BERKO PERSONAL DATA STORAGE AND DESTRUCTION POLICY

1. PURPOSE

The purpose of this policy is; to determine the rules, roles and responsibilities to be applied throughout Berko İlaç ve Kimya San.A.Ş. (Company) in order to fulfill the obligations regarding the storage and destruction of personal data and other obligations specified in the Regulation in accordance with the "*Law on the Protection of Personal Data*" and the "*Regulation on the Deletion, Destruction or Anonymization of Personal Data*".

2. SCOPE

The Policy covers the personal data and sensitive personal data held by the Company, defined by Law, all Company employees, managers, consultants and their subsidiaries in all cases of personal data sharing, external service providers and other natural and legal persons with whom the Company has a legal relationship. The Policy covers the personal data contained in the systems in which the data are processed by means of fully or partially automatic or non-automatic means, provided that they are part of any data recording system, as specified in the Law. Unless otherwise stated in the Policy, personal data and sensitive personal data will be referred to together as “Personal Data”.

3. DEFINITIONS

Personal Data: All kinds of information about an identified or identifiable real person,

Sensitive Personal Data: Data about the race, ethnic origin, political thought, philosophical belief, religion, sect or other beliefs of people, disguise and clothing, association, foundation or trade union membership, health, sexual life, criminal conviction and security measures, as well as biometric and genetic data of people,

Explicit consent: A written statement related to a specific issue, based on information and explained by free will,

Data recording system: The registration system in which personal data is processed by structuring according to certain criteria,

Inventory of Personal Data Processing: The inventory detailed by data controllers by explaining the personal data processing activities they carried out depending on their business processes; maximum period created by associating personal data with the purposes of processing, data category, transferred recipient group and data subject person group, and required for the purposes for which personal data is processed, the personal data that is foreseen to be transferred to foreign countries and the measures taken regarding data security.

Masking: Operations such as deletion of certain areas of personal data in such a way that they cannot be associated with an identified or identifiable real person, deletion of their tops, coloring and staining, etc.

Anonymization: Even if the personal data is matched with other data, not be able to be associated with an identified or identifiable real person in any way,

Deletion of Personal Data: The process of making the personal data inaccessible and unusable again for the relevant users in any way,

Destruction of Personal Data: The process of making the personal data inaccessible, irretrievable and unusable again by no one in any way,

Destruction: Deletion, destruction or anonymization of personal data,

Periodic destruction: In the event that all of the conditions for processing personal data contained in the law disappear, the deletion, destruction or anonymization process that will be carried out ex officio at repetitive intervals specified in the retention and destruction policy of personal data,

Personal Data Storage Table: The table showing the periods during which the personal data will be kept by the Company,

4.REGISTRATION ENVIRONMENTS REGULATED BY THE POLICY

All kinds of media containing personal data that are processed fully or partially automatic or by non-automatic means, provided that they are part of any data recording system, include in the scope of the recording environment.

The personal data belonging to the data owners are stored securely by the Company in the environments listed in the table below in accordance with the relevant legislation, especially the provisions of the PDPL, and within the framework of international data security principles:

Electronic media:

- EXCHANGE SERVER
- SAP – SUCCESS FACTORS
- FILE SERVER
- VERIBASE
- POLIMEK-PDKS
- DAPHNE
- MDM
- SECURITY CAMERA
- DC DHCP
- DC
- DC 2

Physical environments:

- Unit Cabinets
- Archive

5. DUTIES AND POWERS OF THE PERSONAL DATA PROTECTION TEAM

5.1. The Personal Data Protection Team is responsible for the announcement of the Policy to the relevant business units and
for following up fulfillment of its requirements by the company units.

5.2. The Personal Data Protection Unit makes the necessary announcements and notifications for the relevant business units to follow up on situations such as legislative changes related to the protection of personal data, regulatory actions and decisions of the Board, court decisions or changes in processes, applications and systems and, if necessary, to update their business processes,

5.3. The Personal Data Protection Unit determines the processes for the examination, evaluation, follow-up and conclusion of the decisions and regulations of the Board, court decisions and other competent authorities with the laws and secondary regulations, and announces them to the relevant units.

