PRIVACY POLICY

CONTENTS

Data Controller

This Privacy Policy describes how the data controller UAB “TAMRO”, legal entity number 111448632, address: Gamybos g. 4, Ramučių k., Kauno r. sav., Lithuania (further in the text referred to as the Company, We/Us or the Data Controller) processes personal data. UAB “TAMRO” is part of the international **PHOENIX group** operating in 27 European countries.

Data Protection Officer

If You would like to clarify or find out how the Company processes Your personal data, or if You intend to exercise Your rights as a data subject, please contact at dpo.lt@tamro.com or the Company’s postal address, indicating that the correspondence is addressed to the Data Protection Officer.

Application of the Privacy Policy

For the purposes of this Privacy Policy, “personal data” means any information that can be used to directly or indirectly identify You. Terminology used in this Privacy Policy, such as the “data controller” and “data processor”, have the meanings defined in the General Data Protection Regulation (the Regulation) and other relevant legislation.

This Privacy Policy applies to all individuals, including but not limited to: suppliers and users of Our services and products; visitors to Our websites or applications; customers who cooperate with Us.

We ensure that Our employees, shareholders and members of Our governing bodies are informed about the processing of their personal data in the manner defined in Our internal rules.

Sources of personal data

We obtain Your personal data from the following sources:

- **directly from You**. We process Your personal data that You provide to Us. For example, when You use Our services, share Your CVs, resume cover letters and communicate with Us by phone calls and emails;
- **via Our website**. When You browse Our website, certain information (such as Your Internet Protocol (IP) address and the type of the web browser You are using) is collected automatically;
- **from devices**. For example, if You visit Our Company’s premises, which are monitored by CCTV cameras, certain personal data may be collected;
- **from third parties**. We may also obtain Your personal data from third parties in the manner set out in the law and/or this Privacy Policy. For example, Your personal data is obtained from Our customers when You are a representative of a legal entity.

Please note that You are not obligated to provide any personal data, but We might be unable to provide You with the services and achieve other defined purposes without such data.

Personal data processing operations

Finding job candidates

As part of the recruitment process and the administration of the job candidate database, We process the following personal data of job candidates: the name, surname, length of service and work history, photo, education, personal phone number, personal email, information on IT and language skills, contact details, job title, and any other information volunteered by candidates.

Legal basis: Article 6(1)(b) of the Regulation – entering into and performance of a contract with the data subject, Article 6(1)(a) of the Regulation – consent of the data subject (after the candidate selection).

Retention period: Data will be stored until the end of the candidate selection. With the consent of the data subject, the data will be retained for 1 year after the candidate selection.

Wholesale and retail pharmaceutical services

Registration of adverse reactions to medicinal products

When recording adverse reactions to medicinal products, We process the following personal data of Our customers (patients): initials of their name and surname, their age, sex, weight, height, the medicinal product used, other medication used, the start, end, duration of the use, a description of the suspected adverse reaction, relation of the suspected adverse reaction to clinical trials, results of trials, other additional information relevant to the investigation of the suspected adverse reaction.

Legal basis: Article 6(1)(c) of the Regulation – a legal obligation, Article 6(1)(f) of the Regulation – legitimate interests of the data controller in the processing of the personal data of healthcare professionals, Article 9(2)(i) of the Regulation – data processing is necessary for reasons of public interest in the field of public health.

Retention period: 10 years.

Data recipients: the State Medicines Control Agency, pharmaceutical manufacturers.

Recall of a product from the market

In cases of product recalls, We process the following personal data of customers' representatives, manufacturers' representatives and purchasers: the name, surname, place of work (only for representatives of manufacturers and customers), contact details (telephone number and email address), history of medicinal products purchased (only for purchasers).

Legal basis: Article 6(1)(b) of the Regulation – entering into and performance of a contract with the data subject, Article 6(1)(f) of the Regulation – legitimate interests of the data controller to process contact details of representatives of legal entities, Article 9(2)(i) of the Regulation – processing is necessary for reasons of public interest in the field of public health.

Retention period: 10 years.

Data recipients: pharmaceutical manufacturers, regulatory authorities.

The supplier's audit report, the service provider's approval (wholesale distribution), Good Pharmacy Practice (GPP), internal audits

The following personal data of customers, service providers, suppliers of goods, employees is processed: the name, surname, contact details, place of work, employee qualifications.

