KİMYAPSAN KİMYA ve YAPIŞTIRICI SANAYİ A.Ş.

PERSONAL DATA PROCESSING,

PROTECTION and DESTRUCTION POLICY

DOCUMENT NAME:

"Kimyapsan Kimya ve Yapıştırıcı Sanayi A.Ş. Personal Data Processing, Protection and Destruction Policy"

EFFECTIVE DATE:

02/09/2020

1. PURPOSE and SCOPE

This **"Kimyapsan Kimya ve Yapıştırıcı Sanayi A.Ş. Personal Data Processing, Protection and Destruction Policy"** ("Policy") has been prepared in order to determine the procedures and principles regarding the business and transactions regarding the personal data processing, storage and destruction activities carried out by "**KİMYAPSAN KİMYA ve YAPIŞTIRICI SANAYİ A.Ş." ("KİMYAPSAN A.Ş.").**

This policy applies to the processing of personal data of employees, employee candidates, shareholders, suppliers, visitors, product / service recipients and other relevant third parties within the scope of the Personal Data Protection Law No. 6698 ("**PDPL**").

2.DEFINITIONS

Explicit Consent: Consent on a specific subject, based on information and expressed with free will.
Recipient Group: The category of natural or legal person to whom personal data is transferred by the Data Controller.
Anonymization: Making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data.
Disclosure Obligation: These are the matters that the data controller is obliged to provide the information to the person concerned personally or through the person authorized by him during the acquisition of personal data within the framework of Article 10 of PDPL.
Employee: Persons employed by the company based on an employment contract.
Employee Candidate: A natural person who makes his/her resume and related information accessible to the Company by applying for a job or by any other means.
Shareholder: A person or organization that legally owns shares in a public or private company.
Relevant Person: An identified or identifiable natural person to whom the data belongs.
Destruction : The deletion, destruction or anonymization of personal data.
Law: Law No. 6698 on the Protection of Personal Data (PDPL).
Recording Medium: Any medium in which personal data processed by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system.
Personal Data Processing Inventory: It is the inventory in which the personal data processing activities carried out by the data controller depending on the business processes, personal data processing purposes, data category, transferred recipient group and person concerned group are detailed by explaining the maximum time required for the purposes for which personal data are processed, personal data foreseen to be transferred to foreign countries and the measures taken regarding data security.

Personal Data: Means any information relating to the person concerned, such as name, address, telephone number, e-mail address or similar identification information.

Processing of Personal Data: It refers to all kinds of operations performed on personal data such as obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic or non-automatic means provided that it is part of any data recording system.

Deletion of Personal Data: It is the process of making personal data inaccessible or non-reusable in any way for the relevant users.

Destruction of Personal Data: It is the process of making personal data inaccessible, unrecoverable and unusable by anyone in any way.

PDPL: Personal Data Protection Law

Board: Personal Data Protection Board

Institution: Personal Data Protection Authority

Customer: Natural persons whose personal data are obtained due to business relations within the scope of the activities carried out by the company, regardless of whether there is any contractual relationship.

Special Categories of Personal Data: Data relating to a person's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

Periodic Destruction: It is the process of deletion, destruction or anonymization to be carried out ex officio at recurring intervals specified in the personal data storage and destruction policy in the event that all of the conditions for processing personal data specified in the Law disappear.

Third Parties: Other natural persons, including but not limited to suppliers, victims, family members, etc., whose personal data are processed within the framework of this Procedure, although not defined in the Procedure.

Supplier Official: Officials affiliated with real or legal persons who provide inputs, raw materials, products to the company in order to provide a product or service.

Supplier Employee: Employees of natural or legal persons who provide inputs, raw materials or products to the company in order to provide a product or service.

VERBIS: Data Controllers Data Registry Information System

Data Processor: A natural or legal person who processes personal data on behalf of the data controller based on the authorization granted by the data controller.

Data Controller: 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.

Visitors: Real persons who physically enter the areas belonging to the company for various purposes or visit the websites.

