Joint Stock Company "Grindeks", 53 Krustpils Street, Riga, LV-1057, Latvia
E-mail: grindeks@grindeks.com, www.grindeks.com
Unified registration No. 40003034935

GRINDEKS PRIVACY POLICY

1. ABOUT US

1.1. Grindeks (hereinafter also **we**) is the leading manufacturer and distributor of medicines in the Baltic States. Our portfolio includes original products, generic medication, and active pharmaceutical ingredients.

1.2. The Grindeks Group comprises the joint stock company "GRINDEKS" and its subsidiaries. For clarity, within this Privacy Policy, "Grindeks" refers to the entire group, including its subsidiaries, representative offices, and branches abroad. However, some companies within the Grindeks Group have developed their privacy policies. Specifically, this Privacy Policy applies to the entire Grindeks Group, except for the joint stock company "Kalceks", HBM Pharma s.r.o., and Tallinna Farmaatsiatehase AS (Tallinn Pharmaceutical Factory). More information about the Grindeks Group can be found on our website.

2. PURPOSE OF THE PRIVACY POLICY

2.1. The purpose of this Privacy Policy (hereinafter referred to as "**the Policy**") is to provide information on how Grindeks processes the personal data of identifiable natural persons (hereinafter referred to as "**Data Subjects**") that come into our possession.

2.2. The Policy outlines how our subsidiaries process personal data and specifies what Grindeks may process. Please get in touch with us if you require more detailed information or have any questions while reading this Policy.

2.3. Grindeks processes personal data in compliance with the laws and regulations of the Republic of Latvia, the European Union, and other relevant laws and regulations in the field of privacy and data processing, including Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC (General Data Protection Regulation, (hereinafter – **GDPR).**

3. POLICY SCOPE

3.1. In some cases, Grindeks operates in retail, selling goods directly to end consumers. However, most of our clients are legal entities. According to Recital 14 of the GDPR, the regulation does not apply to processing personal data concerning legal persons, specifically those established as legal entities, including the legal person's name, form, and contact details. Additionally, in cases where an individual's personal data is related to commercial activities, it may, in certain situations, be considered as the data of a legal person. Therefore, this Policy does not apply to our customer and partner base where the requirements of the GDPR are not applicable.

3.2. However, under specific circumstances, we process personal data, and this Policy applies to any Data Subject whose personal data we process (except when anonymized). For example, this Policy is applicable when:

a) You visit our Website.

b) You report side effects or the quality of our medicines.

c) You visit Grindeks premises, where, among other things, video surveillance may be conducted, of which you will be informed through signage.

d) You receive services from us (e.g., by participating in events or training seminars we organized) or cooperating with us.

3.3. Regarding employment matters and the selection of candidates, Grindeks will provide additional information through relevant privacy statements.

3.4. Additionally, subsidiary companies or representative offices (branches) may have privacy policies that comply with their respective countries' mandatory data protection legislation. Our subsidiaries and representative offices (branches) are required to adhere to the mandatory data protection laws of their country of residence. In the event of a conflict between this Privacy Policy and the mandatory legislation of the country where the subsidiary or representative office (branch) is located, the required legislation of the country in question will take precedence.

4. EXPLANATIONS AND TERMS

4.1. This Policy has been prepared to present issues related to personal data protection as clearly as possible. However, certain definitions are used per the terminology provided in the GDPR:

a) **Personal Data**: Any information relating to an identified or identifiable natural person ("**Data Subject**"). An identifiable natural person can be identified, directly or indirectly, particularly by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
b) **Processing**: Any operation or set of operations performed on Personal Data or sets of Personal Data, whether by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
c) **Controller**: A natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.
d) **Supervisory Authority**: An independent public authority established by a Member State in compliance with Article 51 of the GDPR requirements.
e) **Website**: Refers to www.grindeks.com.

5. CONTROLLER AND CONTACT INFORMATION

5.1. The primary controller of personal data processing is the joint stock company "GRINDEKS," registration No. 40003034935, with its registered office at Krustpils Street 53, Riga, LV-1057. However, in certain cases, another subsidiary or representative office (branch) of Grindeks may act as the controller of personal data processing. If you require more specific information about the processing of Personal Data about your situation, please get in touch with us.

5.2. If you have any questions or concerns regarding this Policy or the processing of Personal Data, please email grindeks@grindeks.com or contact us personally at the legal address provided.

.

