DATA.....	14
3.1 Legal Basis for Processing Personal Data	Error! Bookmark not defined.
3.2 Purposes of Processing Personal Data.....	Error! Bookmark not defined.
PART 4: STORAGE, DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA	18
4.1 Storage and Storage Periods of Personal Data.....	Error! Bookmark not defined.
4.2 Deletion, Destruction, and Anonymization of Personal Data	Error! Bookmark not defined.
PART 5: RIGHTS OF RELEVANT PERSONS.....	20
5.1 Scope of Rights of Relevant Persons and Use of These Rights.	Error! Bookmark not defined.
PART 6: ENSURING THE SECURITY OF PERSONAL DATA.....	21
6.1 Technical and Administrative Measures Taken to Ensure Processing of Personal Data In Compliance With Law.....	Error! Bookmark not defined.
6.2 Technical and Administrative Measures Taken in the Processing of Sensitive Personal Data	Error! Bookmark not defined.

	<h1>Policy</h1>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 3 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

PART 1: INTRODUCTION

1.1 The Importance of Personal Data Protection

The protection of personal data is a constitutional right and is a priority for CFN Kimya Sanayi ve Dis Ticaret A.S. (“**CFN Kimya**,” “**Company**,” or “**Our Company**”). Accordingly, CFN Kimya aims to establish a continuously updated system for the protection of personal data, and hereby policy has been created.

CFN Kimya acts in capacity of data controller within the scope of Law No.6698 on the Protection of Personal Data (“**LPPD**” or “**Law**”), and hereby Policy on the Protection and Processing of Personal Data POL.021 (“**Policy**”) has been prepared to fulfill the general disclosure obligation stipulated by the LPPD and to establish the fundamental principles of CFN Kimya’s personal data processing rules.

In this context, our Company aims to establish an updatable system for all its departments in personal data processing activities, and relevant processes are being brought into compliance with the legislation. Hereby Policy sets out the fundamental principles for protecting the personal data of our customers, potential customers, employees, candidate employees, interns and students, supplier/subcontractor employees and officials, company shareholders and partners, visitors, and other third parties whose personal data is processed for any reason.

In order to implement the respects specified in the Policy, the necessary procedures are established within our Company, detailed disclosure documents regarding the protection of personal data are prepared, confidentiality agreements are signed with employees and third parties who have access to personal data, employee job descriptions are revised to ensure compliance with data security processes, and our Company conducts regular audits by taking the necessary technical and administrative measures to protect personal data.


The protection of personal data is embraced by our Company's senior management, and personal data security processes are managed by the CFN Kimya Personal Data Protection Committee (“**Committee**”), established under PR.030 LPPD Management Procedure.

1.2 Purpose of the Policy

The main objective of hereby Policy is to determine the personal data processing activities carried out by our Company in accordance with the law and the principles for the protection of personal data, and to ensure transparency by informing the relevant parties whose personal data is processed.


1.3 Scope

Hereby Policy includes all personal data of individuals categorized under the headings “*our customers, potential customers, employees, job candidates, interns, supplier and subcontractor employees and their officers, CFN Kimya shareholders and partners, visitors, employee references, employee families and relatives, parents/guardians/representatives, and other third parties whose personal data we process for any reason under applicable legislation,*” processed automatically or non-automatically, provided that it is part of any data recording system.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 4 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

1.4 Definitions

Explicit Consent	: The consent on a specific subject based on information and expressed with free will.
Anonymization	: Making a personal data incapable of being linked together with an identified or identifiable natural person, even by matching with other data.
Relevant Person	: The natural person whose personal data is processed.
Law/LPPD	: The Law No.6698.On Personal Data Protection
Personal Data	: Any information related to an identified or identifiable natural person.
Processing of Personal Data	: Any kind o transaction carried out on personal data, such as obtaining, recording, storing, preserving, altering, reorganizing, disclosing, transferring, acquiring, making available, classifying, or preventing the use of personal data, whether fully or partially by automatic means, or non-automated means provided that it is part of any data recording system.
Board	: Personal Data Protection Board.
Authority	Personal Data Protection Authority.
Sensitive Personal Data	: Data related to race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, dress, association, foundation, or union membership, health, sexual life, criminal convictions, and security measures, as well as biometric and genetic data.
Data Processor	: A natural or legal person who processes personal data on behalf of the data controller by the authority granted by the data controller.
Data Recording System	A recording system in which personal data is structured and processed according to specific criteria.
Data Minimization	: Requesting and processing personal data as much as required for the purpose of processing, and deleting the data completely if the purpose of use ends.
Data Controller	: The person who determines the purposes and means of processing personal data and manages the location where the data is systematically stored.

	Policy	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 5 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

1.5 Implementation of the Policy and Relevant Legislation

The provisions of the Law on the Protection of Personal Data (LPPD) No. 6698 and other relevant legislation in force shall be primarily applied regarding the processing and protection of personal data. The provisions of the LPPD and other relevant case of any inconsistency between the applicable legislation and hereby Policy prepared by our Company, our Company agrees that the provisions of the applicable legislation will prevail.

1.6 Access and Updating

Hereby Policy is published by our Company on the website of www.cfnkimya.com and made available to relevant persons. It will also be submitted to personal data owners upon their request.

Our Company maintains its processes regarding the protection and processing of personal data in compliance with applicable legislation and the Policy may be updated if there are changes to the relevant legislation or our Company's practices. Any changes, along with the updated Policy, will be published on our Company's website and made available to the relevant persons.

PART 2: PROCESSING OF PERSONAL DATA

Our company processes personal data in accordance with Article 20 of the Constitution and Article 4 of the Law on Personal Data Protection;


- In compliance with the law and good faith,
- Accurate and up-to-date, when necessary,
- In line with specific, clear, and legitimate purposes,
- In a purpose-related, limited, and moderate manner

and carries out personal data processing activities in accordance with relevant legislation. Our Company stores personal data for the period stipulated by law or required by the purpose of processing personal data, and when the purpose of processing ends, it deletes, destroys, or anonymizes the relevant data as stipulated by law.