3. PROCESSING OF PERSONAL DATA

Article 3 of the PDPL defines the concept of "*processing of personal data",* Article 4 states that the personal data processed must be "*relevant, limited and proportionate to the purpose for which they are processed and retained for the period stipulated in the relevant legislation* or required for the purpose for which they are processed", and Articles 5 and 6 list the "conditions for processing personal data".

4. GENERAL PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

Pursuant to Article 4 of PDPL, personal data may be processed by our data controller company ("KİMYAPSAN A.Ş.") only in accordance with the procedures and principles stipulated in this Law and other laws.

The following are requirements for the processing of personal data by the data controller:

a. Compliance with the law and honesty rules,
b. Being accurate and up-to-date when necessary,
c. Processing for specific, explicit and legitimate purposes,
d. Being relevant, limited and proportionate to the purpose for which they are processed,
e. comply with the general principles set out in the relevant legislation or retained for the period required for the purpose for which they are processed.

5. CONDITIONS FOR PROCESSING PERSONAL

Personal data cannot be processed by the data controller company **("KİMYAPSAN A.Ş.")** without the explicit consent of the relevant person. In order for personal data to be processed and used in accordance with this policy, the Personal Data Protection Law and secondary legislation, the relevant person must be informed about the processing activities, permission must be requested for the processing of personal data and the explicit consent of the person concerned must be obtained. In this context, action will be taken based on the documents created by **("KİMYAPSAN A.Ş.")** for the declaration of clarification and explicit consent.

Pursuant to Article 5 of the PDPL, the requirement to obtain explicit consent from the person concerned should not apply if one of the following exceptions applies:

a. This being clearly stipulated in the Laws
b. It being mandatory for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid.

c. Provided that it is directly related to the establishment or performance of a contract, this being necessary to process the personal data of the parties to the contract.
d. This being mandatory for the data controller to fulfill its legal obligation.
e. This being been made public by the person concerned himself/herself,
f. Data processing being mandatory for the establishment, exercise or protection of a right,
g. Data processing being mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the person concerned.

6. PERSONAL DATA OF SPECIAL NATURE

Pursuant to Article 6 of the PDPL, certain personal data, which, when processed unlawfully, may cause victimization or discrimination, are designated as "special categories". Personal data of special nature includes data relating to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data.

7. RULES TO BE FOLLOWED IN THE PROCESSING OF PERSONAL DATA OF SPECIAL NATURE

It is prohibited for the data controller to process personal data of special nature without the explicit consent of the data subject.

If there is no explicit consent of the personal data owner, personal data is processed in the following cases:

- Personal data of special nature, other than the health and sexual life of the personal data subject, are processed in cases stipulated by law
- Personal data of special nature relating to the health and sexual life of the personal data owner is processed only by persons or authorized institutions and organizations under the obligation of confidentiality for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing.

The "**Policy on Processing and Protection of Personal data of special nature"** has also been issued by the data controller in order to determine the procedures and principles regarding the processing of special categories of personal data.

8. OBLIGATION TO DISCLOSE

Pursuant to Article 10 of PDPL, during the acquisition of personal data, the company ("**KİMYAPSAN A.Ş.")** or the person authorized by it as the data controller is obliged to provide information to the relevant persons on the following issues:

a. Identity of the data controller and its representative, if any,
b. The purpose for which personal data will be processed,
c. To whom and for what purpose the processed personal data may be transferred,

d. The method and legal reason for collecting personal data,
e. Other rights listed in Article 11 of the PDPL,

In the fulfillment of the disclosure obligation by the data controller, the matters set out in the "*Communiqué on the Procedures and Principles to be followed in the Fulfillment of the Disclosure Obligation*" must be complied with.

9. CATEGORIES OF PERSONAL DATA

Criminal Convictions and Security Measures: Information such as criminal record, court decree, etc.