6. WHAT PERSONAL DATA DO WE PROCESS? WHAT IS THE PURPOSE AND LEGAL BASIS OF DATA PROCESSING?

6.1. We process different types of Personal Data, which largely depend on the services used by the Data Subject, or the activities performed by the Data Subject himself or herself. For the provision

of our services under the requirements of regulatory enactments and the performance of other functions, it is necessary to process your Personal Data. For example, the processing of your Personal Data may be carried out for the following reasons:

PURPOSE	CATEGORIES OF PERSONAL DATA	LEGAL BASIS
Ensuring general communication (not relevant for adverse drug reactions): We collect and process questions, suggestions, complaints, and other information to prepare responses and ensure effective communication with you. Communication can occur via email, mail, phone, or in person, depending on how you contact us.	Name, contact information, and other personal information contained in the question, suggestion, or complaint.	• Consent of the data subject: By submitting this information to us, you consent. • Our legitimate interest in ensuring effective communication.
Adverse Reaction Monitoring (Pharmacovigilance): Pharmacovigilance is a system designed to detect and effectively address the undesirable effects of our drugs on time. One of the key tools in this system is monitoring adverse reaction reports from all countries where our medicines are authorized. Reporters may include medical practitioners,	The adverse reaction report should include the following information: • Patient data • Data on the submitter of the report • Data on the medicinal product used • Details of the adverse reaction • Cited data	The legal basis may vary depending on the reporter, such as whether the report is submitted by the consumer (patient) or a medical practitioner (pharmacist). • Processing personal data is necessary to fulfill our legal obligations related to the safety of medicinal products, as required by regulatory enactments. • For additional issues, the data subject consents by actively providing this information to us or a medical treatment institution. • It is in our legitimate interest to promote effective pharmacovigilance and maintain a robust system for monitoring adverse reactions. The exception for the processing of health data is:

consumers, pharmacists, and others.	More information about the personal data processed is available on our Website's adverse reaction reporting form.	• GDPR Article 9(2)(a) or the consent of the data subject. GDPR Article 9(2)(i) or the processing of personal data is necessary for reasons of public interest in public health, such as ensuring high standards of quality and safety for medicinal products, based on European Union or Latvian law, which provides for appropriate and specific measures to protect the rights and freedoms of the data subject, particularly confidential information.
Clinical examination: • Clinical examinations encompass a range of activities to ensure the examination's quality, safety, and compliance with regulatory standards. These tests vary in nature, including studies for new and existing products. Data Subjects participating in clinical trials will receive additional information on processing their Personal Data • Preparation and maintenance of clinical trial documents, including archiving • Involvement and selection of participants • Data collection and management including collecting data from participants for the clinical trial • Communication with stakeholders, including study participants, study teams, and supervisory authorities	Depending on the nature of the study, various types of Personal Data may be processed. As the sponsor, we typically only receive pseudonymized data about participants. **Research centre staff data**: Name, surname, contact details, CV information, including professional experience and education. **Test Participants' Data:** **Identification data:** Name, surname, date of birth, sex data of the identity document. **Contacts:** Phone number, e-mail. **Physical parameters and characterization data:**	• Consent of the Data Subject: Participants provide consent to participate in the clinical trial through active actions. Based on our contractual relationship with the involved parties (e.g., researchers), we may receive data. • Contractual Basis: This includes contracts between us and research personnel for the conduct of clinical trials. • Compliance with Legal Obligations: Processing of personal data is necessary to comply with legal obligations related to inspections. • Legitimate Interest: Ensuring and improving an efficient and secure research process. Exception for Processing Health Data: • GDPR Article 9(2)(a): Consent of the data subject • GDPR Article 9(2)(i): Processing of personal data is necessary for reasons of public interest in the field of public health, such as ensuring high standards of quality and safety for medicinal products, based on Union or Latvian law, with appropriate and specific measures to protect the rights and freedoms of the data subject, particularly regarding confidentiality.

• Safety evaluation, including the preparation of **adverse drug reaction** reports • Audit or monitoring of the clinical trial to ensure compliance with protocols, standard operating procedures, and relevant regulatory requirements • Data analysis and interpretation of results, including, in some cases, additional studies • Publication and submission of results to regulatory authorities to register medicinal products. High data safety standards are observed during clinical trials, with data being pseudonymized per legal requirements.	Weight, height, information on diet, physical activity, lifestyle, etc. **Health data**: Health history, medications used (including doses), history of allergies, laboratory test results (assessment of reactions, diagnosis, severity of adverse reactions), information on pregnancy and breastfeeding, information on alcohol and drug use, surgical manipulation data, vaccination information, psychological state data, clinical status data before and after administration, etc. **Biological samples:** Blood, urine, saliva, and other biological samples.	
Within the framework of business: To provide our services and facilitate product sales, we process your Personal Data for various purposes, including: • Verifying your identity, such as authorization to enter into legal transactions on behalf of a legal entity	**Identification Data and Contact Information:** Name, surname, date of birth, personal identification number, address, telephone, email, etc. **Partner research information:** Information about the partner, including publicly available	• Processing is necessary for the performance of a contract (e.g., a service contract between us). • Processing is necessary to comply with legal obligations (e.g., customer due diligence, record-keeping). • Legitimate Interest: for example, improving our services, checking U.S. sanctions lists, etc. • In exceptional cases, the data subject provides consent by actively submitting information to us.