6.TECHNICAL AND ADMINISTRATIVE MEASURES RELATED TO THE STORAGE OF PERSONAL DATA

For the purpose of storing personal data securely, preventing illegal processing, access and destruction of data in accordance with the law, all administrative and technical measures taken by the Company within the framework of the principles in the article 12 of PDPL are listed below:

6.1. Administrative Measures:

6.1.1. It limits internal access to the stored personal data to the personnel who are required to access it according to the job definition. In limiting access, whether the data is of a sensitive nature and the degree of importance are also taken into account.
6.1.2.If the processed personal data is obtained by others through unlawful means, it notifies this situation to the relevant person and the Board as soon as possible.
6.1.3. Regarding the sharing of personal data, it signs a framework agreement on the protection of personal data and data security with the persons to whom personal data is shared, or ensures data security with the provisions added to its existing agreement.
6.1.4. It employs knowledgeable and experienced personnel about the processing of personal data and provides the necessary trainings to its personnel within the scope of the legislation on the protection of personal data and data security.
6.1.5. It performs and makes necessary inspections in order to ensure the implementation of the provisions of the Law before its own legal entity. It resolves privacy and security vulnerabilities that arise as a result of audits.

6.2. Technical Measures:

6.2.1. It performs the necessary internal controls within the scope of the established systems.
6.2.2. Within the scope of the established systems, it carries out the processes of information technologies risk assessment and business impact analysis.
6.2.3. It provides the provision of technical infrastructure to prevent or monitor the leakage of data outside the institution and the creation of related matrices.
6.2.4. It provides control of system vulnerabilities by taking penetration testing service regularly and when the need arises.
6.2.5. It ensures that the access rights of employees in information technology units to personal data are kept under control.
6.2.6. The destruction of personal data is ensured in such a way that it cannot be recycled and does not leave an audit trail.
6.2.7. In accordance with the article 12 of the Law, all kinds of digital media in which personal data are stored are protected by encrypted or cryptographic methods in such a way as to meet the information security requirements.

7. WHAT TO DO IN CASE THE CONDITIONS FOR THE PROCESSING OF PERSONAL DATA DISAPPEAR

7.1. In the event that the purpose factor for the processing of personal data disappears, the express consent is withdrawn or all the conditions for processing personal data in Articles 5 and 6 of the Law are eliminated, or there is a situation where none of the exceptions in the mentioned articles can be applied, personal data whose processing conditions are eliminated are masked, deleted, destroyed or anonymized by the relevant business unit, taking into account business needs, within the scope of Articles 7, 8, 9 or 10 of the Regulation, by explaining the reason for the method applied.

However, in the event of a finalized court decision, the method of destruction ordered by the court decision should be applied.

7.2. All users who process or store personal data and Company units holding data will review whether the conditions related to processing have disappeared or not within 6 months at the latest in the data recording environments they use. Upon the application of the personal data owner or the notification of the Board or a court, the relevant users and units will conduct this review in the data recording environments they use, regardless of the periodic audit period.

7.3. If it is determined that the data processing conditions have disappeared as a result of periodic reviews or at any time, the relevant user or data owner will decide to delete, destroy or anonymize the relevant personal data from the recording environment under its own responsibility in accordance with this policy. In cases of hesitation, the transaction will be made by obtaining the opinion of the relevant data owner business unit. If it is necessary to take a decision regarding the destruction of personal data with multi-stakeholder data ownership in the Central Information Systems, the opinion of the Personal Data Protection Unit will be taken and the storage or deletion, destruction or anonymization of the data in accordance with this policy will be decided by the relevant data owner business unit.

7.4. All transactions related to the masking, deletion, destruction or anonymization of personal data are recorded and these records are stored for at least 3 years, excluding other legal obligations.

7.5. On the deletion, destruction or anonymization of personal data, it is obligatory to act in accordance with the general principles in Article 12 of Law and the technical and administrative measures to be taken within the scope of the article 12 of Law, the provisions of the relevant legislation, the decisions of the Board and the decisions of the court.

7.6. When a natural person who owns personal data requests the deletion, destruction or anonymization of his personal data by applying to the Company pursuant to Article 13 of the Law, the relevant data subject business unit examines whether all the conditions for processing personal data have disappeared. If all the processing conditions have disappeared; it deletes, destroys or anonymizes the personal data subject to the request. The request is finalized within 30 days at the latest from the date of application and information is provided to the relevant person through the Personal Data Protection Unit. If all the conditions for processing personal data have disappeared and the personal data subject to the request have been transferred to third parties, the relevant data subject business unit immediately notifies the third party to which the transfer has been made and ensures that the necessary actions are taken by the third party within the scope of the Regulation.