Other Information: Information such as family relative information, vehicle information, audit and inspection information, request complaint information, purchase transaction information

Financial Information: Personal data processed regarding information, documents and records showing all kinds of financial results created according to the type of legal relationship established with the personal data owner and data such as bank account number, IBAN number, income information, debt / receivable information

Physical Space Security Information: Personal data related to the records and documents taken at the entrance to the physical space, during the stay in the physical space, information such as camera records, vehicle information records and records taken at the security point

Audio and Visual Records: Information such as photos, videos, audio recordings

Legal Process Knowledge: Information in correspondence with judicial authorities, information in case file

Contact Information: Information such as phone number, address, e-mail address

Process Security Information: Information such as log records, IP information, authentication information, passwords, passphrases

Transaction Information: Information such as survey information, declaration information, shopping information, call center records, membership information, which is processed within the framework of the activities carried out by the company, related to the services provided or in order to protect the legal and other interests of the company and the personal data owner

Identity Information: Data containing information about the identity of the person, name-surname, Turkish ID number, nationality, place of birth, date of birth, gender, workplace information, registration no., tax number, title, biography, etc. and information such as driver's license, professional ID, identity card and passport

Location Information: Real-time location information tracking via cell phone, real-time location information tracking via computer/tablet, vehicle tracking system

Professional Experience Information: Information such as the company where the relevant person works, duration of employment, type of insurance, sector of employment, title, level of education, total working time

Customer Transaction: Order information, request information, etc.

Sensitive Personal Data: Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, sexual life, criminal convictions and security measures, genetic data, criminal convictions and security measures information, biometric data, genetic data information

Personnel Information: Payroll information, disciplinary investigation, employment records, resume information, performance evaluation reports, etc.

Marketing Information: Shopping history information, etc.

Health Information: Information on disability status, blood type information, personal health information, information on devices and prostheses used, health report, employment periodic examination form, psychotechnical certificate/report, etc.

Request/Complaint Information: Personal data regarding the receipt and evaluation of any request or complaint addressed to the data controller

10. LEGAL REASONS FOR PROCESSING AND STORING PERSONAL DATA

Personal data processed within the framework of business activities are processed and stored in accordance with the periods stipulated in the relevant legislation. In this context, personal data must be clearly stipulated in the Personal Data Protection Law No. 6698, Labor Law No. 4857, Occupational Health and Safety Law No. 6361, Social Security and General Health Insurance Law No. 5510, Turkish Code of Obligations No. 6098, Turkish Commercial Code No. 6102, Consumer Protection Law No. 6502, Regulation on Health and Safety Measures to be Taken in Workplace Buildings and Annexes and other laws, and provided that the data controller can fulfill its legal obligation specified in Articles 5 and 6 of the PDPL and provided that it does not harm fundamental rights and freedoms, data processing is mandatory for the legitimate interests of the data controller, secondary regulations in force within the scope of personal data processing conditions (legal reasons) and limited to these, Personal data are stored and processed for the retention periods stipulated in accordance with the legislation and administrative regulations that the data controller must comply with.

11.KİŞİSEL VERİLERİ İŞLEME AMAÇLARI

Personal data is processed for the following purposes: To fulfill our obligations specified in the Personal Data Protection Law No. 6698, Labor Law No. 4857, Social Security and General Health Insurance Law No. 5510, Occupational Health and Safety Law No. 6331, Turkish Commercial Code No. 6102, Turkish Code of Obligations No. 6098 and secondary regulations issued under the above-mentioned laws, Execution of emergency management processes, execution of information security processes, execution of application processes of employee candidates, fulfillment of employment contractual and regulatory obligations for employees, Conducting fringe benefits and benefits processes for employees, conducting audit/ethics activities, conducting training activities, execution of access authorizations, execution of activities in accordance with the legislation, conducting financial and accounting affairs, ensuring the security of physical space, carrying out assignment processes, follow-up and execution of legal affairs, conducting internal audit/investigation/intelligence activities,

conducting communication activities, planning of human resources processes, execution/supervision of business activities, conducting occupational health/safety activities, carrying out activities to ensure business continuity, receiving and evaluating suggestions for the improvement of business processes, execution of logistics activities, conducting performance evaluation processes, execution of customer relationship management processes, carrying out storage and archive activities, execution of contract processes, follow-up of requests/complaints, ensuring the security of movable property and resources, execution of supply chain management processes, execution of the remuneration policy, execution of product/service procurement processes, execution of product/service sales processes, execution of product/service after-sales support services, execution of marketing processes of products/services, carrying out production activities of products/services, informing authorized persons, institutions and organizations, execution of management activities, creation and follow-up of visitor records