Our Company processes personal data only on the basis of at least one of the legal bases specified in Article 5 of the Law, in accordance with Article 20 of the Constitution and Article 5 of the Law. In addition to this, pursuant to Article 419 of the Turkish Code of Obligations, the personal data of employees and candidate employees is processed for the purposes of job aptitude assessment and the execution of employment contracts. Our Company informs personal data owners in accordance with Article 20 of the Constitution and Article 10 of the Law and provides the necessary information and respond to applications within the legally mandated timeframes in case data owners request information or make application to exercise their rights under the law.

In addition, our Company acts in compliance with the special regulations stipulated for the processing of sensitive personal data in accordance with Article 6 of the Law.

On the other hand, regarding the transfer of personal data It takes the necessary legal and technical measures in accordance with Articles 8 and 9 of the Law and its practices are implemented considering the resolutions, communiques, and lists of safe countries, safe sectors, or safe international organizations published by the Personal Data Protection Board ("**Board**").

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 6 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

2.1 Processing of Personal Data in Accordance with the Principles and Rules Stipulated in the Legislation

2.1.1 Principles of Processing of Personal Data

A. Processing in Accordance with Law and Good Faith

The Company acts in accordance with applicable legal regulations and good faith in the processing of personal data. In this context, it identifies the legal basis requiring the processing of personal data and carries out its transactions in accordance with the principle of moderateness and processes personal data only for the specified purpose. The Company does not process personal data without the consent of the relevant persons and acts in a manner that does not violate the fundamental rights of data owners.

B. Ensuring Personal Data is Accurate and, Where Necessary, Up-to-Date

The Company takes measures to ensure that the personal data that it processes is accurate and up-to-date by considering the fundamental rights of personal data owners and its own legitimate interests, and operates the necessary control mechanisms accordingly.

In this context, data of all categories of individuals is ensured to be kept up-to-date, and customer, employee, and supplier data in particular is regularly reviewed and updated. In addition, marketing and promotion-related emails and offers are not sent without the consent of the relevant persons.

C. Processing for Specific, Clear, and Legitimate Purposes

The Company clearly and definitely defines its legitimate and lawful data processing purposes and processes personal data only in connection with the services that it offers and to the extent necessary. Data processing processes are based on unambiguous purposes and in compliance with relevant legislation.

D. Processing in a Purpose-Related, Limited and Moderate Manner

The Company acts in accordance with the principle of processing personal data only to the extent necessary to achieve the specified purposes and not to exceed the limits required for that purpose.

In this context:

- Personal data processing is constantly reviewed.
- Only data necessary for business processes is processed by applying the principle of "**Data Minimization**" and unnecessary data processing is avoided.


E. Storing for Period Specified in Relevant Legislation or as long as Necessary for the Purpose of Processing

The Company stores the personal data only for the period specified in relevant legislation or as long as necessary for the purpose of processing.

In this context;

- First of all, the periods specified for the storage of personal data in the relevant legislation are determined,
- If a special time is determined in the legislation, it is acted in accordance with these periods,
- The storage time of personal data is determined by considering the period of limitations for law and criminal cases,
- When the storage period ends, personal data is deleted, destroyed or anonymized within the scope of the **PR.049 Asset Management Procedure**.

In accordance with these principles, our company is responsible for constantly reviewing the personal data processing processes and making the necessary updates.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 7 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

2.1.2 General Data Processing Rules of Personal Data

The protection of personal data is a constitutional right, and the fundamental rights and freedoms can only be processed on the basis of the reasons specified in the relevant articles of the Constitution and provided that it is limited to the law. In accordance with the third paragraph of Article 20 of the Constitution, the personal data may be processed only in cases stipulated in the law or by the explicit consent of the relevant person.

The company can only process personal data without seeking the explicit consent of the relevant person when the following legal conditions are met:

- a. It is clearly foreseen by the laws,
- b. It is obligatory to protect the life or body integrity of the person who is unable to explain his/her consent due to actual impossibility or who are not granted legal validity for his/her consent.
- c. It is necessary to process personal data of the parties of the contract, provided that it is directly related to the establishment or performance of a contract,
- d. It is obligatory for the data controller to fulfill its legal obligation,
- e. It has been made public by the relevant person himself/herself,
- f. It is obligatory to process data for the establishment, use or protection of a right,
- g. It is obligatory to process data for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the relevant person.

In the absence of the above conditions, the company should take explicit, free will based and informed consent from the relevant person. Especially in Human Resources and Labour Relations processes, the personal data are primarily processed on legal reasons other than consent by considering the dependency relationship between the employee and the employer. However, in the absence of these legal reasons, the employee's explicit consent is asked. In addition, in any case where personal data is processed, the relevant persons are primarily clarified and data processing activities are carried out in a transparent way.


2.1.3 Rules of Processing Sensitive Personal Data

In the processing of personal data determined by the company as “**Sensitive data**” in the law, the relevant legislation and the additional security measures determined by the Personal Data Protection Board are applied. In accordance with Article 6 of the Law, a number of personal data that risks people to cause victimization or discrimination when processed unlawfully is determined as “Sensitive Data and it is required to show maximum attention and sensitivity in the processing of such data.

