PLEKSUS PHARMACOVIGILANCE SERVICES AND CLINICAL TRIAL PERSONAL DATA PROCESSING AND PROTECTION POLICY

1. INTRODUCTION

Within the framework of this Personal Data Protection and Processing Policy ("Policy"), "Pleksus Pharmacovigilance Services and Clinical Trial Ltd. Şti." (Hereinafter referred to as "Pleksus Pharmacovigilance" for short.) The principles adopted in the execution of personal data processing activities carried out by Pleksus Pharmacovigilance and the basic principles adopted in terms of compliance of data processing activities with the regulations in the Personal Data Protection Law No. 6698 ("Law") are explained and our Company informs personal data owners about the provisions of the law and general principles adopted by our Company.

With full awareness of our responsibility in this context, your personal data is processed within the scope of this Policy and is reasonably protected.

2. PURPOSE OF THE POLICY

The main purpose of this Policy is to set forth the principles regarding the personal data processing activity carried out by Pleksus Pharmacovigilance in accordance with the law and the protection of personal data, and to ensure transparency by enlightening and informing the persons whose personal data are processed by our company in this context.

3. SCOPE OF THE POLICY

This Policy; Regarding your personal data processed by Pleksus Pharmacovigilance; The principles of processing personal data and personal health data, the purposes and conditions of processing these data, and the practices and principles regarding the transfer and destruction of these data in the country and abroad and your rights on the processed data are notified to you below.

4. ACCESS AND UPDATE

The Policy is published on our Company's website and made available to the relevant persons upon the request of personal data owners and updated when necessary. (Your personal data that we collect and process must be accurate and up-to-date when necessary in accordance with Article 4 of the Personal Data Processing Law No. 6698. Therefore, in case of any change in your personal data, you can report your up-to-date and accurate personal information through the methods described in the Clarification Text on our website.)

Our Company reserves the right to make changes to the Policy in parallel with legal regulations.

In case of conflict between the legislation in force, especially the Law, and the regulations included in this Policy, the provisions of the legislation shall be applied.

5. 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 owner	The real person whose personal data is processed, who is considered as the "relevant person" in the PDP Law
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 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
Data Controllers Registry	Data controllers' registry (VERBIS) kept by the Presidency under the supervision of the Personal Data Protection Board

Data Inventory	**The personal data processing activities carried out by Pleksus Pharmacovigilance** depending on its business processes; the inventory created and detailed by associating it with the purposes of personal data processing, the recipient group to whom the personal data is transferred and the relevant personal data owner group.

6. PERSONAL DATA INVENTORY AND CLASSIFICATION OF PERSONAL DATA

In terms of Pleksus Pharmacovigilance; Article 5 of the PDP Law. And based on and limited to one or more of the personal data processing conditions specified in Article 6, in accordance with the general principles specified in the PDP Law, especially the principles specified in Article 4 regarding the processing of personal data, and all obligations regulated in the PDP Law, and personal data owners within the scope of this Policy (Product and Service Recipient, Potential Product and Service Buyer, Patient, Parent/Guardian/ Representative, Employees, Employee Candidates, Visitors, Supplier Employees, Supplier Officials, Shareholders/Partners, Employee Relatives, Employee Candidates' Relatives, Emergency Contacts, Patient Relatives, Health Professionals, Reporters, Consultants and Reference Persons) are processed for the following data processing purposes;

Pleksus Pharmacovigilance collects and processes information about the pharmacovigilance data reported to it from patients, healthcare professionals and other reporters within the scope of pharmacovigilance activities carried out in accordance with the Regulation on the Safety of Medicines and Good Pharmacovigilance Practices Guidelines published by the Turkish Medicines and Medical Devices Agency. The personal data received is stored securely in physical or electronic environment in accordance with the PDPL and the periods specified in other relevant laws.

The personal data received are protected by Pleksus Pharmacovigilance by taking administrative and technical measures in accordance with the obligations stipulated in all

relevant legislation, especially the PDPL. Personal data processing purposes of Pleksus Pharmacovigilance;

- To fulfill the requirements of the activities carried out by our company, and to ensure that the relevant persons benefit from the services offered by our company with the performance of the service,
- Carrying out the necessary work by the relevant business units of our company and carrying out the related business processes and making reports,
- Evaluation of requests and complaints,
- In accordance with the services offered by our company; establishment, exercise and protection of rights arising from the legislation,
- Ensuring that our company activities are carried out in accordance with company procedures or relevant legislation,
- Fulfilling the information sharing, reporting and information obligations stipulated by the Public Institution and all authorities,
- Fulfilling the information and document retention obligations arising from the legal legislation,
- In order to manage our legal processes and to provide you with better and more reliable service without interruption, personal data will be processed within the processing conditions and purposes specified in Articles 5 and 6 of Law No. 6698.