Legal basis: Article 6(1)(f) of the Regulation - the legitimate interest of the data controller in carrying out audits.

Retention period: 10 years.

Collaboration with healthcare professionals, presentation of pharmaceutical and promotional materials

We process the following personal data of healthcare professionals who are experts: the name, surname, contact details, workplace, specialisation, date and time of visits, bank account number, list of participants, signature.

Legal basis: Article 6(1)(a) of the Regulation – consent of the data subject, Article 6(1)(b) of the Regulation – entering into and performance of a contract with the data subject.

Retention period: 10 years from the end of the business relationship.

Data recipients: the State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania, the State Social Insurance Fund Board under the Ministry of Social Security and Labour.

Maintenance of information on cash and non-cash transactions

We adhere to the principle of transparency, follow the Disclosure Code of EFPIA and the Code of Ethics of the Lithuanian Innovative Pharmaceutical Industry Association, and process the following personal data of healthcare professionals, participants, cash and non-cash transaction beneficiaries: the name, surname, contact details, date of birth, place of work, specialisation, email address, signature, address of the health facility. Cash and non-cash transactions may include fees paid by UAB "Tamro" for services rendered by healthcare professionals, as well as travel or accommodation costs incurred by healthcare professionals or another entity (e.g., representatives), also their training costs, e.g., for participation in medical congresses, and costs paid or reimbursed by UAB "Tamro" for the benefit of such healthcare professionals (directly or indirectly).

Legal basis: Article 6(1)(a) of the Regulation – consent of the data subject (to the sharing of personal data with business partners); Article 6(1)(c) of the Regulation – a legal obligation (to provide personal data to the State Medicines Control Agency under the Ministry of Health of the Republic of Lithuania); Article 6(1)(f) of the Regulation – the data controller's legitimate interest to comply with the principle of transparency and take legal action.

Retention period: 10 years.

Recipients: the Company shares personal data and information about cash and non-cash benefits received (or to be received) by healthcare professionals from the Company and its business partners, in accordance with the provisions concerning cash and non-cash transactions of the Disclosure Code of the EFPIA and the Code of Ethics of the Lithuanian Innovative Pharmaceutical Industry

Association. Personal data is transferred to PHOENIX group companies, its business partner GSK Services Unlimited or related companies; service providers.

The data are also submitted to the State Medicines Control Agency under the Ministry of Health of the Republic of Lithuania and made publicly available on its website www.vvkt.lt.

Provision of support

When providing support, We process the following personal data of applicants' representatives, doctors and beneficiaries: the name, surname, job title, date of birth, initials of beneficiaries.

Legal basis: Article 6(1)(f) of the Regulation – the legitimate interest of the data controller to provide support; Article 6(1)(c) of the Regulation – a legal obligation; Article 9(a)(h) of the Regulation – consent of the data subject.

Retention period: 10 years.

Data recipients: the State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania.

Business administration

Business Partner Due Diligence

The electronic Business Partner Due Diligence System (BPDDS) developed by PHOENIX Group allows Us to check whether the business partner We are planning to sign a contract with is not on any international sanctions lists, as communication with sanctioned partners is prohibited by law. The verification through the BPDDS involves the processing of company data (the name, registration details, information on the services provided) and, in a second stage, it may involve processing of data (the name, surname, position) of natural persons (managers/owners of the company, employees, as well as natural persons who provide services personally (health professionals) under contracts concluded with them).

Legal basis: Article 6(1)(f) of the Regulation – legitimate interests of the data controller in ensuring compliance with the law; Article 6(1)(b) of the Regulation – performance of a contract.

Retention period: 10 years.

Data recipients: companies in the PHOENIX Group.

Scanning of emails to ensure antitrust compliance

For the purpose of avoiding and early detection of possible antitrust infringements and inappropriate wording in emails, We process the following personal data of employees and/or representatives of business partners: their email address, emails, attachments. Emails received and sent by relevant employees (who are subject to this process) are searched for the recipient's email address and search keywords, and copied where necessary. The searches are intended to look for (i) certain words in the emails AND (ii) certain external email domains as well as business contact details and correspondence.

Legal basis: the legitimate interest of PHOENIX and third parties in ensuring compliance with antitrust rules and protecting their business.

Retention period: all copied emails are manually deleted after 2 weeks (if not required for further action).

Data recipients: only authorised members of the Compliance Team.