In this context, sensitive personal data are included in the following categories:

- *Race or ethnic origin*
- *Political Opinion*
- *Philosophical belief, religion, sect or other beliefs*
- *Dress*
- *Association, foundation or union membership*
- *Health data*
- *Sexual Life Data*
- *Data on criminal conviction and security measures*
- *Biometric and genetic data*

As a rule, sensitive personal data are not processed by the company. However, as a requirement by business processes, in cases where the processing of such data is obligatory, it can be processed in the following cases by taking the necessary security measures within the framework of the relevant legislation and the rights of the relevant person:

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 8 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

- The fact that the relevant person has given his/her explicit consent,
- It is clearly foreseen by the laws,
- It is obligatory to protect the life or body integrity of the person who is unable to explain his/her consent due to actual impossibility or who are not granted legal validity for his/her consent.
- It is required to process the personal data made public by the relevant person and in accordance with the will to make it public,
- It is obligatory to process data for the establishment, use or protection of a right,
- It is necessary to process data for the protection of public health by persons or authorized institutions and organizations under the obligation to keep secrets, the execution of preventive medicine, medical diagnosis, treatment and care services, and for health services for the purpose of planning, management and financing.
- It is obligatory to process data in order to fulfill the legal obligations in the fields of occupational health and safety, employment, social security, social services and social aid,
- To carry out processing activities targeting current or former members and affiliates or persons who are in regular contact with these organizations and formations, provided that it complies with the legislation and objectives of foundations, which the associations and other non-profit organizations or formations are subject to, established for political, philosophical, religious or union purposes, is limited to their fields of activity and is not disclosed to third parties;

The company takes all technical and administrative measures in order to ensure the security of the relevant data categories for the protection of sensitive personal data. In this context, the **PR.0112 Sensitive Personal Data Protection Procedure** was put into force in the company regarding the protection of sensitive personal data. The relevant business units act in accordance with this procedure and apply additional security measures stipulated in the legislation on the protection of sensitive personal data. It is fully complied with the general data processing principles regulated in Article 4 of the Law in all processes related to the processing of sensitive personal data.


2.1.4 Clarification and Informing the Relevant Persons Whose Data Is Processed

The Company clarifies and informs the relevant persons during obtaining of personal data in accordance with Article 10 of the Law. In this context, the relevant persons whose data is processed are clarified about the following subjects:

- What purposes for personal data are processed,
- To Whom and for what purposes can personal data be transferred,
- The method and legal reason for collecting personal data,
- The rights of the persons whose personal data are processed within the scope of the law.

The relevant departments of the Company fulfill the obligation of clarification in line with the clarification texts prepared by the company and provide the necessary information to the relevant persons.

Furthermore, in accordance with Article 11 of the Law, the persons whose personal data is processed have the right to "request information. Accordingly, the company evaluates the information requests coming from personal data owners in accordance with Article 20 of the Constitution and Article 11 of the Law and responds to the relevant persons within the framework of the periods and principles stipulated in the Law.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 9 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

The Company takes the necessary administrative and technical measures in order to manage the applications of the relevant persons effectively and applies procedures that determine the application processes to ensure that data owners can use their rights.

2.2 Transferring Personal Data

For the personal data processing purposes, the Company can transfer the personal data and sensitive personal data of the relevant persons to third parties in accordance with the law by taking the necessary safety measures to the third parties. Accordingly, the Company fully complies with the regulations stipulated within the scope of Article 8 of the Law.

2.2.1 Principles of Transferring Personal Data

For the purpose of legitimate and lawful personal data processing purposes, the company can transfer personal data to third parties based on one or more of the personal data processing conditions specified in Article 5 of the Law:

- The fact that the relevant person has given his/her explicit consent,
- Presence of a clear regulation in the law regarding that personal data will be transferred,
- It is necessary to protect the life or physical integrity of the relevant person or another person and the relevant person is unable to give his consent due to actual impossibility or his consent is not recognized as legally valid,
- It is necessary to process personal data of the parties of the contract, provided that it is directly related to the establishment or performance of a contract,
- Personal data transfer is obligatory for the company to fulfill its legal obligations,
- Transfer of personal data made public by the relevant person in accordance with the purpose of making it public,
- It is obligatory to process data for the establishment, use or protection of a right,
- It is necessary to transfer personal data for the legitimate interests of the company, provided that it does not harm the fundamental rights and freedoms of the relevant person concerned.


In addition to these, the Company keeps and processes all commercial records, documents, and personal data within the scope of the services that it offers in accordance with its legal data storage obligations.

In case of a legal dispute between the Company and data owners, the relevant personal data may be used to resolve the dispute and may be transferred to competent courts, prosecutors' offices, other judicial and administrative authorities, and alternative resolution authorities.

The Company may share personal data processed within the scope of personal data processing purposes with the followings:

- Authorized state institutions and organizations (Ministries, courts, enforcement offices, independent administrative authorities, tax authorities, etc.),
- Its main shareholders and affiliates,
- Service providers, business partners, consultants, and suppliers,
- Banks and financial institutions,
- Legally authorized public legal entities, private individuals, or judicial authorities, International public organizations and private institutions.

These transfers are carried out in accordance with the personal data processing conditions and purposes stipulated in Articles 8 (domestic transfer) and 9 (transfer abroad) of the Law.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 10 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

Regardless of the legal basis, the fundamental principles set forth in Article 4 of the Law are always considered in the transfer of personal data, and it is ensured to comply with these principles completely.

2.2.2 Transfer of Sensitive Personal Data

The Company demonstrates the utmost care regarding the protection and processing of sensitive personal data, takes all necessary administrative and technical measures, and manages the transfer of sensitive personal data by implementing adequate measures determined by the Board.

The Company may share sensitive personal data with third parties in accordance with its legitimate and lawful personal data processing purposes in the following cases:

- In case of explicit consent of the relevant person.
- In the absence of explicit consent of the relevant person:
- Sensitive personal data excluding the health and sexual life of the relevant person (data related to race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership in associations, foundations or unions, criminal convictions and security measures, as well as biometric and genetic data), in cases clearly foreseen in the laws,
- On the other hand, sensitive personal data related to health and sexual life of the relevant person may be transferred only to persons or authorized institutions and organizations subject to a confidentiality obligation for the purposes of protecting public health, providing preventive medicine, medical diagnosis, treatment and care services, and planning and managing the financing of healthcare services.

The Company has put **PR.0112 Sensitive Personal Data Protection Procedure** regarding the transfer of sensitive personal data in effect, and all relevant business units act in accordance with this procedure and take all necessary security measures.


Regardless of the legal basis, the fundamental principles set forth in Article 4 of the Law are always considered in the transfer of sensitive personal data, and it is ensured to comply with these principles completely.