7.7. In cases where all the conditions for processing personal data have not been eliminated, the requests of the personal data owners for the deletion or destruction of their data may be rejected by the Company by explaining the reason in accordance with paragraph 3 of Article 13 of the Law. The rejection response is notified to the relevant person in writing or electronically no later than 30 days.

7.8. Requests for deletion or destruction of personal data will be evaluated only on the condition that the identification of the relevant person has been made. In the requests to be made outside these channels, the relevant persons will be directed to the channels where identification or verification can be made.

8. INTRODUCTION OF THE POLICY, VIOLATION SITUATIONS AND SANCTIONS

8.1. This Policy will enter into force by being announced to all employees and will be binding on all business units, consultants, external service providers and everyone who processes personal data on behalf of the other Company as of its entry into force.

8.2. Monitoring whether the company's employees comply with the requirements of the Policy will be the responsibility of the supervisors of the relevant employees. If a violation of the policy is detected, the matter will be immediately reported to the affiliated manager by the relevant employee's supervisor. If the violation is of a significant size, information will be provided to the Personal Data Protection Unit by the manager without delay.

8.3. The necessary administrative action will be taken against the employee who acts contrary to the policy after the evaluation to be made by Human Resources.

9. THE PERSONS WHO WILL TAKE PART IN THE STORAGE AND DESTRUCTION OF PERSONAL DATA AND THEIR RESPONSIBILITIES

In general, all employees, consultants, external service providers and everyone else who stores and processes personal data within the Company are responsible for fulfilling these requirements in order to fulfill the requirements for the destruction of data specified by the Law, Regulation and Policy. The title, unit and duty list of specially assigned personnel are included in Table Annex 1. Each business unit is obliged to store and protect the data it generates in its own business processes; however, if the data generated is located only in information systems outside the control and authority of the business unit, the data in question will be stored by the units responsible for information systems. Periodic destruction that will affect business processes and cause data integrity to deteriorate, data loss and results contrary to legal regulations will be carried out by the relevant information systems departments, taking into account the type of relevant personal data, the systems in which it is contained and the business unit that owns the data.

10. PERIODS OF STORAGE AND DESTRUCTION OF PERSONAL DATA

The Table Showing the Storage and Destruction Periods of Personal Data is included in Annex 2. The storage and destruction periods in question will be taken into account in periodic destruction or destruction operations to be carried out upon request. The Table Showing the Periods of Storage and Destruction of Personal Data will be updated by the business units that own the processes that will be included in the Company's personal data inventory, taking into account the evaluations of the Personal Data Protection Unit in case of hesitation.

11. PERIODIC DESTRUCTION PERIODS

The Period of Periodic Destruction of Personal Data is determined and designated by the relevant business units of the data subject; however, in any case, this period cannot exceed 6 (six) months.

12. METHODS OF DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

12.1 Deletion of Personal Data:

Secure Deletion from Software: When deleting data processed by fully or partially automatic means and stored in digital media, methods related to deleting data from the relevant software are used in such a way as to make it inaccessible and unusable again for the relevant Users in any way. Deletion of the relevant data in the cloud system by issuing the delete command; removal of the access rights of the relevant user on the file located on the central server or the directory where the file is located; deletion of the relevant lines in databases by database commands; deletion of data in portable media, i.e. flash media, using appropriate software may be considered in this context.

However, if the deletion of personal data will result in the inability to access other data within the system and the inability to use this data, the personal data will also be deemed deleted if the personal data is archived by making it impossible to be associated with the relevant person, provided that the following conditions are met.

− Closing to the access of any other institution, organization or person,
− Taking all kinds of necessary technical and administrative measures to ensure that personal data is accessed only by authorized persons.

Safe Deletion by an Expert: In some cases, it may agree with a specialist to delete personal data on his behalf. In this case, the personal data will be securely deleted by the person who is an expert on this subject in such a way that it will not be accessible to the Relevant Users in any way and will not be reusable.

Obscuration of Personal Data Contained in the Paper Medium(Masking): In order to prevent the inappropriate use of personal data or to delete the data requested for deletion, it is a method of physically cutting out the relevant personal data and removing it from the document or making it irreversible and invisible by using fixed ink which it cannot be read with technological solutions, closing it.

12.2. Destruction of Personal Data:

12.2.1 Electronic Records;
Physical Destruction,
It can be destroyed by overwriting.
For flash-based hard drives containing personal data that have ATA (SATA, PATA, etc.), SCSI (SCSI Express, etc.) interfaces, it is destroyed by using the command if it is supported, by using the manufacturer's recommended destruction method if it is not supported, or by using one or more of the appropriate methods.
Personal data contained in data storage media such as CDs, DVDs are destroyed by physical destruction methods such as burning, breaking into small pieces, melting.
For personal data in peripherals such as a printer with removable data recording media, fingerprint door access system, the appropriate destruction method is selected according to the nature of the unit after verifying that all data recording media have been removed.