Contract administration

We process the following personal data of service providers, recipients and their representatives and responsible employees: the name, surname, date of birth, contact details, subject matter of the contract, address, business license number, individual activity certificate number (for independent contractors), power of attorney, signature.

Legal basis: Article 6(1)(f) of the Regulation – legitimate interests of the data controller to process personal data of representatives of legal entities (if the party to the contract is a legal entity), Article 6(1)(b) of the Regulation – entering into and performance of a contract with the data subject (if the party to the contract is a natural person).

Retention period: 10 years.

Data recipients: postal service providers, other business partners.

Handling of requests, complaints and enquiries from individuals

When responding to requests, enquiries or complaints about Our services and products, We process the following personal data of Our customers and patients: the name, surname, contact details, and the information provided in the enquiry or complaint.

Legal basis: Article 6(1)(c) of the Regulation – a legal obligation arising from the Law of the Republic of Lithuania on Documents and Archives; the Rules on Preparation of Documents; and the Rules on Document Management and Accounting.

Retention period : 1 year from the end of the examination of complaints and enquiries.

Recipients: addressees.

Internal and external audits

As part of Our internal and external audits, We may process all personal data of partners, suppliers, customers, patients and their representatives processed by the Company.

Legal basis: Article 6(1)(f) of the Regulation – the legitimate interest of the data controller in carrying out audits, Article 9(2)(f) of the GDPR – processing is necessary for the establishment, exercise or defence of legal claims.

Retention period: 10 years.

Data recipients: internal and external auditors.

Ensuring security of property and persons (video surveillance)

For the purpose of ensuring the security of property and persons, We carry out video surveillance and process the following personal data of the persons in the surveillance field: video recordings, the image, time and date of a video recording, the car registration numbers.

Legal basis: Article 6(1)(f) of the Regulation – legitimate interests of the data controller in ensuring the security of property and persons.

Retention period: data is stored for 90 days.

Data recipients: service providers.

Recording phone calls

For the purpose of ensuring the quality of appropriate consultations on the services provided by the Company, and for the purpose of confirming the content of conversations, We record conversations and process the following personal data of the persons who have called the Company: the telephone number, date of conversation, time of conversation, duration of the conversation, and a recording of the conversation.

Legal basis: Article 6(1)(a) of the Regulation – consent of the data subject to the recording of telephone conversations; Article 6(1)(f) of the Regulation - legitimate interests of the data controller to ensure the content of the conversations and the quality of the service.

Retention period: data is stored for more than 30 days.

Data recipients: service providers.

Organising and conducting online meetings, conference calls, video conferences, webinars

To ensure organisation of online meetings as well as convenient and secure communication, We process the following personal data of the persons participating in online meetings: the information about the participants (their names, surnames), data about the meeting (the topic, IP address of the participants, the start and end time of a video conference), recordings (not required), and text data (if required).

Legal basis: Article 6(1)(a) of the Regulation – consent to the recording of the meeting; Article 6(1)(f) of the Regulation – legitimate interests of the data controller in ensuring convenient online communication.

Retention period: the data collected for this purpose are processed for a period of time set by the operators of the online meeting platforms.

Data recipients: service providers.

Marketing

Conducting direct marketing

We send emails to customers about the Company's goods and services, We also send surveys, and process the following personal data of direct marketing recipients: the name, surname, telephone number, email address.

Legal basis: Article 6(1)(a) of the Regulation – consent of the data subject, Article 6(1)(f) of the Regulation – legitimate interests of the data controller to inform customers about the goods and services provided by the Company and to collect statistical information on the readership of direct marketing messages.

Retention period: 2 years.

Data recipients: service providers.

Processing of personal data on social media

The information that You provide on social network profiles operated by the Company (including messages, use of the "Like" and "Follow" buttons and other communications) or the information obtained when You visit the Company's accounts (including information obtained by means of cookies used by social media operators) is controlled by the social media operator with whom the Company acts as a joint data controller. We therefore recommend that You should read the privacy notices of the social media operator, where You can find all the information about the categories of personal data collected, the retention periods and the recipients.

Legal basis: Article 6(1)(f) of the Regulation – the legitimate interest of the data controller in ensuring the development and visibility of the business.

As the administrator of a social media account, We choose the appropriate settings based on Our target audience and Our performance management and promotion objectives. The social media operator may have limited the ability to change certain, essential settings when enabling the Company to create and administer a social media account, and thus We cannot influence what information the social media operator will collect about You after the Company has created a social media account.