2.2.3 Transfer of Personal Data Abroad

Personal data processed by the Company may be transferred abroad if one of the legal conditions specified in Articles 5 and 6 of the Law is met and an adequacy decision has been issued by the Board regarding the country, industry, or international organization to which the transfer will be made.

In the absence of an adequacy decision, personal data may be transferred abroad if one of the legal conditions specified in Articles 5 and 6 of the Law is met, the relevant person is able to use their rights abroad, and one of the appropriate assurances listed below is met, provided that the person concerned can also use his/her rights in the country abroad and has the opportunity to take legal steps:

- i. The presence of an agreement, that was made between institutions and organizations or international organizations abroad and state institutions and organizations or professional organizations with public institution status in Turkey, and that does not constitute an international contract, and the Board's approval for the transfer.
- ii. Companies within a group of undertakings engaged in common economic activities have obligation to comply with binding rules regarding the protection of personal data, and the Board's approval for these rules,

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 11 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

- iii. The presence of an agreement announced by the Board, that includes matters such as data categories, data transfer purposes, recipients and recipient groups, technical and administrative measures to be taken by the data recipient, and additional measures for sensitive personal data.
- iv. The preparation of a written commitment containing provisions to ensure adequate protection, and the Board's approval for the transfer.

In cases such assurances cannot be provided, personal data may only be transferred abroad if one of the following conditions is met:

1. The relevant person has been informed of the potential risks and has given explicit consent to the transfer.
2. The transfer is obligatory for the performance of a contract between the related person and the data controller or for the implementation of pre-contractual measures upon the relevant person's request.
3. The transfer is obligatory for the establishment or performance of a contract between the data controller and another natural or legal person for the benefit of the relevant person.
4. The transfer is obligatory for a superior public interest.
5. The transfer of personal data is obligatory for the establishment, use, or protection of a right.
6. The transfer of personal data is necessary for the protection of the life or physical integrity of a person who is unable to give consent due to a physical impossibility or whose consent is not legally valid,
7. The transfer is made from a registry accessible to the public or to persons with a legitimate interest, provided that the conditions required for accessing the registry in the relevant legislation are met and the person with a legitimate interest requests it.

In its processes for data transfer abroad, the Company fully complies with all obligations under Articles 8 and 9 of the Law, takes all necessary administrative and technical measures, and takes the utmost care to ensure the security of the transferred data.

2.2.4 Purposes of Transfer of Personal Data by CFN Kimya and Categories of Persons to Whom Transfers Are Made

2.2.4.1 Purposes of Data Transfer

Company carries out personal data transfers in accordance with the law within the scope of Articles 8 and 9 of the Law and transfers data for the following purposes:

- Carrying out and developing the commercial activities of the Company,
- Providing the Company with outsourced services from suppliers,
- Conducting human resources and employment policies of the Company,
- Fulfilling legal obligations and taking necessary measures within the framework of occupational health and safety,
- Effective management, auditing, and reporting of internal company operations,
- Ensuring regulatory compliance processes and fulfilling legal obligations.

2.2.4.2 Categories of Persons to Whom Data is Transferred

The Company may transfer personal data to the following categories of persons in accordance with Articles 8 and 9 of the Law:

PERSONAL DATA PROTECTION AND PROCESSING POLICY


Person Category	Description	Purpose of Data Transfer
Authorized State Institutions and Organizations	State institutions authorized to request information and documents from the Company (ministries, regulatory and supervisory authorities, judicial authorities, etc.)	Data sharing is done in order to fulfill obligations and meet legal demands in accordance with relevant legislation.
Authorized Private Legal Entities	Private law legal entities authorized to request information and documents from the Company,	Limited data sharing is done for the purposes requested within the scope of legal authorizations.
Shareholders and Partners	The Company's shareholders and partners	Data sharing is done in order to make strategic plans for the Company's commercial activities and to audit management processes.
Business Partners	Parties with which the Company collaborates in conducting its commercial activities (service providers, distributors, etc.)	Data sharing is done in order to ensure service delivery within the scope of business partnership agreements.
Suppliers	Parties from which the Company receives services in conducting its commercial activities	Data sharing is done in order to ensure the delivery of outsourced services to the Company.
Foreign or International State and Private Institutions	State or private institutions with which the Company collaborates within the framework of its international activities	Data sharing is done in order to ensure to meet the requirements of the sector in which the Company operates and to comply with international regulations.

The Company carries out personal data transfers in full compliance with the principles and rules stipulated in hereby Policy and relevant legislation, and takes all necessary technical and administrative measures to ensure data security.

A. Categories of Individuals Whose Data is Processed by the Company and the Data Processed

The individuals whose personal data is processed within the Company are categorized as follows:

Person Category	Description
Candidate Employee	Natural persons who have applied for a job with the Company through any means or submitted their resume and relevant information for review by the Company.
Employee	Natural persons who work within the Company.
Shareholder/Partner	Natural persons who are shareholders or partners of the Company.
Potential Customer/ Customer	Natural persons who are interested in the products and services offered by the Company, who have applied to benefit from these products and services, or who are deemed to be interested in them based on commercial practice and good faith.
Intern/Student	Natural persons who have completed internships or who are assigned as subject to specific training processes within the Company.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 13 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		


Supplier's Employee	Natural persons who work or serve as subcontractors in companies with which the Company has business relationships (suppliers, business partners, etc.)
Supplier's Official	Natural persons who are shareholders and officers of companies with which the Company has business relationships.
Parent/Guardian/Representative	Natural persons whose personal data is processed in capacity of parent, guardian, or representative.
Visitor	Natural persons who enter the Company's physical premises, use the hotspot service during this visit, or visit the Company's websites.
Other	Third-party natural persons whose personal data is processed within the scope of the Company's human resources processes and service operations (such as family members and relatives of employees, employees' references).

Personal data processing activities carried out by the Company are carried out in accordance with the law and for limited purposes, within the framework of the fundamental principles set forth in Article 4 of the Law.