• Ensuring compliance with legal or internal regulatory requirements (e.g., conflict of interest prevention, business partner inspections, economic sanctions checks, compliance with supply chain and quality requirements, customs and export regulations, product traceability) • Fulfilling our contractual obligations related to any service or product you use • Ensuring effective communication with you • Organizing record-keeping, accounting, and payments • Analysing, evaluating, and improving our services and products for quality control purposes • Making and receiving bank transfers, as necessary for fulfilling contractual obligations or complying with the law, or for safeguarding legitimate interests • Recovering debts and exercising other rights.	sources such as media and databases **Services Used and Products Purchased:** for example, Payment information and payment history **Record-Keeping Documents**: Documentation, correspondence, and contracts containing Personal Data **Information on debt obligations:** for example, debt-related information, including amounts owed	
Entry/Exit Control of Natural Persons: To ensure safety, joint stock company "GRINDEKS" has implemented strict security measures, including the control of entry and exit of individuals and monitoring activities,	Information about the visit, such as name, time and visit date.	• Our legitimate interest, is to effectively organize entry and exit control.

such as card registration and log maintenance. Following regulatory enactments, as an object of increased danger, our company has a strict security system with a pass system limiting access to staff and visitors. Visitors can stay in the territory of our company only if employees of our company accompany them, and they must comply with the internal rules of procedure established by the company.		
Video surveillance: To protect property against crimes such as theft, robbery, and vandalism, we use video surveillance to ensure the safety and health of employees and visitors. This allows for the timely detection and prevention of incidents or violations. Video surveillance may also be used in anonymized form for employee training purposes. Surveillance is not conducted in areas where individuals expect greater privacy, such as	Height, facial image, physical characteristics, time, and location within our premises	• Our legitimate interest in the protection of property. • Vital interests of the data subject, ensuring safety, particularly given our status as an object of increased danger.

recreation areas or changing rooms. CCTV camera recording areas focus on hallways, entrances/exits, building perimeters, and other high-risk areas.		
Seminars, Excursions, and Events: We organize and support various events, including seminars, excursions, and other activities, to raise our company's profile and achieve other goals, such as promoting education and attracting new specialists. Events are organized for different groups, including schoolchildren, students, trainees, and medical practitioners. We will inform you if any events are being photographed or recorded.	Participation in events may require submitting your application, for which various personal data must be indicated. For example, your name and contact information. If we organise events for medical practitioners, additional information about participation is also processed to administer (further-)education points/certifications. If events take place at our premises, we will also administer information about the visit for issuing passes. In addition, photographs and video recordings may be taken at events.	**Legitimate interest**: to promote and promote the recognition of the Grindeks brand among industry specialists, as well as to the public, as well as to promote commercial activities.
Posts About Current Events: To provide news and information to the public, we prepare records of events,	The recordings we make may contain photographs and video recordings, as well as other Personal Data,	Legitimate interest – to promote and promote the recognition of the Grindeks brand among industry specialists, as well as to the public, as well as to promote commercial activities.

seminars, and activities organized or sponsored by us, which may be published on our Website and/or social networks like Facebook. We adhere to high ethical standards to ensure that the use of personal data does not harm your rights and freedoms. If you have concerns about the processing of your Personal Data, you can contact us and object to the relevant data processing. You may also request that your image not be included in photographs or videos where you are clearly identifiable or avoid appearing in photos or videos during our events. However, at large events, it may be challenging or impossible to fully comply with such requests.	such as the names of participants.	
Commercial Communications to Medical Practitioners This communication is intended to personalize the content provided to healthcare professionals and includes information on the following topics:	**Contact information**: name, address, private or work email address. **Workplace and specialization**: Information regarding your workplace(s) (e.g., medical treatment institution)	• Consent of the data subject – medical practitioner. • Our legitimate interest in sending commercial communications, as permitted by the regulatory framework, such as Article 9 of the Law on Information Society Services.

