PLEKSUS PHARMACOVIGILANCE

PERSONAL DATA STORAGE AND DESTRUCTION POLICY

1. PURPOSE OF THE POLICY

The purpose of this policy; In order to fulfill the obligations regarding the storage and destruction of personal data and other obligations specified in the Regulation in accordance with Articles 5 and 6 of the Regulation on the Deletion, Destruction or Anonymization of Personal Data (Regulation), which was issued based on the Law No. 6698 on the Protection of Personal Data (Law) and published in the Official Gazette No. 30224 on 28.10.2017; **Pleksus Pharmacovigilance Services and Clinical Trial Ltd. Sti."** (Hereinafter **referred to as "**Pleksus Pharmacovigilance")to determine the rules, roles and responsibilities to be applied throughout the country.

Pleksus Pharmacovigilance; It undertakes to comply with the tools, programs and processes to be applied in accordance with this Policy during the deletion, destruction or anonymization of personal data that it contains, which are fully or partially automatic or processed by non-automatic means provided that it is a part of any recording system.

2. SCOPE OF THE POLICY

This Policy; Personal data belonging to **Pleksus Pharmacovigilance** employees, employee candidates, service providers, suppliers, visitors, customers and other third parties are within the scope of this Policy, and **this Policy is applied in all recording environments and activities related to personal data processing where personal data** owned or managed **by** Pleksus Pharmacovigilance are processed.

3. RECORDING ENVIRONMENTS REGULATED BY THE POLICY

With this policy, Pleksus Pharmacovigilance agrees to cover personal data in the following environments where personal data is present and in all environments that may arise in addition to the specified environments;

1. **Electronic Environments;**

a. **Servers used on behalf** of Pleksus Pharmacovigilance (backup, e-mail, database, web, file sharing, etc.)
b. Software (Office Software, ERP, CRM, etc.)
c. Information security devices (firewall, intrusion detection and prevention, log file, antivirus, etc.)
d. Personal computers (Desktop, laptop)
e. Optical discs (CD, DVD, etc.)
f. Mobile devices (phone, tablet, etc.)
g. Removable memories (USB, Memory Card, etc.)
h. Printer, scanner, copier
i. Cloud systems

2. **Non-Electronic Environments;**

a. Paper,
b. Manual data logging systems (survey forms, visitor entry book)
c. Written, printed, visual media

4. DEFINITIONS

The definitions used in this Policy are as follows:

Explicit consent	Consent regarding a specific subject, based on information and expressed with free will

Anonymization	Making personal data incapable of being associated with an identified or identifiable natural person in any way, even by matching it with other data
Personal Data	Any information relating to an identified or identifiable natural person
Processing of personal data	Any operation 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 means or non-automatic means provided that it is a part of any data recording system
PDP Law	Law No. 6698 on the Protection of Personal Data
PDP Board	Personal Data Protection Board
PDP Institution	Personal Data Protection Authority
Special categories of personal data	Data related to race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance, membership of associations, foundations or unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data of individuals
Data processor	A natural or legal person who processes personal data on behalf of the data controller based on the authority granted by the data controller
Personal data owner	The real person whose personal data is processed, who is considered as the "relevant person" in the PDP Law
Related user	Except for the person or unit responsible for the technical storage, protection and backup of the data, they are the real or legal persons who process personal data within the data controller organization or in line with the authorization and instruction received from the data controller.
Data controller	A 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

Data Controllers Registry	Data controllers' registry (VERBIS) kept by the Presidency under the supervision of the Personal Data Protection Board
Regulation	Regulation on the Deletion, Destruction or Anonymization of Personal Data.
Recording media	It is the name given to any environment where personal data is stored that is processed by fully or partially automatic means or non-automatic means provided that it is a part of any data recording system.
Data Processing Inventory	The personal data processing activities carried out by data controllers depending on their business processes; It is the inventory they create and detail by associating the purposes of processing personal data, data categories, the transferred recipient group and the data subject group with the data subject group.
Periodic disposal	It is the process of deleting, destroying or anonymizing personal data to be carried out ex officio at repeated intervals specified in the personal data storage and destruction policy in the event that all the conditions for processing personal data in the law disappear.

5. EXPLANATIONS ON STORAGE

In Article 4 of the Law, it is stated that the processed personal data must be relevant, limited and proportionate to the purpose for which they are processed and must be stored for the period stipulated in the relevant legislation or required for the purpose for which they are processed, and in Articles 5 and 6, the conditions for processing personal data are listed.

Accordingly, within the framework of our company's activities, personal data is stored for the period stipulated in the relevant legislation or in accordance with our processing purposes.