2.3 Categorization of Personal Data by the Company

Personal data processed by the Company are evaluated within the scope of the following categories and are processed in accordance with the Law and relevant legislation:

Data Category	Description
Identity Information	Information related to an identified or identifiable natural person, such as a driver's license, identity card, residence permit, passport, work permit, attorney identity, or marriage certificate.
Contact Information	Contact information such as phone number, address, email address, and fax number.
Location Information	Data related the location of the relevant person while using Company vehicles or benefiting from certain services.
Personnel Information	All kind of data processed for the purpose of establishing and monitoring the personal rights of Company employees or natural persons who have a business relationship with the Company.
Legal Transaction and Compliance Information	Personal data processed for the purposes of establishing and monitoring legal rights and receivables, fulfilling debts, fulfilling legal obligations, and ensuring compliance with Company policies.
Customer Transaction Information	Information such as records regarding the use of services, customer requests, and instructions.
Physical Location Security Information	Data processed to ensure physical security, such as security camera recordings and visitor information regarding individuals entering and exiting the Company's premises.
Transaction Security Information	IP address, user login and logout information, access logs, and technical security data processed by the Company to ensure information security.
Risk Management Information	Information processed to manage commercial, administrative, and technical risks, obtained in accordance with legal and commercial practices.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 14 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

Financial Information	Information, documents, and records showing all types of financial results generated based on the type of legal relationship the Company has with the relevant person.
Performance and Career Development Information (Professional Experience Information)	Personal data processed for the purposes of measuring employee performance, providing career planning, and conducting human resources processes.
Internet and Transaction Security Information	Data processed in accordance with the Company's obligations to fight against crimes committed through internet access, in accordance with Law No.5651 and related legislation.
Visual and Audio Recordings	Photos, camera recordings, audio recordings, and copies of documents containing personal data. (Except for records within the scope of Physical Location Security Information)
Employee Relatives and Family Information	Information regarding employees' close and family members.
Reference Information	Information regarding individuals who serve as references for employees and job candidates.

All data processing processes carried out by the Company are carried out in accordance with the law, in line with the basic principles set out in Article 4 of the Law, for specific, clear and legitimate purposes, and unnecessary data processing activities are avoided.

PART 3: LEGAL BASIS AND PURPOSES OF PROCESSING PERSONAL DATA

3.1. Legal Basis for Processing Personal Data

3.1.1 General Principles

While the legal bases for processing personal data by the Company may vary, all personal data processing activities comply with the fundamental principles set forth in Article 4 of the Law. Accordingly, the following fundamental principles are complied with in all data processing activities conducted by the Company:

- Compliance with the law and good faith,
- Accuracy and, where necessary, up-to-dateness,
- Processing for specific, clear, and legitimate purposes,
- Relevance, limitation, and moderateness to the purpose of processing,
- Storage for the period stipulated in relevant legislation or necessary for the purpose of processing.

In this context, the following legal reasons are considered in the personal data processing processes carried out by the Company:

3.1.2 Reasons for Compliance with Law


A. Having Explicit Consent of the Relevant Person

Explicit consent of the relevant person may be required for the processing of personal data. Explicit consent is an informed-based and freely given declaration of consent regarding a specific matter.

B. Being Clearly Foreseen in Laws

Processing of personal data is considered lawful in case there is a clear adjustment in the relevant legislation stipulating that personal data will be processed.

For example: Reporting employee identification information to the relevant official authorities in accordance with the Identity Notification Legislation.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 15 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

C. Failure to Obtain Explicit Consent of the Relevant Person Due to a Factual Impossibility

If processing of personal data is required to protect the life or physical integrity of persons who are unable to give their consent due to a factual impossibility or whose consent is not legally recognized, the personal data of the relevant person may be processed.

For example: Sharing the blood type information of an unconscious employee with healthcare personnel in a situation that require urgent medical intervention.

D. Being Directly Related to the Establishment or Performance of a Contract

Processing personal data belonging to the parties to a contract may be necessary if it is directly related to the establishment or performance of a contract.

For example:

- *Requesting CVs from job applicants,*
- *Processing personal data for the purpose of establishing a contract between the parties during sales and supply processes.*

E. Company's Fulfilling Its Legal Obligations

The Company may process personal data to fulfill its legal obligations arising from the laws.

For example:

- *Storing employee payroll information in accordance with tax legislation,*
- *Reporting employee information to the relevant institution under Social Security Institution (SSI) legislation.*

F. Relevant Person's Making His/Her Personal Data Public

If the relevant person has made his/her personal data publicly accessible, this data may be processed.

For example:

- *Customers sharing complaints about the Company's products and services on a public platform,*
- *Job applicants publishing their resumes on public professional platforms such as LinkedIn.*

G. The Fact That Data Processing Is Necessary to Establish, use, or Protect a Right

If processing personal data is necessary to establish, use, or protect a right, the relevant person's data may be processed.

For example:

- *Company's Preserving sales contracts and invoices for the to defend its legal rights,*
- *Using employee records as legal evidence in disputes arising from employment contracts.*


H. ata Processing Is Necessary for the Company's Legitimate Interest

Personal data may be processed if data processing is necessary to protect the Company's legitimate interests, provided that it does not harm the fundamental rights and freedoms of the relevant person.

For example:

- *Using closed circuit security camera systems (CCTV) to ensure security in the company premises,*
- *Implementing cyber security measures on company computers,*
- *Performing specific data analyses to ensure the Company's business continuity.*

The Company processes personal data only for the legal reasons stipulated in the Law, conducts its data processing activities in accordance with the law, and adopts a transparent approach. All processes related to the processing of personal data are also supported by the Company's POL.020 Personal Data Storage and Disposal Policy.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 16 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

3.1.3 Processing of Sensitive Personal Data and Compliance with Law


In case the relevant person does not give explicit consent, the Company may process sensitive personal data only in cases prescribed by law, provided that adequate measures are taken, as determined by the Board. Sensitive personal data concerning the relevant person's health and sexual life may only be processed by persons under a confidentiality obligation or by authorized institutions and organizations for the purposes of protecting public health, providing preventive medicine, medical diagnosis, providing treatment and care services, and planning and managing healthcare services and their financing. Regardless of the reason, general data processing principles are always considered in processing processes, and it is ensured compliance with these principles (Article 4 of the Law; see above, Part 2.1.1).