12. METHODS OF COLLECTING PERSONAL DATA

Your personal data may be collected through electronic and/or physical media by filling out forms, website, data integration, fax, short message (SMS), encrypted corporate e-mail, registered electronic mail (KEP) account. In addition, your personal data will be collected within the scope of personal data processing conditions (legal reasons), except for explicit consent, provided that it is clearly stipulated in the laws as specified in Articles 5 and 6 of the Law, that the data processing is mandatory for the legitimate interests of the data controller, provided that the data controller can fulfill its legal obligation and does not harm your fundamental rights and freedoms.

13. METHODS OF STORING PERSONAL DATA

Personal data are securely stored in accordance with the law in the environments determined by the data controller company **("KİMYAPSAN A.Ş.")**

Electronic media, servers, software, information security devices (firewall, intrusion detection and prevention, logging file, antivirus, etc.) personal computers (desktop, laptop), mobile devices (phone, tablet, etc.), optical disks (CD, DVD, etc.), removable memories (USB, memory card, etc.) printer, scanner, copier, software, firewall, intrusion detection and prevention system, antivirus, logging, cloud storage systems, personal computers, mobile phones, tablets, optical disks (CD, DVD, etc.).) printers, scanners, copiers, software, firewalls, intrusion detection and prevention systems, antivirus, logging, cloud storage systems, personal computers, mobile phones, tablets, optical disks, camera recording systems, voice recording systems, printers, copiers, scanners

Non-electronic media, forms, documents, visitor log books and other documents

14. ADMINISTRATIVE AND TECHNICAL MEASURES TAKEN BY THE DATA CONTROLLER TO PROTECT PERSONAL DATA

Within the scope of Article 12 of the PDPL, technical and administrative measures are taken by the data controller in accordance with the Personal Data Protection Law and within the framework of adequate measures determined and announced by the Personal Data Protection Board in order to store personal data securely, to prevent unlawful processing and access and to destroy personal data in accordance with the law.

14.1. ADMINISTRATIVE MEASURES

- Training and awareness raising activities on data security are carried out at regular intervals for employees.
- Authorization matrix has been created for employees.
- Confidentiality undertakings have been made.
- The authorizations of employees who change their duties or leave their jobs are removed.
- Signed contracts have been harmonized with the Personal Data Protection Law.
- Extra security measures are taken for physically transferred personal data.
- Personal data security is monitored.
- Necessary security measures are taken for entry and exit to and from physical environments containing personal data.
- Physical environments containing personal data are secured against external risks (fire, flood, etc.).
- Personal data is minimized as much as possible.
- Personal data is backed up and the security of backed up personal data is ensured.
- Access to personal data is limited only to those employees who are required to access this information during the performance of their duties.
- Physical access to files containing personal data is restricted as necessary and appropriate.
- When the Company becomes aware of incidents and situations such as unauthorized access to personal data or improper use of personal data, these are immediately reported to the data controller.

- Before using personal data for a purpose other than the first stated purpose, the obligation to obtain explicit consent from the person concerned in accordance with the Data Protection Legislation and to inform about the subject of processing is fulfilled.
- Internal periodic and/or random audits are conducted or commissioned.
- Data processing service providers are periodically audited on data security.
- In order to improve the quality of employees, trainings are provided on preventing unlawful processing of personal data, preventing unlawful access to personal data, and ensuring the protection of personal data.
- "Personal Data Processing Inventory" has been prepared.
- Internal periodic and random audits are conducted.
- Information security trainings are provided for employees.
- "Clarification Text", "Explicit Consent Text", "Confidentiality and Personal Data Protection Agreement" were signed by the data controller.