• Grindeks Seminars, Lectures, and Events: Invitations and details about seminars, lectures, and other events organized for medical practitioners. • Grindeks Products: Comprehensive information about our products, including usage instructions, packaging, dosage, supplements, changes in descriptions, and recommendations. • Grindeks News: Updates and other relevant information about current affairs at Grindeks. You can unsubscribe from receiving commercial communications at any time. For example, by pressing the corresponding link in the email. Please note that processing your unsubscription request may take up to 5 working days, depending on technological capabilities.	and your medical specialization. **Information on the type of information/type of products that the medical practitioner wishes to receive** information about what information or product offers the doctor wants to receive, for example, topics.	
For the fulfilment of legal obligations, exercise of rights and other legitimate purposes: We process your Personal Data to: • in cases provided for by law, hand them over to	Depending on the specific situation. This includes documentation, correspondence and contracts containing your Personal Data.	• The processing of Personal Data is necessary to comply with legal obligations applicable to Us, as determined by regulatory enactments. • We also process your data following our legitimate interests, for example, protecting us in cases of legal proceedings.

public authorities (e.g. anti-tax and financial fraud authorities, etc.). • to help detect or prevent criminal offences or other offences. • to pursue their interests in cases of legal proceedings or claims.	

7. FROM WHAT SOURCES DO WE OBTAIN PERSONAL DATA?

7.1. We may collect Personal Data through the following sources**:**

a) **Directly from You:** We obtain Personal Data directly from you as data subjects, for example, when you submit questions, proposals, or complaints**.**

b) **Created Through Activities:** Personal Data is generated because of our activities, such as payments made, products and services used, cookies, and video surveillance records**.**

c) **Adverse Reaction Reports:** We may receive reports of adverse drug reactions from medical practitioners and other reporters, including doctors, pharmacists, distributors, importers (including parallel importers), and parallel distributors.

d) **Received from Grindeks representative offices, branches or group companies**: Personal Data may be received from Grindeks' representative offices, branches, or group companies.

e) **From Cooperation Partners and Institutions:** We may obtain Personal Data from public authorities or other cooperation partners, such as researchers providing pseudonymous data from clinical trials.

f) **Public and Private Registers:** In certain cases, we may acquire data from public registers and databases, such as Lursoft or state registers pertaining to relevant licenses.

8. HOW LONG DO WE KEEP PERSONAL DATA?

8.1. Grindeks retains Personal Data under the following conditions:

a) Personal Data is stored as long as necessary to meet obligations established by regulatory frameworks, such as accounting requirements.

b) If Personal Data is processed based on your consent, it is retained as long as the consent is valid and not withdrawn.

c) Personal Data is kept for as long as necessary to fulfil the specified purpose of processing and to consider legitimate interests (e.g., addressing requests, protecting rights, resolving issues, and adhering to limitation periods for actions).

8.2. Individual video recordings are retained for up to 30 days unless the footage indicates potential illegal activity or information that could assist Grindeks or third parties in protecting legal interests. In such cases, the recording will be kept until the legal interest is resolved.

8.3. Clinical trial master files are stored for at least 25 years.

8.4. Photos and videos from events released by Grindeks are intended to be stored permanently as part of an archive. This archive provides evidence of the relevant period and historical information about Grindeks' evolution, including the expansion of services and products.

8.5. When the retention period for Personal Data expires, Grindeks will ensure that the data is securely deleted, archived, or anonymised so that it can no longer be linked to you.

9. WHERE IS YOUR PERSONAL DATA STORED?

9.1. We strive to process Personal Data within the EU/EEA wherever possible.

9.2. However, Personal Data may be transferred and processed outside the EU/EEA when necessary and legally justified, for instance, if the project involves data subjects from countries outside the EU/EEA or includes Group companies located outside the EU/EEA. If such transfers are necessary, we will comply with GDPR requirements and established procedures to ensure adequate protection of Personal Data.

10. TO WHOM IS YOUR PERSONAL DATA TRANSFERRED?

10.1. We may transfer your Personal Data to other recipients to provide services or as necessary. We ensure that only the information required for the specific purpose of processing is provided.