3.2 Purposes of Processing Personal Data

The Company processes personal data in accordance with the personal data processing conditions specified in Article 5, paragraph 2, and Article 6, paragraph 3, of the Law, and only within the framework of its legal bases. In data processing processes, the general principles set forth in Article 4 of the Law are observed, and personal data processing activities are carried out in accordance with the law. Unless there are other legal reasons, data processing activities are carried out with the explicit consent of the relevant person. Explicit consent must be specific to a matter, informed-based, and expressed with free will.


Personal data is processed within the Company specifically for the following **purposes**:

- In order to fulfill our mutual obligations arising from the employment contract, the employer must process the personal data of EMPLOYEES AND INTERNS (in a broad sense, defined as employees) and their PARENTS/GUARDIANS. Employees' personal data is processed and stored in accordance with the law and the rules of good faith, in an accurate and, where necessary, up-to-date manner; for specific, clear, and legitimate purposes; and in a purpose-related, limited, and moderate manner. In this context, in line with the purposes necessary to ensure that employees are employed in compliance with the law. the legal basis for personal data processing consists of the carrying out the processes of establishment, execution, and termination of employment contracts in compliance with the law; the legitimate interests of the Company, situations explicitly stipulated by law, fulfillment of legal obligations related to employee employment; situations where data processing is necessary for the establishment, use, and protection of rights in legal proceedings; and in other cases, and the express, informed, and freely given consent of employees to be requested from employees provided that they do not violate fundamental rights and freedoms.
- Within the scope of the activities required by the Company's field of activity, the employer's legitimate interests require the processing of employees' personal data. Thus, processing of employees' personal data may be carried out for reasons such as preventing abuse, preventing theft, ensuring general security, or ensuring occupational health and safety. However, in such cases, great care is taken to ensure that the fundamental rights and freedoms of employees are not violated.
- In case employees' race, ethnic origin, political opinions, philosophical beliefs, religion, sect, or other beliefs, as well as dress are not included in the personal data processed unless expressly stipulated by law, and If an exceptional practice is to be implemented, the requirements are carefully evaluated before processing personal data, and explicit consent is obtained from the relevant person. The Company conducts audits and surveillance activities on information and communication tools (telephones, mobile devices, computers, and internet access), and these

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 17 / 23
<h3>PERSONAL DATA PROTECTION AND PROCESSING POLICY</h3>		

activities have a legal basis within the scope of Law No.5651, relevant legislation, and the Company's legitimate interests.

- Security cameras may be used in Company facilities or office areas to ensure security, maintain work discipline, and manage business processes more effectively. Visitor records may be kept and access control systems may be operated within this scope.
- Vehicle tracking systems are used on company vehicles for operational efficiency, security, and the protection of employees. These activities are carried out in accordance with the Company's legitimate interests and are carried out in a manner that does not violate the fundamental rights and freedoms of data owners.
- Personal data of **EMPLOYEE RELATIVES AND FAMILY MEMBERS** is also processed in connection with emergency contact and communication (for example, notification in case of an accident), fulfillment of legal obligations such as minimum living allowances, and for employee relations processes.
- In accordance with the Labor Law No.4857, the Code of Obligations No.6098, Article 419, Law No 6698 on the Protection of Personal Data and relevant legislation, the Company may process personal information of **EMPLOYEE CANDIDATES** such as their name, address, date of birth, e-mail address, telephone number and other contact details, resume, cover letter, past or relevant work experiences or other experiences, educational status, transcript, language test results or supporting or explanatory documents related to the job application, records of information obtained during the interview in case of a face-to-face interview or interview via means such as video conference, telephone, and the references you have specified in the job application. Within the scope of candidate employment, it is strongly recommended that candidates refrain from providing any personal information not directly related to their qualifications, and particularly any sensitive data (such as race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance, association, foundation or union membership, health, sexual life, criminal convictions and security measures, and biometric and genetic data), and It is also strongly recommended that relevant parts of written CVs and documents be blackened and then submitted to the Company. Furthermore, any **PERSONAL DATA** (name, surname, telephone number, email, etc.) of **REFERENCE PERSON(S)** included in the candidate's CV and whose data is processed during this process must be informed of the relevant person(s) and submitted to the Company, with the understanding that it is the candidate's responsibility to obtain their explicit consent.
- Our Company also processes the personal data of **SUPPLIER/SUB-EMPLOYER OFFICIALS AND EMPLOYEES** in accordance with the Law. Thus, Occupational Health and Safety Law No.6331 specifies the documents and information that must be checked by the primary employer regarding employees coming from another workplace regarding occupational health and safety. Similarly, Labor Law No.4857 and Social Security and General Health Insurance Law No.5510 impose obligations on the primary employer regarding subcontractor workers and temporary workers, and specify the matters that must be checked within this scope. Accordingly, the processing of personal data of employees working for suppliers and other employers is based on the Company's legitimate interests, primarily the requirements of these legal regulations and the fulfillment of legal obligations. Also, the data of **PERSONS PURCHASING PRODUCTS/SERVICES OR THEIR OFFICIALS** is processed within the scope of the commercial activity and legal relationship with the relevant person.
- Our Company implements **CAMERA SURVEILLANCE ACTIVITIES AND VISITOR REGISTRATION SYSTEMS** in workplaces for occupational health and safety, general security, and product safety purposes. These activities are carried out in accordance with the Law and relevant legislation and are carried out within the framework of our Company's legitimate

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 18 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

interests. Camera surveillance activities are limited to the purposes of ensuring physical space security, ensuring the safety of employees and visitors, protecting Company assets and business processes, and preventing theft, workplace accidents, and other security risks. Necessary technical and administrative measures are taken during the collection and storage of camera recordings to prevent violations of the fundamental rights and freedoms of the relevant individuals, and these activities are carried out within the framework of the principle of transparency. On the other hand, visitor registration processes are carried out in accordance with our Company's security procedures to prevent unauthorized access and ensure the complete implementation of occupational health and safety measures. Visitor identification information and entry and exit records are processed only for specified security purposes and are destroyed at the end of the storage periods stipulated in the legislation, in accordance with PR.049 Asset Management Procedure.