5.1 Legal Reasons Requiring Retention

Personal data processed within the framework of the activities of Pleksus Pharmacovigilance are kept for the period stipulated in the relevant legislation.

In this context, personal data;

a. Law No. 6698 on the Protection of Personal Data,
b. Regulation on the Safety of Medicines
c. Labor Law No. 4857,
d. Turkish Code of Obligations No. 6098,
e. Turkish Commercial Code No. 6102
f. Social Security and General Health Insurance Law No. 5510,
g. Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications,
h. Occupational Health and Safety Law No. 6331,
i. Good Pharmacovigilance Practices (IFU) Guidelines
j. It is stored for the retention periods stipulated within the framework of other secondary regulations in force in accordance with these and other laws not listed.

5.2 Processing Purposes Requiring Storage

Pleksus Pharmacovigilance stores the personal data it processes within the framework of its activities for the following purposes.

a. Clearly stipulating the storage of personal data in the legislation,
b. Storing personal data because it is directly related to the establishment and performance of contracts,
c. Storing personal data for the purpose of establishing, exercising or protecting a right,
d. It is mandatory to store personal data for the legitimate interests **of Pleksus Pharmacovigilance,** provided that it does not harm the fundamental rights and freedoms of individuals,
e. Storing personal data **for the purpose of fulfilling any legal obligation** of Pleksus Pharmacovigilance,
f. Explicit consent of data owners in terms of storage activities that require the explicit consent of data owners

6. REASONS FOR DESTRUCTION

Personal data;

a. Amendment or abolition of the provisions of the relevant legislation that constitute the basis for its processing,
b. The disappearance of the purpose that requires processing or storage,
c. In cases where the processing of personal data is carried out only on the basis of explicit consent, the data subject withdraws his/her explicit consent,
d. Acceptance by the Authority of the application made by the relevant person regarding the deletion and destruction of his/her personal data within the framework of his/her rights in accordance with Article 11 of the Law,
e. In cases where the Authority rejects the application made by the relevant person with the request for the deletion, destruction or anonymization of his/her personal data, finds his/her answer insufficient or does not respond within the period stipulated in the Law; To make a complaint to the Board and this request is approved by the Board,

In cases where the maximum period requiring the storage of personal data has expired and there are no conditions that justify storing personal data for a longer period of time, **they are deleted, destroyed or deleted ex officio by** Pleksus Pharmacovigilance upon the request of the person concerned.

7. TECHNICAL AND ADMINISTRATIVE MEASURES

Technical and administrative measures are taken by **Pleksus Pharmacovigilance** within the framework of the adequate measures determined and announced by the Board for special categories of personal data in accordance with Article 12 of the Law and Article 6, paragraph 4 of the Law, in order to securely store personal data, to prevent unlawful processing and access, and to destroy personal data in accordance with the law.

1. Technical Measures

The technical measures taken by Pleksus Pharmacovigilance regarding the personal data it processes are listed below:

1.1. Network security and application security are ensured.

1.2. An authorization matrix has been created for employees.

1.3. Access logs are kept regularly.

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

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

1.6. Firewalls are used.

1.7. Personal data security is monitored.

1.8. Necessary security measures are taken regarding entry and exit to physical environments containing personal data.

1.9. The security of physical environments containing personal data against external risks (fire, flood, etc.) is ensured.

1.10. The security of environments containing personal data is ensured.

1.11. Personal data is reduced as much as possible.

1.12. Personal data is backed up and the security of the backed up personal data is also ensured.

1.13. Penetration testing is applied.

1.14. Encryption is done.

2. Administrative Measures

The administrative measures taken by Pleksus Pharmacovigilance regarding the personal data it processes are listed below:

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

2.2. Corporate policies on access, information security, use, storage and destruction have been prepared and started to be implemented.

2.3. Confidentiality commitments are made.

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

2.5. The signed contracts contain data security provisions.

2.6. Personal data security policies and procedures have been determined.

2.7. Personal data security issues are reported quickly.

2.8. Personal data security is monitored.

2.9. Personal data is reduced as much as possible.

2.10. In-house periodic and/or random audits are carried out and carried out.

2.11. Existing risks and threats have been identified.

2.12. Protocols and procedures for the security of sensitive personal data have been determined and implemented.

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

In fulfilling the requirements regarding the destruction of data specified in the Law, Regulation and Policy within Pleksus Pharmacovigilance, all employees, consultants, external service providers and everyone who stores and processes personal data at Pleksus Pharmacovigilance are responsible for fulfilling these requirements.