Pleksus Pharmacovigilance has created a personal data inventory in accordance with the Data Controllers Registry Regulation issued by the Personal Data Protection Authority. This data inventory includes data categories, the source of the data, data processing purposes, the data processing process, the recipient groups to which the data is transferred, and the retention periods.

In this context, **the following types of data categories are included in Pleksus Pharmacovigilance**, although they are not limited to these types;

Credential	Written on your identity card; name, surname, mother's name, father's name, place of birth, date of birth, marital status, religion, blood type, registered province, district and neighborhood and the information written on your identity card, including but not limited to these.
Contact Information	In order to communicate with you, you are requested or given; your contact data such as home phone number, mobile phone number, residence address or other address information, e-mail address.

Personal Information	**Employees;** • Photocopy of identity card, • Identity register copy, • Certificate of Residence, • Health report, • Photocopy of diploma, • Criminal record, • Passport photo, • Document stating family status, • Military status certificate, • Employment Contract / Service Contract, • SSI employment declaration, • Your criminal record (criminal record), • Information and documents regarding your health status.
Professional Experience	• Such as professional information, diploma information, courses attended, in-service training information, certificates.
Bank Account Information (Finance)	• Bank account number, IBAN number, other information about the bank card.
Transaction Security	• IP address information, website login and exit information, password and password information, etc.

CV Information	**For employee candidates;** • Your education information written in your CV document or **requested by Pleksus Pharmacovigilance** or given by you, school information related to your education, certificate information, education status and information about your training, • The place, date and duration information regarding your work experiences written in your CV document or **requested by Pleksus Pharmacovigilance** or given by you, information about the job and task you have worked before, all kinds of information about your working experiences, • Your photograph written on your CV or **requested by Pleksus Pharmacovigilance** or given by you, • Your driver's license written on your CV or **requested by Pleksus Pharmacovigilance** or issued by you and the information written on your driver's license, • References and information about your references written in your CV document or **requested by Pleksus Pharmacovigilance** or given by you.

Health Data	**From the employees;** • All kinds of health information and data taken while creating the personnel file (disability information, blood group information, personal health information,) **For Adverse Event Reporting from Patients;** • Medical history, concurrent disease information (e.g.: allergy, pregnancy, smoking/alcohol use, hepatic/renal failure, diabetes, hypertension, etc.), information on congenital anomalies (e.g.: medications used by the mother during pregnancy, diseases she was exposed to, date of last menstruation), drug information used, laboratory findings
Criminal Conviction Data	• Criminal record information obtained while creating the personnel file,
Customer Transaction	• Such as invoice, promissory note, check information, information on box office receipts, order information, demand information,
Legal Action	• Information in correspondence with judicial authorities, such as information in the case file,
Audio and Visual Recordings	• Call center records, closed circuit security camera recordings, photos and videos if you share them within the scope of corporate communication activities.
Risk Management	• Risk factors for adverse events
Physical Space Security	• Visitors' name, surname, visiting hours, camera recording, internet access information, visited person and other information.

7. GENERAL PRINCIPLES REGARDING THE PROCESSING OF PERSONAL DATA

7.1. Compliance with Law

Our company carries out its personal data processing activities in accordance with the law and good faith rules, in accordance with the Constitution, the PDP Law and the relevant legislation. In this context, our Company takes action by determining the legal grounds that will require the processing of personal data, takes into account the requirements of proportionality, does not use personal data other than what is required by the purpose, and does not carry out processing activities without the knowledge of individuals.

7.2. Accurate and Up-to-Date Data

Our company; It ensures that the personal data it processes is accurate and up-to-date, taking into account the fundamental rights of personal data owners and its own legitimate interests, and takes the necessary measures in this direction. In this context, all data on all categories of persons are tried to be kept up-to-date, and all kinds of administrative and technical measures are taken to ensure their accuracy and up-to-dateness.

7.3. Specific, Legitimate and Clear Purpose

Our Company processes personal data only for clearly and precisely determined legitimate purposes and does not carry out data processing activities other than these purposes. The purpose for which personal data will be processed by our Company is determined before the processing activity and **is processed in the** "Personal Data Inventory".

7.4. Data Being Relevant, Limited and Proportionate to the Purpose for which they are Processed

Personal data is processed by our Company to the extent necessary to achieve the specified purposes. Data processing activities are not carried out with the assumption that it can be used later. In this context, processes are constantly reviewed and **the principle of reducing personal data** is tried to be implemented.