Any such settings may affect the processing of personal data when You use social media, visit the Company's account or read the Company's posts on the social media network. Even if You only look at Our posts, the LinkedIn social network manager may receive certain personal information, such as which terminal device You are using, what Your IP address is, etc.

Retention period: based on settings of social media.

Data recipients: social media operators.

Protection of information

Reporting system

PHOENIX Group and its subsidiaries, including UAB “Tamro” and BENU Vaistinė Lietuva, UAB, have developed a web-based reporting system that allows employees, business partners, customers and third parties to report incidents and events easily. Such reports are taken seriously and analysed, and regular measures are taken to improve the protection of personal data.

The reporting tool is available at any time at https://phoenixgroup-databreach.integrityplatform.org/

To explain the reporting system in more detail, We have answered some frequently asked questions which are listed below:

When should I report an incident?

The PHOENIX Group is obligated to inform the supervisory authority within 72 hours of becoming aware of an incident, which is why all incidents have to be reported via the online reporting tool.

Which data-related incidents should be reported and how?

All incidents involving personal data should be reported to the data protection officers via the online reporting tool https://phoenixgroup-databreach.integrityplatform.org/.

What is a data protection incident?

A data protection incident is any event that results in, or may result in, the accidental or intentional loss of personal data (whether electronic or stored in paper format), or the destruction of data, or the unauthorised retrieval of data (e.g., a loss or theft of a laptop, a smartphone, paper documents, prescriptions).

What happens when I report an incident?

Data protection professionals will review the details of the incident and contact You for further information or, where necessary, help You take action after the incident.

Detection of security incidents

In order to detect, assess and respond to information security incidents, We process the following personal data of Our customers, suppliers, business clients and their representatives: the IT usage data / logs, IP address, contact details, name, surname, call, system login information, address, location.

Legal basis: Article 6(1)(f) of the Regulation – the legitimate interest of the data controller in enhancing information security.

Retention period: up to 1 year.

Imitating phishing emails

PHOENIX Group sends simulated phishing emails to inform representatives of business partners about potential phishing attacks and processes the following personal data of representatives of business partners: the email address, contact details.

Legal basis: Article 6(1)(f) of the Regulation – the legitimate interest of the data controller to send simulated phishing emails and enhance information security.

Retention period: 3 months.

Guaranteeing security of the digital environment of PHOENIX Group

We process the following personal data of customers, suppliers, contact persons of business partners, applicants: the address, IT usage data / log data / log files, IP address, contact details, name, call, title, location data, system connection information.

Legal basis: Article 6(1)(f) of the Regulation - the legitimate interest of the data controller in enhancing information security.

Retention period: 6 months.

Ensuring security of guest Wi-Fi network

To ensure network security and to protect the network infrastructure from unauthorised activities, We manage the use of Our guest Wi-Fi network and process the following personal data of the persons connected to the network: the connection time, IP address, MAC address of the device, the type of the device used, volume of traffic, network services used (e.g., DNS queries, web pages visited).

Legal basis: Article 6(1)(f) of the Regulation – legitimate interests of the data controller in ensuring network security and access control.

Retention period: data are stored for a maximum period of 12 months.

Internet traffic inspection (SD-WAN)

Normally, all data traffic on the Company's network is subject to full SSL inspection, so even *transport-encrypted* data *transmissions* can be decrypted and systematically filtered. Data processed for this purpose include the IP address of the sender and recipient, the active directory user name, the destination address (https://... / email address, etc.), the name of the associated application (e.g., Outlook), the timestamp of the call to the inspected transmission, and the result of the content check.

Legal basis: Article 6(1)(f) of the Regulation – the legitimate interest of the data controller in ensuring data security. Full SSL inspection of internet traffic ensures the long-term reliability, integrity, availability and resilience of the Company's systems (Article 32(1)(b) GDPR).

Retention period: the results of inspections are stored in log records for 7 days, the content of the documents inspected is not kept.

Recipients of personal data

We may provide Your personal data to the following persons or entities, taking into account the basis for the provision of the data and ensuring security of the data transmitted: to the companies belonging to the same group of companies, state authorities, law enforcement agencies and other persons in the procedure prescribed by the legislation of the Republic of Lithuania or where the provision of data is necessary to establish, exercise or defend the Company's legal claims; the State Social Insurance Fund Board; auditors; business partners; carriers of goods; companies providing electronic payment services; the State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania; the State Data Protection Inspectorate; the Ministry of Health of the Republic of Lithuania; the state enterprise Centre of Registers (*Registrų centras*); the State Medicines Control Agency under the Ministry of Health of the Republic of Lithuania; pharmaceutical manufacturers; companies providing postal services; outsourced data processors (server administrators, cloud service providers, IT service providers, etc.).