14.2. <u>TECHNICAL MEASURES</u>

- Network security and application security are ensured.

- Closed system network is used for personal data transfers through the network.

- Information systems are kept up-to-date and strong passwords are used in electronic media where personal data are processed.

- Necessary measures are taken for the physical security of information systems equipment, software and data.

- The security of personal data stored in the cloud is ensured.

- There are disciplinary regulations that include data security provisions for employees.

- Training and awareness raising activities on data security are carried out for employees at regular intervals.

- Hardware (access control system allowing only authorized personnel to enter the system room, 24/7 monitoring system, fire extinguishing system, air conditioning system, etc.) and software (firewalls, intrusion prevention systems, network access control, malware prevention systems, etc.) measures are taken to ensure the security of information systems against environmental threats.

- Access to personal data stored in electronic or non-electronic media is restricted according to access principles.

- Procedures are established and implemented for access authorization and role distribution, and an authorization matrix is applied.

- Accesses are recorded and inappropriate accesses are kept under control, and destruction processes are defined and implemented in accordance with the retention, storage and destruction policy.

- Corporate policies on the use, storage and destruction of personal data have been prepared and implemented.

- Confidentiality undertakings are made.

- The authorizations of employees who change their duties or leave their jobs in this area are removed.

- Up-to-date anti-virus systems are used.

- Security vulnerabilities are monitored and appropriate security patches are installed.

- Secure record keeping (logging) systems are used.

- Risks to prevent unlawful processing are identified and technical measures are taken in accordance with these risks.

- In case of detection of unlawful processing, a system and infrastructure is established to notify the relevant person and the board.

- Cryptographic methods are used in the electronic environment where personal data of a special nature are processed, cryptographic keys are kept in secure environments, transaction records are logged, security tests are regularly performed, if transfer via e-mail is required, encrypted corporate e-mail or cap is used, and transfer between servers is carried out by SFTP method.

- In addition to the technical measures taken for personal data, policies and procedures for the security of special categories of personal data are determined. Access authorization and role distribution are clearly defined.

- Backup programs that ensure the secure storage of personal data are used.

- Strong passwords are used in electronic media where personal data are processed.

- Destruction processes are defined in accordance with the retention and destruction policy.

15. PRINCIPLES FOR DATA SECURITY

Our Company **("KİMYAPSAN A.Ş.")** has taken all necessary technical, legal and administrative measures to ensure the appropriate level of security in order to prevent unlawful processing and access to personal data and to ensure its protection. If personal data is processed by another natural or legal person on its behalf, it is responsible for taking measures to prevent unlawful processing and access to personal data and to ensure its protection.

In the event that personal data processed by our Company **("KİMYAPSAN A.Ş.")** is obtained by others through unlawful means, our Company (**"KİMYAPSAN A.Ş.")** notifies the "**Personal Data Protection Board**" by organizing a violation notification form as soon as possible (**not exceeding 72 hours).**

16. TRANSFER OF PERSONAL DATA

Personal data cannot be transferred without the explicit consent of the data subject. Personal data may be transferred in the following cases,

a. If expressly provided for in the law,
b. If it is necessary for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid, or of another person,
c. Provided that it is directly related to the conclusion or performance of a contract, it is necessary to process personal data of the parties to the contract,
d. If it is mandatory for the data controller to fulfill its legal obligation
e. If it has been made public by the person concerned,
f. Data processing is mandatory for the establishment, exercise or protection of a right,
g. If data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject,

Personal data of a private nature other than health and sexual life may be transferred to third parties without the explicit consent of the data subject in cases stipulated by law. Personal data relating to health and sexual life can only be transferred for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing, provided that adequate measures are taken, in the presence of one of the specified conditions, without seeking the explicit consent of the person concerned.