Our company processes personal data for the purposes specified above in accordance with the general principles set forth in Article 4 of the Law and ensures data security by taking the necessary technical and administrative measures.

PART 4: STORAGE, DELETION, DESTRUCTION, AND ANONYMIZATION OF PERSONAL DATA

Although the Company has processed personal data in accordance with the relevant legal provisions, as regulated in Article 138 of the Turkish Penal Code and Article 7 of this Law, if the reasons requiring processing no longer exist, personal data will be deleted, destroyed, or anonymized based on the Company's own decision or upon the request of the relevant person.

4.1 Storage and Storage Periods of Personal Data

CFN Kimya primarily stores personal data for the period specified in relevant laws and legislation, if stipulated in relevant legislation. If legislation does not specify the period for which personal data must be stored, storage periods are determined by considering any period of limitations/period of prescription that may apply within the scope of the legal relationship with the relevant person. Regarding the Storage of Personal Data, PR.049 Asset Management Procedure has been put into effect, and detailed storage periods are specified.


4.2 Deletion, Destruction, and Anonymization of Personal Data

As regulated in Article 138 of the Turkish Penal Code and Article 7 of the Law, if the reasons requiring processing are no longer exist despite processing in accordance with the relevant legal provisions, CFN Kimya deletes, destroys, or anonymizes personal data at its own discretion or upon the request of the relevant person. In this context, CFN Kimya fulfills its obligations through the methods described in this part.

4.2.1 Deletion of Personal Data

A. Transaction of Deletion of Personal Data

Although processed in accordance with relevant legal provisions, the Company may delete personal data at its own discretion or upon the request of the relevant person if the reasons requiring processing no longer exist. Deletion of personal data is the process of making personal data inaccessible and non-reusable for the relevant users. The Company takes all necessary technical and administrative measures to ensure that deleted personal data is inaccessible and non-reusable for the relevant users.

	<h1>Policy</h1>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 19 / 23
<h2>PERSONAL DATA PROTECTION AND PROCESSING POLICY</h2>		

B. Personal Data Deletion Process

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

- Identifying the personal data that will be subject to deletion.
- Identifying the relevant users for each personal data item by using an access authorization and control matrix or similar system.
- Identifying the relevant users' authorizations and methods for access, retrieval, and reuse.

The closure and elimination of the relevant users' access, retrieval, and reuse authorizations and methods for personal data.

4.2.2 Destruction of Personal Data

A. Destruction of Personal Data

The Company may destroy personal data at its own discretion or upon the request of the relevant person, even if the reasons requiring processing are no longer exist. Destroying personal data is the process of making personal data inaccessible, irretrievable, and reusable by anyone. The Company takes all necessary technical and administrative measures for the destruction of personal data.

B. Methods for Destroying Personal Data

In order to destroy personal data, all copies of the data are identified, and the systems containing the data are destroyed individually.

4.2.3 Anonymizing Personal Data


A. Transaction of Anonymizing Personal Data

Anonymizing personal data means making personal data incapable of being associated with an identified or identifiable natural person, even by matching it with other data. Our company may anonymize personal data processed in accordance with the law when the reasons requiring processing are no longer exist. The company takes all necessary technical and administrative measures to anonymize personal data.

Personal data anonymized in accordance with Article 28 of the Law may be processed for purposes such as research, planning, and statistics. Such processing is outside the scope of the Law, and the explicit consent of the relevant person will not be required.

B. Methods of Anonymizing Personal Data

Anonymization is the removal or modification of all direct and/or indirect identifiers in a dataset, preventing the identification of a specific individual or making it indistinguishable from a group or through the crowd Data that does not identify a specific individual as a result of these features being removed or lost is considered anonymized. The purpose of anonymization is to break the link between the data and the individual that it identifies. All link-breaking processes, whether automatic or non-automatic, implemented through methods such as grouping, masking, derivation, generalization, and randomization, applied to records in the data recording system where personal data is stored are called anonymizing methods. The data obtained by applying these methods must be incapable of identifying a specific person.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 20 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

PART 5: RIGHTS OF RELEVANT PERSONS

5.1 Scope of Rights of Relevant Persons and Use of These Rights

5.1.1 Rights of Relevant Persons

The persons whose personal data is processed by the Company have the following rights:


- To learn whether personal data is processed or not,
- To ask for information about it if it has been processed,
- To learn the purpose of processing personal data and whether they are used in accordance with the purpose,
- To know the third parties to whom the data is transferred in the country or abroad,
- To request correction of personal data in case of incomplete or incorrect processing and to request that the transaction carried out in this context be notified to third parties to whom personal data has been transferred,
- To request the deletion or destruction of personal data in case the reasons requiring processing no longer exist, even though it has been processed in accordance with the law and other relevant legal provisions, and requesting that the action taken in this context be notified to third parties to whom personal data has been transferred,
- To object to the appearance of a result against himself/herself due to that the processed data has been analyzed only through automatic systems,
- To demand the compensation for his/her damage in case of suffering damage due to that the personal data has been processed illegally.

5.1.2 Use of Rights by Relevant Persons

It is necessary and sufficient for relevant persons to submit their requests to use their rights specified above, as per Article 13, paragraph 1 of the Law, to our Company by choosing one of the following methods and addresses:

Method of Application	Address to Application	Information to be Stated While Submitting the Application
Application in Person (The applicant must come in person and apply with a document proving his/her identity)	Demirciler OSB Mah. Murat Yildiran Cad. No: 3/3 Dilovasi/Kocaeli	" <i>Information Request Within the Scope of the Personal Data Protection Law</i> " will be written on the envelope.
Notification via Notary Public	Demirciler OSB Mah. Murat Yildiran Cad. No: 3/3 Dilovasi/Kocaeli	" <i>Information Request Within the Scope of the Personal Data Protection Law</i> " will be written on the notification envelope.
Via Registered Electronic Mail (KEP) by signing with Secure Electronic Signature	kvkk@cfnkimya.com	" <i>Personal Data Protection</i> " will be written in the subject section of the e-mail.