7.5. Retention of Personal Data for as Long as Necessary and Subsequent Deletion

Our company retains personal data only for the period specified in the relevant legislation or required for the purpose for which they are processed. In this context, our Company first determines whether a period is stipulated for the storage of personal data in the relevant legislation, if a period is determined, it acts in accordance with this period, takes into account the civil and criminal statute of limitations in this context, and stores personal data for the period required for the purpose for which they are processed. In the event that the period expires or the reasons requiring processing disappear, personal data are deleted, destroyed or anonymized in accordance with our Company's "Data Destruction Policy".

8. CONDITIONS FOR PROCESSING PERSONAL DATA

Personal data may only be collected, processed, or used under the legal bases set out below.

8.1. Explicit Consent

Explicit consent in Article 3 of the Law; It is defined as "consent regarding a specific subject, based on information and expressed with free will". In addition, paragraph 3 of Article 20 of the Constitution stipulates that personal data can only be processed in cases stipulated by law or with the explicit consent of the person. Explicit consent is stipulated in Law No. 6698 as the main reason for compliance with the law in terms of both special categories of personal data and non-special categories of personal data.

Accordingly, personal data is processed by obtaining explicit consents declared by our company with free will and received in a provable manner (written, electronic or recorded oral). In case of processing of special categories of personal data, explicit consents will be obtained in writing when necessary.

Process managers who process personal data are obliged to control the existence and validity of the explicit consent of the relevant data owner while collecting the personal data they process. If it is determined that there is no explicit consent (except for the following exceptions), data processing will not be carried out.

8.2. Processing of Personal Data Without Explicit Consent

In the presence of one of the following conditions, it is possible to process personal data without seeking the explicit consent of the data subject:

a. It is clearly stipulated in the laws,
b. It is mandatory for the protection of the life or physical integrity of the person who is unable to express 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, it is necessary to process the personal data of the parties to the contract.
d. It is mandatory for the data controller to fulfill its legal obligation,
e. It has been made public by the data owner himself,
f. Data processing is mandatory for the establishment, exercise or protection of a right,
g. Provided that it does not harm the fundamental rights and freedoms of the data owner, it can be processed without explicit consent in cases such as when data processing is mandatory for the legitimate interests of the data controller.

8.3. Processing of Special Categories of Personal Data

Our company shows special sensitivity in the processing of special categories of personal data, the protection of which is more critical for data owners in various respects. In this context, provided that adequate measures determined by the Board are taken, such data are not processed without the explicit consent of the data owners. However, it can be processed without explicit consent, provided that adequate measures are taken and in the presence of the following reasons:

8.3.1. It is clearly stipulated in the laws,

8.3.2. It is necessary for the protection of the life or physical integrity of the person who is unable to express his/her consent due to actual impossibility or whose consent is not legally valid,

8.3.3. It is related to the personal data made public by the data subject and is in accordance with the will to make it public,

8.3.4. Being mandatory for the establishment, exercise or protection of a right,

8.3.5. It is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and planning, management and financing of health services by persons or authorized institutions and organizations under the obligation of confidentiality,

8.3.6. It is mandatory for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services and social assistance,

8.3.7. Provided that foundations, associations and other non-profit organizations or formations established for political, philosophical, religious or trade union purposes comply with the legislation and purposes to which they are subject, limited to their fields of activity and not disclosed to third parties; It is aimed at current or former members and members or people who are in regular contact with these organizations and formations,

In any case where special categories of personal data need to be processed, the PDPL Committee will be informed.

9. TRANSFER OF PERSONAL DATA

Your personal data is processed by our company in accordance with the law and good faith, accurately and up-to-date when necessary, for specific, clear and legitimate purposes, in connection with the purpose for which they are processed, limited and

measured, in accordance with the principles of retention for the period stipulated in the relevant legislation or required for the purpose for which they are processed.

Your personal data; In order to fulfill the legal obligations stipulated in the legislation for monitoring drug safety, provided that the public interest is taken into account, in accordance with the basic principles stipulated in the PDPL and within the personal data processing conditions and purposes specified in Articles 8 and 9 of the PDPL; It can be shared with the Ministry of Health, the Turkish Medicines and Medical Devices Agency, business partners and service providers (suppliers, consultants, legally authorized institutions and organizations and legally authorized private law legal entities from which storage, archiving, information technology support is received). Pharmacovigilance data can also be anonymized and entered into the database of the World Health Organization within the scope of the Drug Monitoring and Cooperation Program.