17. THIRD PARTIES TO WHOM PERSONAL DATA IS TRANSFERRED and PURPOSES OF TRANSFER

In accordance with Article 8 of the Personal Data Protection Law, the personal data of the data owners governed by this "Policy" may be transferred to natural persons or private legal entities, shareholders, business partners, suppliers, legally authorized public institutions and organizations, legally authorized private law persons limited to the purpose requested by

the relevant public institutions and organizations within the legal authority of the relevant public institutions and organizations, limited to the purpose requested by the relevant private law persons within the legal authority..

18. PERSONAL DATA DESTRUCTION TECHNIQUES

Personal data, the amendment or abolition of the provisions of the relevant legislation that constitute the basis for the processing of personal data, the disappearance of the purpose requiring its processing or storage, the withdrawal of the explicit consent of the person concerned in cases where the processing of personal data is carried out only on the basis of explicit consent, the acceptance by the company of the application made by the person concerned for the deletion and destruction of personal data within the framework of his rights pursuant to Article 11 of the law. In cases where the company accepts the application made by the data subject for the deletion and destruction of personal data within the framework of the rights of the data subject pursuant to Article 11 of the Law, the company rejects the application made by the data subject with the request for deletion, destruction or anonymization of personal data, finds the answer insufficient or does not respond within the period stipulated in the Law, In the event that the data subject makes a complaint to the Board and this request is deemed appropriate by the Board, the maximum period of time required for the storage of personal data has expired and there are no conditions that justify storing personal data for a longer period of time, the personal data shall be deleted, destroyed or ex officio deleted, destroyed or anonymized by the company upon the request of the data subject.

At the end of the period stipulated in the relevant legislation or at the end of the retention period required for the purpose for which they are processed, personal data are destroyed by the company ex officio (periodic destruction periods) or upon the application of the person concerned, in accordance with the provisions of the relevant legislation, by the following techniques.

18.1. Deletion of Personal Data

Data Recording Environment	Explanation
Personal Data on Servers	For the personal data on the servers, deletion is made by the system administrator by removing the access authorization of the relevant users for those whose retention period has expired.
Personal Data in Electronic Media	The personal data stored in electronic media that expire after the period of time required for their storage shall be rendered inaccessible and non-reusable in any way.

Personal Data in Physical Media	For personal data kept in physical media, those that expire after the period of time required to be stored are made inaccessible and non-reusable in any way for other employees, except for the unit manager responsible for the document archive. Blackout process is also applied by drawing/painting/erasing the data so that it cannot be read.
Personal Data on Portable Media	Personal data on portable media, those whose retention period has expired, are rendered inaccessible and non-reusable in any way.

18.2. Destruction of Personal Data

Personal Data in Physical Media	Personal data on paper media that expire after the expiration of the retention period are irreversibly destroyed in paper shredding machines.
Personal Data in optical/magnetic media	Personal data contained in optical media and magnetic media The process of physically destroying the data whose retention period has expired is applied. In addition, the data on the magnetic media is rendered unreadable by passing it through a special device and exposing it to a high magnetic field.

18.3. Anonymization of Personal Data

Anonymization of data is the process of making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even if the personal data is matched with other data. In order for personal data to be anonymized, personal data must be rendered unassociated with an identified or identifiable natural person even through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as the return of personal data by the data controller or third parties and / or matching the data with other data.

In accordance with Article 28 of the KVK Law, anonymized personal data can be processed for purposes such as research, planning and statistics. Anonymization techniques of personal data are listed below.

Data Masking: Data masking is a method of anonymizing personal data by removing the basic identifying information of personal data from the data set.

Data Aggregation: With the data aggregation method, many data are aggregated and personal data cannot be associated with any person.

Data Derivation: With the data derivation method, a more general content is created from the content of personal data and personal data is rendered unassociable with any person.