For a fast and efficient evaluation of applications, one of the aforementioned methods must be used. Our company will act in accordance with the Law and relevant legislation during the evaluation and response of applications.

	Policy	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 21 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

In application;

The application must include your name, surname, and signature if the application is in writing; your Turkish Identity Number (T.R.ID) for Turkish citizens; your nationality, passport number or ID number (if applicable) for foreigners; your residence or workplace address for notification; your email address, telephone and fax numbers, and the subject of the request. Relevant information and documents must also be included in the application.

It is not possible for third parties to submit a request on behalf of the relevant person. For a person other than the relevant person to submit a request, a special power of attorney must be issued by the relevant person to the person making the application. The application must include explanations of the rights demanded to be used as the relevant person; the requested matter must be clear and understandable; the matter requested is related to the relevant person or, if acting on behalf of someone else, you must be specifically authorized to do so and document this authorization; the application must include your identity and address; and documents verifying your identity must be enclosed to the application. The Relevant Person Application Form is available on CFN Kimya's website.

5.1.3 Responding to Applications


In case the relevant person submits his/her request to the Company in accordance with the prescribed procedure, the Company will process the 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 process requires additional costs, the Company will charge the applicant the fee determined by the Board. The Company may request information from the relevant person to determine whether the applicant is the relevant person. The Company may ask the relevant person questions regarding the application to clarify the matters included in the application.

PART 6: ENSURING THE SECURITY OF PERSONAL DATA

6.1 Technical and Administrative Measures Taken to Ensure Processing of Personal Data in Compliance with Law

The Company takes all necessary technical and administrative measures to ensure the legal processing of personal data and continuously conducts improvement efforts in this regard. Accordingly, the following measures are implemented:

- The Company fully and accurately fulfills its obligation to inform all relevant persons with whom it interacts, as per Article 10 of the Law.
- Company employees are regularly informed and trained on personal data protection legislation and data security. Periodic training sessions are organized to raise employee awareness on this issue, and guide documents are provided.
- The activities carried out across all of the Company's business units are analyzed in detail, and the necessary measures are taken to ensure that personal data processing processes comply with the Law and relevant legislation.
- In order to ensure that the Company's personal data processing activities comply with the personal data processing requirements stipulated in the Law, specific requirements are determined for each business unit, and business processes are organized according to this.
- The contracts and documents managing the legal relationship between the Company and its employees include provisions stating that the employees are required to process personal data only in accordance with the Company's instructions and within the scope of relevant legislation, and this obligation puts employees under obligation not to process, disclose, or misuse personal data. Regular audits are conducted to ensure employee compliance with these obligations.

	<h2>Policy</h2>	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 22 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

- Contracts signed between the Company and third parties with whom it has business relationships (suppliers, service providers, etc.) include commitments and obligations regarding the processing, protection, and confidentiality of personal data. This provides the necessary assurance to prevent unauthorized processing and disclosure of personal data.
- The Company continuously reviews and updates its technical and administrative measures to ensure personal data security.

6.2 Technical and Administrative Measures Taken in the Processing of Sensitive Personal Data


The Company shows maximum sensitivity in protecting personal data designated as "sensitive" by law and processed in accordance with the law. Sensitive personal data includes data related to race, ethnicity, political opinions, philosophical beliefs, religion, sect or other beliefs, dress, membership in associations, foundations, or unions, health, sexual life, criminal convictions, and security measures, as well as biometric and genetic data.

The Company takes all technical and administrative measures stipulated in the Law and relevant legislation when processing sensitive personal data, and implements high-level protection mechanisms to ensure the security of this data. In this context, the technical and administrative measures implemented by the Company are meticulously implemented to protect sensitive personal data and are regularly audited.

In this respect, PR.0112 for the Processing of Sensitive Personal Data Procedure has been implemented regarding the security and processing principles of sensitive personal data.

6.2.1.1 Technical Measures Taken to Store Personal Data in Secure Environments

- The Company implements various administrative measures to prevent unlawful access to personal data. Employees are regularly trained on personal data security, and awareness campaigns are conducted. Employees are informed that they will not unlawfully disclose personal data that they learn during their work processes or use it for purposes other than those intended for processing, and they are also required to undertake in writing that these obligations will continue after they leave their duties. Furthermore, the Company's data security policies and procedures are regularly reviewed, necessary controls are implemented, and action plans are developed to resolve any identified deficiencies.
- Processed Personal Data is stored in accordance with the storage periods specified in relevant legislation, ensuring that it is accurate, up-to-date, and fit for purpose. Data, the intended use of which ends or which is out-of-date is regularly reviewed and deleted, destroyed, or anonymized in accordance with the Company's current personal data storage and destruction policy. Furthermore, when receiving services from data processors, the Company ensures that these service providers keep providing at least the same level of security as the Company itself regarding the protection of personal data, and in this context, additional obligations regarding the protection of personal data are added to contracts with data processors, ensuring that these obligations are clearly defined and monitored through regular audits.

	Policy	Policy No: POL.021
		Revision No: 0
		Approval date: 25.02.2024
		Page No: 23 / 23
PERSONAL DATA PROTECTION AND PROCESSING POLICY		

6.2.1.2 Measures to be Taken in Case of Unauthorized Disclosure of Personal Data

- In accordance with Article 12 of the Law, the Company operates systems to promptly notify the relevant parties and the Board in case personal data is obtained by unauthorized persons or processed unlawfully.
- When a data breach is detected, technical and administrative measures are immediately taken to minimize risks depending on the nature of the incident.
- Security policies and data processing processes are reviewed and necessary revisions are made in order to prevent the recurrence of unauthorized disclosures.