Each business unit is obliged to store and protect the data it produces in its own business processes; However, if the data produced is only available in information systems outside the control and authority of the business unit, the data in question will be stored by the units responsible for the information systems.

Periodic destructions that will affect business processes and cause deterioration of data integrity, data loss and results contrary to legal regulations will be carried out by the relevant

information systems departments, taking into account the type of personal data concerned, the systems in which it is located and the data owner business unit.

Pleksus Pharmacovigilance has established the "Pleksus Pharmacovigilance PDPK Committee" in accordance with the **decision of the Board of Directors to manage this Policy and other policies related to this Policy**. The duties of this committee are stated below;

a. To prepare the basic policies regarding the Protection and Processing of Personal Data and to submit them to the approval of the Board of Directors in order to put them into effect.
b. To decide how the implementation and supervision of the policies regarding the Protection and Processing of Personal Data will be carried out, and **to submit to the approval of the Board of Directors the issues of assigning and coordinating** within the company in Pleksus Pharmacovigilance within this framework.
c. To determine the issues that need to be done to ensure compliance with the Law and the relevant legislation and to submit what needs to be done to the approval of the Board of Directors; to supervise and coordinate its implementation.
d. To raise awareness on the Protection and Processing of Personal Data **within Pleksus Pharmacovigilance** and among the institutions with **which Pleksus Pharmacovigilance** cooperates.
e. **To identify the risks that may occur in the Personal Data processing activities of Pleksus Pharmacovigilance and to ensure that the necessary measures are taken; to submit improvement proposals to the approval of the Board of Directors.**
f. To design and implement trainings on the protection of Personal Data and the implementation of policies.
g. To decide on the applications of Personal Data owners at the highest level.
h. Personal Data owners; To coordinate the execution of information and training activities in order to ensure that they are informed about Personal Data processing activities and their legal rights.

i. To prepare the amendments in the basic policies regarding the Protection and Processing of Personal Data and to submit them to the approval of the Board of Directors to put them into effect.
j. To follow the developments and regulations on the Protection of Personal Data; to **advise the Board of Directors on what to do within** Pleksus Pharmacovigilance in accordance with these developments and regulations.
k. To coordinate the relations with the Personal Data Protection Board and the Authority.
l. To perform other duties assigned by the Board of Directors regarding the protection of Personal Data.

9. DELETION, DESTRUCTION AND ANONYMIZATION OF PERSONAL DATA

The destruction of personal data can be achieved in three different ways: deletion, destruction or anonymization of data. The purpose of the destruction process is that it is not possible to reach the real person with the remaining data.

9.1 Deletion of Personal Data

The deletion will be done **in cases where Pleksus Pharmacovigilance** processes the data by all or automated means, and where **Pleksus Pharmacovigilance** deletes personal data, it must make the data inaccessible or unusable in any way for the users concerned. **Pleksus Pharmacovigilance** must guarantee that the data is inaccessible or non-reusable by any user when performing this process. This guarantee is the responsibility of the data controller.

If personal data that should not be deleted is also affected by the deletion and becomes inaccessible and/or unusable during deletion, providing the following methods together will also be considered deletion:

a) Archiving personal data in a way that cannot be associated with the data subject
b) Closure and elimination of the authorizations and methods such as access, retrieval, reuse of the relevant users for each personal data
c) Taking all necessary technical and administrative measures to ensure that personal data is accessed only by authorized persons only when necessary

The specified deletion methods are subject to the Regulation and it is the responsibility of the Data Controller to update them when relevant.

Personal data is deleted by the following methods.

Data Recording Media	Description
On servers Personal Data Contained	For the personal data on the servers that require storage to be stored has expired, the system administrator removes the access authorization of the relevant users and deletes them.
Electronics Personal Data in the Environment	Personal data in electronic media whose period requiring storage has expired are made inaccessible and unusable in any way for other employees (relevant users) except the database manager.
Personal Data in the Physical Environment	For personal data kept in the physical environment, the period requiring storage has expired, and it is made inaccessible and unusable in any way for other employees, except for the unit manager responsible for the document archive. In addition, blackening is also applied by scratching/painting/erasing it in a way that cannot be read.
Personal Data in Portable Media	Personal data kept in flash-based storage media that require storage has expired is encrypted by the system administrator and access is given only to the system administrator and stored in secure environments with encryption keys.

9.2 Destruction of Personal Data

The destruction will be carried **out in cases where Pleksus Pharmacovigilance** processes the data in physical recording media and **Pleksus Pharmacovigilance** is obliged to make this data impossible to retrieve and reuse. During these processes, **Pleksus Pharmacovigilance** employees and relevant departments are obliged to notify the Data Controller of the relevant

data to be destroyed, and then the Data Controller will take all necessary technical and administrative measures.