Data Hashing: With the data hashing method, the values in the personal data set are mixed and the link between the values and the persons is broken

19. PERSONAL DATA STORAGE and DESTRUCTION PERIODS

Our company ("KİMYAPSAN A.Ş.") keeps personal data for the period required for the purpose for which they are processed and in accordance with the minimum periods stipulated in the legal legislation to which the relevant activity is subject. In this context, our company first determines whether a period is stipulated for the storage of personal data in the relevant legislation, and if a period is determined, it acts in accordance with this period. If there is no legal period, personal data are stored for the period required for the purpose for which they are processed. Personal data are destroyed at the end of the specified storage periods in accordance with the periodic destruction periods or in accordance with the data owner's application and with the specified destruction methods (deletion and/or destruction and/or anonymization).

DATA CATEGORY	RETENTION/ STORAGE TIME	DESTRUCTION TIME
Credentials	**10 Years**	At the first periodic destruction following the end of the storage period
Contact information	**10 Years**	At the first periodic destruction following the end of the storage period

Location Information	**10 years**	At the first periodic destruction following the end of the storage period
Personal Information	**10 years**	At the first periodic destruction following the end of the storage period
Legal Process Information	**10 years**	At the first periodic destruction following the end of the storage period
Customer Transaction Information	**10 years**	At the first periodic destruction following the end of the storage period
Physical Space Security	**2 years**	At the first periodic destruction following the end of the storage period
Transaction Security Information	**10 years**	At the first periodic destruction following the end of the storage period
Information on Finances	**10 years**	At the first periodic destruction following the end of the storage period
Information of Professional Experience	**10 years**	At the first periodic destruction following the end of the storage period

Marketing Information	**10 years**	At the first periodic destruction following the end of the storage period
Audio and Visual Recordings	**10 years**	At the first periodic destruction following the end of the storage period
Health Information	**10 years**	At the first periodic destruction following the end of the storage period
Criminal Conviction and Security Measures	**10 years**	At the first periodic destruction following the end of the storage period
Vehicle Information	**10 years**	At the first periodic destruction following the end of the storage period
Request Complaint Information	**10 years**	At the first periodic destruction following the end of the storage period
Performance and Career Development Information	**10 years**	At the first periodic destruction following the end of the storage period
Education Planning Information	**05 years**	At the first periodic destruction following the end of the storage period

Visitor and Camera Records	**2 years**	At the first periodic destruction following the end of the storage period
Records Regarding Employee Candidates	**2 years**	At the first periodic destruction following the end of the storage period
Audit and Inspection Information	**10 years**	At the first periodic destruction following the end of the storage period
Information on affiliation of family members	**10 years**	At the first periodic destruction following the end of the storage period

One of the general principles to be complied with in the processing of personal data is that the data should be "relevant, limited and proportionate to the purpose for which they are processed". **The periodic destruction period** of personal data is set as **6 months.**

20. REASONS REQUIRING THE DESTRUCTION OF PERSONAL DATA

Personal data, amendment or abolition of the provisions of the relevant legislation that constitute the basis for the processing of personal data, the disappearance of the purpose requiring its processing or storage, the withdrawal of the explicit consent of the person concerned in cases where the processing of personal data is carried out only on the basis of explicit consent, the acceptance by the company of the application made by the person concerned for the deletion and destruction of his personal data within the framework of his rights pursuant to Article 11 of the Law, the rejection of the application made by the company with the request for deletion, destruction or anonymization of personal data by the person concerned. In cases where the application made by the data subject for the deletion and destruction of personal data within the framework of the rights of the data subject pursuant to Article 11 of the Law is accepted by the company, the company rejects the application made by the data subject with the request for the deletion, destruction or anonymization of personal data, the response is found insufficient or does not respond within the period stipulated in the PDPL, In the event that a complaint is made to the Personal Data Protection Board and this request is deemed appropriate by the Personal Data Protection Board, the maximum period required for the storage of personal data has expired and there is no condition that justifies storing personal data for a longer period, the company **("KİMYAPSAN A. Ş."),** upon the request of the person concerned or ex officio, is deleted, destroyed or anonymized.