Some Pharmacovigilance data also need to be reported to other health authorities in Europe and around the world, including countries with varying levels of data protection. However, these reports contain detailed information about the incident and personal data is anonymous. (The initials of the patient's name are present and are not clearly reported)

10. RIGHTS OF RELEVANT PERSONS

10.1. Pleksus Pharmacovigilance will respond to the requests of the data subjects whose personal data it processes within 30 days within the scope of the following rights:

a. To learn whether personal data is processed,

b. Requesting information if personal data has been processed,

c. To learn the purpose of processing personal data and whether they are used in accordance with their purpose,

d. To know the third parties to whom personal data is transferred at home or abroad,

e. To request correction of personal data in case of incomplete or incorrect processing and to request notification of the transaction made in this context to third parties to whom personal data has been transferred,

f. Although it has been processed in accordance with the provisions of the PDP Law and other relevant laws, to request the deletion or destruction of personal data in case the reasons requiring its processing disappear and to request that the transaction made in this context be notified to third parties to whom personal data has been transferred,

g. To object to the emergence of a result against the person himself by analyzing the processed data exclusively through automated systems,

h. To request compensation for the damage in case of damage due to unlawful processing of personal data.

10.2. Data owners can apply within the scope of the above-mentioned rights with the information and documents that will determine their identity, by the methods specified below or by other methods determined by the Personal Data Protection Board, with the PDPL application form on the website.

11. PRIVACY AND DATA SECURITY MEASURES;

All personal data processed within Pleksus Pharmacovigilance are confidential and are subject to Article 12 of the Law. Stated in the article;

a) To prevent the unlawful processing of personal data,

b) To prevent unlawful access to personal data,

c) To ensure the protection of personal data,

It takes all necessary technical and administrative measures to ensure the level of security suitable for its purpose.

11.1. Technical Measures Taken to Ensure the Lawful Processing of Personal Data and to Prevent Unlawful Access to Personal Data

Pleksus Pharmacovigilance has taken all kinds of technical and technological security measures to protect your personal data and protects your personal data against possible risks. For example;

a. Network security and application security are ensured.

b. An authorization matrix has been created for employees.

c. Access logs are kept regularly.

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

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

f. Firewalls are used.

g. Personal data security is monitored.

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

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

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

k. Personal data is reduced as much as possible.

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

m. Penetration testing is applied.

n. Encryption is done.

11.2. Administrative Measures Taken to Ensure the Lawful Processing of Personal Data and to Prevent Unlawful Access to Personal Data

- A management framework has been established within the organization to initiate and control information security operation and implementation.

    1. PDPL Committee and Contact Person have been appointed and their job descriptions have been determined.
    2. PDPL Application channels have been determined.
    3. Violation, request/complaint management workflows have been determined.

- The Main Principles, policies and procedures regarding the processing and protection of personal data have been determined.

    1. Data Processing and Storage Policy Has Been Established.
    2. Personal Data Processing and Protection Policy has been established.
    3. A policy has been established for the security of sensitive personal data.

- Existing risks and threats within the scope of processed personal data have been determined.
- Training and awareness activities are carried out for employees on personal data security.
- In order to ensure that employees and contractors are aware of and fulfill their information security responsibilities, roles and responsibilities and job descriptions regarding data security have been determined.
- Confidentiality commitments are made.
- Clarification text has been published for employees, customers, suppliers, etc.
- The processes that require explicit consent have been determined and implemented.

- In-house periodic and/or random audits are carried out and carried out. It eliminates privacy and security vulnerabilities that arise as a result of audits.
- In terms of the purpose of processing, it is evaluated whether there is a need for the aforementioned personal data, and personal data is reduced as much as possible.
- In case the data is obtained by others unlawfully, necessary measures are taken by the employees to notify the relevant person and the Board as soon as possible.

11.3. Measures to be Taken in Case of Unlawful Disclosure of Personal Data

In the event that the processed personal data is obtained by others illegally, our Company will notify the relevant data owner and the Board as soon as possible (within a maximum of 72 hours).

12. CONDITIONS FOR DESTRUCTION (DELETION, DESTRUCTION AND ANONYMIZATION) OF PERSONAL DATA

In Article 138 of the Turkish Penal Code, Article 7 of the PDP Law. In accordance with the article and the "Regulation on the Deletion, Destruction and Anonymization of Personal Data" issued by the Authority; Although it has been processed in accordance with the provisions of the relevant law, **personal data is deleted, destroyed or anonymized based on Pleksus Pharmacovigilance's own decision or upon the request of the personal data owner,** in the event that the reasons requiring its processing disappear.**Pleksus Pharmacovigilance** has established a Policy in accordance with the provisions of the regulation on this issue and in accordance with this Policy, destruction is carried out according to the nature of the data. In accordance with this regulation**, periodic disposal dates have been determined by Pleksus Pharmacovigilance, and a calendar has been created according to the periodic destruction to be carried out at various intervals with the start of the obligation.**

13. EXECUTION

A management structure has been established by Pleksus Pharmacovigilance **to ensure that the execution of this Policy** is carried out in accordance with the regulations of the PDP Law.

14. EFFECTIVE DATE OF THE POLICY

This Policy entered into force on 17.02.2023 and was revised on 20.05.2025.