Data Recording Media	Description
Personal Data in the Physical Environment	The personal data in the paper environment, whose period requiring storage has expired, is irreversibly destroyed in paper clipping machines.
Personal Data in Optical / Magnetic Media	The process of physically destroying the personal data in optical media and magnetic media, such as melting, burning or pulverizing, is applied. In addition, the magnetic media is passed through a special device and exposed to a high magnetic field, making the data on it unreadable.

9.3 Anonymization of Personal Data

Anonymization is the process **of removing or changing the direct and/or indirect identifiers of personal data in cases where Pleksus Pharmacovigilance processes personal data completely or automatically, making it incapable of being associated with an identified or identifiable natural person, even if it is matched with other data.**

During the anonymization of data, methods such as **Pleksus Pharmacovigilance** irreversible masking, one-way functions and encryption can be used. If the accuracy of the method to be applied cannot be approved by the Data Controller, the board should be consulted.

Methods of Anonymization of Personal Data;

Anonymization Methods That Do Not Provide Value Disorder	• Extracting Variables • Extracting Recordings • Lower and Upper Bound Coding

Anonymization Methods That Provide Value Disorder	• Micro-Splicing • Data Exchange • Adding Noise

10. STORAGE AND DISPOSAL PERIODS

10.1 Periodic Disposal and Statutory Retention Periods

Physical and digital data that have completed their legal storage and destruction periods are destroyed periodically. **Pleksus Pharmacovigilance** deletes, destroys or anonymizes the Personal Data in the first periodic destruction process following the date on which the obligation to delete, destroy or anonymize the Personal Data arises. Periodic destruction is carried out at 6-month intervals for all Personal Data. The legal storage and destruction periods to be taken as a basis during periodic destruction **are determined in the Pleksus Pharmacovigilance** Personal Data Processing Inventory. **Pleksus Pharmacovigilance** undertakes to comply with the new periods if the Board shortens the periods within the scope of Article 11(4) of the Regulation.

Transactions related to deleted, destroyed and anonymized data are stored for at least 3 years, excluding other legal obligations. **Pleksus Pharmacovigilance reserves the right to** store Personal Data arising from other legal obligations.

10.2 Deletion and Destruction Process at the Request of Data Owners

In cases where data owners **request the deletion or destruction of their Personal Data by applying to Pleksus Pharmacovigilance,** it checks the current status of the conditions for processing Personal Data and takes relevant actions accordingly.

If all the conditions for processing Personal Data have disappeared, it deletes, destroys or anonymizes the Personal Data subject to the request. **Pleksus Pharmacovigilance concludes** the request of the relevant person **within 30 (thirty) days at the latest** and informs the relevant person. If all the conditions for processing Personal Data have disappeared and the Personal Data subject to the request has been transferred to third parties, the data controller notifies the third party of this situation; ensures that the necessary actions are taken within the

scope of the Regulation before the third party. If all the conditions for processing Personal Data have not disappeared, **Pleksus Pharmacovigilance** may reject the request by explaining the reason to the relevant data owner and notifies the relevant person in writing or electronically within thirty days at the latest.

3. **Storage and destruction periods on a process basis;**

PROCESS	STORAGE PERIOD	DISPOSAL PERIOD
Article 146 of the Code of Obligations, which regulates the general statute of limitations. In accordance with Article	10-year general statute of limitations	In the first periodic disposal period following the end of the storage period (180 Days)
Preparation of contracts	10 years following the termination of the contract	In the first periodic disposal period following the end of the storage period (180 Days)
Human Resources Processes Execution	Activity 10 years following the end of the	In the first periodic disposal period following the end of the storage period (180 Days)
Occupational health and safety practices	15 years following the termination of the employment relationship	In the first periodic disposal period following the end of the storage period (180 Days)
Documents related to Clinical Trials	15 years	In the first periodic disposal period following the end of the storage period (180 Days)
Answering court/ enforcement information requests regarding personnel	10 years following the termination of the employment relationship	In the first periodic disposal period following the end of the storage period (180 Days)
Transaction Security	2 Years	When the storage capacity is full, it is destroyed by overwriting.
Other Relevant Legislation Required	For the period stipulated in the relevant legislation	In the first periodic disposal period following the end of the storage period (180 Days)

11. EFFECTIVE DATE OF THE POLICY

This Policy **entered into force on** 20.05.2025.