12.2.2 Physical Records, on the other hand, are destroyed by paper shredders or clipping machines to an unintelligible size (by shredding vertically and horizontally if possible) or by other means that make them impossible to read (for example, cutting the Record into small pieces that cannot be combined or burning the physical record in a suitable environment, etc.).

12.2.3 For cloud systems; during the storage and use of personal data contained in these systems, they are encrypted using cryptographic methods, and encryption keys are used separately for personal data wherever possible, especially for each cloud solution from which services are received. When the cloud computing service relationship ends, all copies of the encryption keys necessary to make the personal data usable are destroyed.

12.2.4 For devices that fail or are sent for maintenance, the destruction of personal data contained in these devices is carried out as follows:

a) Destruction of the personal data contained in the relevant devices by appropriate method before they are transferred to third parties for maintenance and repair

b) In cases where it is not possible or appropriate to destroy, dismantling and storing data storage media and sending other parts to third parties such as manufacturer, seller, service,

c) Taking the necessary measures to prevent personnel who come from outside for purposes such as maintenance, repair from copying personal data and removing it from the institution,

12.3. Methods of Anonymization of Personal Data:

12.3.1. Anonymization Methods that Do Not Cause Value Irregularity,

These are methods of anonymization applied by generalization of any personal data group, displacement with each other, or removal of a specific data or sub-data group from the group, without making any changes or additions/subtractions to the stored personal data.

Variable Extraction: The existing data set is anonymized by subtracting "high degree descriptive" variables from the variables in the data set created after combining the data collected by the method of extracting descriptive data.

Removing Records: In the Decryption method, the data line containing singularity between the data is decrypted from the records and the stored data is anonymized. For example, if there is a single senior manager in a company, the remaining data may be anonymized by removing the data belonging to this person from the records where the seniority, salary and gender data of employees at the same level as each other are kept.

Regional Concealment: In the regional concealment method, if a single data has a decisive character due to the fact that it creates a combination that is very little visible, hiding the relevant data provides anonymization. For example, if only one person is 65 years old among the relevant data controllers who are on the reserve list of the company's football team, in a dataset where the information about whether they can play football in terms of age, gender and health status is stored together, replacing 'Age:65' with 'Unknown' or leaving this part blank will ensure anonymization.

Lower and Upper Limit Coding: It is anonymized by combining the values in a data set containing predefined categories with the lower and upper limit coding method by determining a specific criterion.

Generalization: With the data aggregation method, many data are aggregated and personal data are made to be unable to be associated with any person. For example; revealing that there are employees as many as Z at the age of X, without showing the ages of the employees individually.

Global Coding: With the data derivation method, a more general content is created than the content of the personal data and it is ensured that the personal data cannot be associated with any person. For example; specifying ages instead of dates of birth; specifying the region of residence instead of a public address.

12.3.2. Anonymization Methods that Cause Value Irregularity

Anonymization methods that provide value irregularity creates corruption by changing some data in personal data groups contrary to those that do not cause value irregularity. When using these methods, deviations will need to be applied carefully in line with the expected/desired benefit to be obtained. By ensuring that the total statistics are not distorted, the expected benefit from the data can continue to be provided.

Adding Noise: Method of adding noise to data, especially in a data set where numerical data are weighted, data are anonymized by adding some deviations in the plus or minus direction at a determined rate to the existing data. For example, in a data group with weight values, by using a deviation of 3 kg (+/−), the display of the actual values is prevented and the data is anonymized. The deviation is applied equally to each value.

Combining: In the micro-merging method, all data will first be sorted into groups in a meaningful order (for example, from large to small), and anonymization will be achieved by writing the value obtained by averaging the groups instead of the relevant data in the existing group. For example, for salary information; If two groups of below and above of 10,000 TL are created, the sum of the salaries of people receiving 10,000 TL and less salaries is divided by the number of people, and this value obtained is written into the salary set of everyone receiving a salary under 10,000 TL.

Data Exchange: In the data exchange method, the values of a variable are exchanged with each other between pairs selected from the data stored. In this method, which is used for data that can be categorized in general, the purpose is to convert the database by replacing the data belonging to the data owners with each other.
All transactions related to the deletion, destruction and anonymization of personal data are recorded by our company and these records are stored for at least 3 (three) years, excluding other legal obligations.