If We disclose Your personal data to other groups of recipients than those specified in this Privacy Policy, We will inform You of this at least at the time of the first disclosure, unless We have already provided You with such information previously. With Your consent, We may also provide personal data to others.

We may also provide Your data to protect Your vital interests (for example, if You suddenly feel unwell while on Our premises and We need to seek medical help).

We may use data processors who will process personal data in accordance with Our instructions and to the extent determined by Us, to the extent necessary to achieve the purposes of the processing. When We use data processors, We aim to ensure that the processors also have appropriate organisational and technical security measures in place and maintain the confidentiality of personal data.

Transfer of personal data outside the EU/EEA

Your data may be transferred outside the European Union, if agreements with data processors that comply with European Union law are signed.

Data may be transferred outside the European Union where the transfer is necessary for the conclusion and performance of contracts and the proper provision of services to the Company's customers. In such a case, the Company shall take steps to ensure that any transfer of personal data outside the EU/EEA is properly executed and that the privacy rights of data subjects are protected to the maximum extent possible. The Company's transfer of personal data outside the EU/EEA shall be guided by: the European Commission's decision on the adequacy of the foreign country; the certification mechanism approved in the foreign country; the European Commission's decision on the standard contractual clauses.

The third country outside the EU/EEA in which the recipient of the personal data is located is required by a decision of the European Commission to ensure an adequate level of protection of personal data.

Rights of the data subject

We would like to inform You about Your rights under the General Data Protection Regulation:

- **Right of access**. You have the right to request confirmation of whether data relating to You are being processed and to request information about such data pursuant to the provisions of Article 15 of the Regulation;
- **Right to rectification of personal data**. In accordance with the provisions of Article 16 of the Regulation, You have the right to have inaccurate data relating to You completed or rectified;
- **Right to erasure**. In accordance with the provisions of Article 17 of the Regulation, You have the right to request the erasure of specific data in the circumstances set out in the Article concerned;
- **Right to restrict processing**. In accordance with the provisions of Article 18 of the Regulation, You may request the restriction of processing under the circumstances set out in the Article concerned;
- **Right to data portability**. In accordance with the provisions of Article 20 of the Regulation, You have the right to request the receipt of the data You have provided to Us and, in addition, to request its transfer to other processors;
- **Right to object**. In accordance with the provisions of Article 21 of the Regulation, You may object to future data processing at any time;
- **Right to withdraw consent**. In accordance with Article 7(3) of the Regulation, You have the right to withdraw Your consent at any time;
- **Right to lodge a complaint with a supervisory authority**. Under Article 77 of the GDPR, You have the right to lodge a complaint with the competent supervisory authority, i.e., the State Data Protection Inspectorate;
- **The right to compensation** for damages suffered as a result of a breach of the data subject's rights. Under Article 82 of the Regulation, You have the right to compensation from the data controller for the damage suffered.

You may contact Us orally or in writing to exercise the data subject's rights by submitting Your request in person, by post or by electronic means to the contacts specified in this Privacy Policy.

You must authenticate Your identity by providing proof of identity. Failure to do so will prevent Us from accepting Your requests and will result in the data subject's rights not being exercised.

Final provisions

The websites may contain links to third-party websites, legislation, as well as links to social networks (the ability to share the website content on Facebook and Instagram). It should be noted that the third-party websites the links to which are provided in Our website are subject to the privacy policies of those websites and the Company does not accept any responsibility for the content of the information provided by those websites, the operation of those websites and the provisions of their privacy policies.

You can contact Us in the following ways for all data processing issues:

- By email: dpo.lt@tamro.com
- Call +370 37 225 522
- Mailing address: Gamybos g. 4, Ramučių k., Kauno r., Lithuania.

The Company has a Data Protection Officer, who can be contacted in the following ways:

- E-mail: rusne@duomenuapsauga.eu
- Call +37069834316.

Policy review

We may review and change this Privacy Policy at any time. Changes are effective from the date of their posting on the websites.

We recommend that You always consult the latest version of the Privacy Policy.

Last updated on 14-01-2025.