10.2. Personal data may be transferred to the following recipients, such as:

a) **Within Grindeks Group**: Other companies within the Grindeks Group.

b) **Cooperation Partners**: Service providers, such as IT system maintainers or pharmacovigilance processing service providers, with whom Grindeks has contracts that include data protection requirements. These partners must ensure an equivalent level of data security.

c) **Regulatory Institutions**: Pseudonymized data on clinical trial participants may be transferred to institutions like the State Agency of Medicines for study supervision, regulatory compliance, safety, efficacy verification, adverse reaction monitoring, and legal reporting requirements.

d) **Authorized Persons**: Data may be shared with authorized individuals upon their written, clear, and unambiguous request, provided their identity is verified.

e) **Law Enforcement and Judicial Authorities**: Data may be disclosed to law enforcement, courts, or other authorities if there is a legal basis and the purpose and legal grounds for the request are specified.

f) **Supervisory Authorities**: Data may be transferred to courts or supervisory authorities in cases where Grindeks has a legitimate interest or to comply with legal obligations.

g) **Banks**: For payment administration.

h) **Debt Collection Companies**: Personal Data may be transferred to debt collection agencies concerning outstanding debts.

i) **Public Access**: Photos and videos from events may be made available to an unlimited range of interested parties, including visitors to our Website or readers of publications.

11. WHAT RIGHTS DOES THE DATA SUBJECT HAVE?

11.1. You have the following rights concerning the protection of Personal Data:

a) **Right to Access:** You may request access to your data by specifying the period and data you wish to obtain. You are entitled to know what data we hold, the purpose of

processing, how it was obtained, and to whom it has been transferred. Detailed requests and specifying your purpose for accessing the data will expedite the process.

b) **Right to Rectification:** If you need to correct or update your Personal Data, clearly indicate the data to be corrected and provide the correct information. If the data was not obtained from you, include a justification for why the information is inaccurate to facilitate a prompt assessment.
c) **Right to Erasure:** To request the deletion of your data, specify which data should be removed and provide justification. Note that data deletion may not always be possible.
d) **Right to Restrict Processing:** If you have concerns about the appropriateness of data processing, you can request a restriction on processing certain data. Indicate why you believe the restriction is necessary.
e) **Right to Object:** You may object to data processing on individual grounds. Your request should detail your specific circumstances for the objection.
f) **Withdrawal of Consent**: If we process data based on your consent, you have the right to withdraw it at any time. We will cease processing your data for the purpose for which you consented. Withdrawal of consent does not affect the legality of processing before the withdrawal.
g) **Right to Data Portability:** If you wish to transfer your Personal Data to another controller or yourself, specify the data you want to transfer.

11.2. Requests for exercising your rights can be submitted:
a) **In-Person:** By presenting an identity document for verification.
b) **Electronically:** By sending a signed request via e-mail with a secure electronic signature.
c) **By Registered Mail.**

11.3. We will respond to your request without undue delay and no later than one month from receipt. If more time is needed, we may extend the response period by up to two months and will inform you within one month.

11.4. We may refuse to process a request or charge a reasonable fee if it is manifestly unfounded, excessive, or in other cases stipulated by regulatory enactments.

11.5. We have the right not to fulfil your request if:
a) It is not clearly formulated.
b) We cannot verify your identity.
c) We have already addressed a similar request.
d) The amount of information requested is disproportionate.
e) The request is unfounded and lacks explanation.
f) Regulatory enactments prevent us from providing certain information or require data retention.

11.6. If you have concerns about how we handle your Personal Data, you may file a complaint with us. If you believe we have processed your data improperly, you have the right to complain to the Supervisory Authority. In Latvia, this is the Data State Inspectorate. Contacts for all EU supervisory authorities are available here.

12. PROTECTION OF PERSONAL DATA

12.1. We continuously implement and enhance data protection measures to safeguard your Personal Data from unauthorized access, accidental loss, disclosure, or destruction. We address specific risks associated with data processing, including accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

12.2. We use appropriate technical and organizational measures, including firewalls, intrusion detection systems, analysis tools, and data encryption.
12.3. We carefully evaluate all cooperation partners who process Personal Data on our behalf to ensure they comply with data protection requirements and provide adequate security measures.
12.4. We ensure that any individuals acting under our authority who access Personal Data do so only according to our instructions unless required by regulatory enactments.
12.5. We comply with data processing and protection requirements as stipulated by regulatory enactments. In the event of a personal data breach that poses a high risk to your rights and freedoms, and if no exceptions apply as per Article 34(3) GDPR, we will notify you without undue delay.

13. COMMUNICATION WITH THE DATA SUBJECT

13.1. We communicate with you using the contact information you provide (phone number, email address, or postal address). Communication related to contractual obligations is conducted based on the details specified in the contract.
13.2. For other cases, we will contact you based on your request, adhering to your preferred communication method and regulatory requirements.

14. FINAL PROVISIONS

14.1. The Company reserves the right to amend this Policy.
14.2. Any updates to this Policy will take effect on the date specified in the revised version.
14.3. To ensure transparency and fairness, the latest version of the Policy is always available on our Website.
14.4. In case of discrepancies between translations of this Policy, the Latvian version will prevail.
14.5. This Policy applies from September 5, 2024.