12. ENFORCEMENT

12.1. The policy will enter into force as of the date of publication.

12.2. It is the responsibility of the Personal Data Protection Unit to announce the policy throughout the Company and to make the necessary updates.

ANNEXES: 1- Personnel Title, Unit And Task List
2- Storage And Destruction Period Table

Date of Publication : 10.07.2018
Version 2

ANNEX- 1
PERSONNEL TITLE, UNIT AND TASK LIST

PERSONNEL	TITLE	ROLE
R&D Coordinator Serap Odabaşı	Research and Development Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
IT Manager Erol Karaca	Information Technologies Department-Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Foreign Markets Project Manager S. Aykut Adalmaz	Foreign Trade Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Factory Manager Nursel Gülsoy	Factory General - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Legal Counselor Şükrü Aymelek	Agreements - Personal data retention and destruction policy enforcement main responsible-Data Controller Representative	Management of the personal data destruction process in accordance with the periodic destruction period and regular audits by ensuring compliance with the retention period of the processes within the scope of its role
Chief of Administrative Affairs H.Medeni Yılmaz	Administrative Affairs Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
HR Manager İbrahim Sariyar	HR Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Quality Assurance and Responsible Manager Haluk Akkuş	Quality Assurance Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Quality Control Manager Erol Taşkan	Quality Control Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role

Corporate Communications Chief Fidan Akur	Corporate Communications Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Finance Director Cem Günbay	Finance Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Group Product Manager Savaş Duman	Marketing Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Regulatory Affairs Manager Neslihan Esen	Regulatory Affairs and Pharmacovigilance Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Purchase Esin Aksu	Purchase Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Sales Coordinator Hüseyin Polat	Sales Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Sales Accounting Selçuk Uğur	Sales Accounting Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Manufacturing Manager Ersin Hayran	Manufacturing Planning Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role
Manufacturing Planning Manager Elif Öztürk	Manufacturing Planning Department - Personal data retention and destruction policy enforcement officer	Management of the personal data destruction process in accordance with the periodic destruction period by ensuring compliance with the retention period of the processes within the scope of its role

ANNEX-2
STORAGE AND DESTRUCTION PERIOD TABLE

Personal data will be kept for the periods specified in the table below, taking into account the issues specified in Article 7 of the Policy, unless there is a final court decision or interim injunction to the contrary, and will be destroyed at the end of the period:

PROCESS	STORAGE PERIOD	DESTRUCTION PERIOD
Ministries/Public Institutions/Tender documents	10 years	Within 180 days after the end of the storage period
Answering court / enforcement information requests regarding personnel	10 years after the end of the employment relationship	Within 180 days after the end of the storage period
Contracts signed with third parties	10 years	Within 180 days after the end of the storage period
Personnel file	10 years after the end of the employment relationship	Within 180 days after the end of the storage period
Negative job applications	2 years from the negative result of the application	Within 180 days after the end of the storage period
All documents related to wages and salary	10 years after the end of the employment relationship	Within 180 days after the end of the storage period
Personnel private health and personal accident insurance policies	10 years after the end of the employment relationship	Within 180 days after the end of the storage period
Vehicle plate information (third parties)	1 year from the date of registration	Within 180 days after the end of the storage period
Occupational health and safety practices	10 years after the end of the employment relationship	Within 180 days after the end of the storage period
Recording/Tracking/Log Systems	1 year	Within 180 days after the end of the storage period
Security camera footage	3 months from the date the image was taken	Within 90 days after the end of the storage period
Payment transactions	10 years	Within 180 days after the end of the storage period
Personnel Financing Processes	10 years after the end of the employment relationship	Within 180 days after the end of the storage period
The part of the contract process related to personal data and the retention of the contract	10 years after the end of the employment relationship	Within 180 days after the end of the storage period
Information obtained via internet and wifi	1 year from the date of registration	Within 180 days after the end of the storage period
Request / Complaint Information	5 years from the date of registration	Within 180 days after the end of the storage period
Filing of all kinds of documents	10 years	Within 180 days after the end of the storage period
Filing of training records	10 years	Within 180 days after the end of the storage period

In the event that personal data is subject to or related to a crime within the scope of the Turkish Penal Code or other legislation imposing criminal provisions, in accordance with Articles 66 and 68 of the Turkish Penal Code	During the statute of limitations and criminal statute of limitations	