21. RESPONSIBLE PERSONS IN THE PROCESS OF STORING AND DESTROYING PERSONAL DATA

All units and employees of "**KİMYAPSAN A.Ş."** support the implementation of technical and administrative measures to ensure data security in all data processing environments in order to ensure the proper implementation of the technical, legal and administrative measures specified within the scope of this Personal Data Protection Law, secondary legislation and Personal Data Processing, Protection and Destruction Policy, to increase the training and awareness of unit employees, to ensure that personal data is processed in accordance with the law, and to work in cooperation with responsible units.

a. It is the responsibility of the "data protection manager" to review all revisions and amendments made to the "Personal Data Processing, Protection and Destruction Policy". The data protection manager is also responsible for developing the procedure, providing the necessary trainings and guiding employees on the interpretation of the procedure. The data protection manager also monitors compliance with this procedure and provides the necessary support for compliance.
b. The data protection manager is responsible for controlling the periodic destruction processes of this procedure, retaining the specified data for the relevant retention periods, monitoring these periods and destroying the data whose retention period has expired.

The principles of deletion, destruction or anonymization of personal data are carried out within the framework of the "*Regulation on Deletion, Destruction or Anonymization of Personal Data".*

22. RIGHTS OF THE PERSON CONCERNED

The data subjects whose personal data are being processed have the following rights in accordance with Article 11 of the PDPL by applying to the data controller **"KİMYAPSAN A.Ş":**

a. The right to learn whether personal data is being processed,
b. The right to request information if personal data has been processed,
c. The right to learn the purpose of processing personal data and whether they are used for their intended purpose,
d. The right to know the third parties to whom personal data are transferred domestically or abroad,
e. To request correction of personal data in case of incomplete or incorrect processing,
f. The right to request the deletion or destruction of personal data within the framework of the conditions stipulated in the Data Protection Legislation,
g. The right to request notification of the transactions made pursuant to subparagraphs (e) and (f) to third parties to whom personal data are transferred
h. The right to object to the occurrence of a result to the detriment of the person himself/herself by analyzing the processed data exclusively through automated systems
i. The right to demand compensation for damages in case of damage due to unlawful processing of personal data

23. COMPLAINT and APPLICATION METHODS

Personal data owners are required to make the following requests regarding their rights in accordance with the provisions of Article 11 of PDPL by filling out the application form available at **kimyapsan.com.tr:**

- To deliver a copy with wet signature to Kimya İhtisas OSB, Recep Yazıcı Cd. No:1, 41455 Demirciler OSB, Dilovası/KOCAELİ in person or through a notary public,
- After signing with your secure electronic signature within the scope of the Electronic Signature Law No. 5070, sending the form with secure electronic signature to **kimyapsan@hs01.kep.tr** via registered electronic mail (KEP),
- Sending an e-mail to the e-mail address **n.korucu@kimyapsangrup.com** by using mobile signature or the e-mail address previously notified to the data controller by the data subject and registered in the system of the data controller,
- Sending them with information and documents that will identify them using other methods determined by the Personal Data Protection Board, (In case third parties request an application on behalf of personal data owners, there must be a special power of attorney issued by the data owner through a notary public on behalf of the person who will make the application).

The data controller "**KİMYAPSAN A.Ş"** is obliged to finalize the requests in the application free of charge as soon as possible and within **30 (Thirty)** days at the latest, depending on the nature of the request. The data controller accepts the request of the person concerned or rejects it by explaining the reason and notifies the person concerned in writing or electronically. In cases where the application of the person concerned is rejected, the answer given is insufficient or the application cannot be answered in time, the person concerned may file a complaint to the Personal Data Protection Board within **30 (thirty)** days from the date of learning the answer of the data controller "**KİMYAPSAN A.Ş"** and in any case within **60 (sixty)** days from the date of application.

24. PUBLICATION and STORAGE OF THE POLICY

This "**Personal Data Processing, Protection and Destruction Policy**" of the data controller "**KİMYAPSAN A.Ş"** is published in two different environments, wet signed and electronically, and disclosed to the public on the website. The printed paper copy shall also be kept in the file.