

## Privacy policy

The respect of privacy is a serious concern to which we pay special attention when processing and using personal data. We therefore attribute great importance to the protection of your personal data. Insofar as personal data is collected (e.g. your name, address or other contact details), it is processed and used exclusively in accordance with applicable data protection regulations.

In the following, we would like to inform you about the processing of your personal data. Personal data are all data that identify you, e.g. name, address, e-mail addresses, user behavior.

### 1. Controller & Data Protection Officer

In the context of the EU's General Data Protection Regulation (GDPR), data controllers responsible for collection, processing and use of personal data as specified below, may include UAB TAMRO, legal entity code 111448632, address 9-ojo Forto g. 70 ir BENU Vaistinė Lietuva, UAB legal entity code 135874035 address 9-ojo Forto g. 70.

You can reach our data protection officer at [dpo.lt@tamro.com](mailto:dpo.lt@tamro.com) or our postal address with the addition "the data protection officer".

### 2. The processing of personal data of candidates taking part in the selection and the administration of the candidate database:

(1) If you have sent your CV (cover letter), motivation letter, letters of references and/or other documents or data on the basis of the information published on our website or in dedicated website intended for the selection of employees and jobseekers or a job ad posted elsewhere, your voluntarily submitted later and other personal data below will be processed for the purpose of staff selection.

(2) We will process your personal data until the end of the selection process, i.e. until we select a candidate for recruitment, the end of his/her probation period or until we decide to complete the selection without recruiting any candidate. Your personal data will be destroyed after expiration of 6 months period from the announcement of the selection to the particular position, unless there is a different basis for handling it.

(3) We will process your personal data and the basis of your consent to participate in the selection, also on the basis of the statutory obligations and rights.

(4) If you submit your data to us without organizing a selection for a particular job, we will process your data for the purpose of administering the database of candidates and, when we experience a need for employees, we will contact you. We will process your data for 6 months from the receiving of the data.

(5) Please be advised that exercising the right granted to us by the personal data protection legislation we can contact your former employers, asking for reference about your qualifications, professional abilities and professional characteristics. However, we will not contact your current employer without your explicit prior consent.

(6) The company, to which you apply in respect to the particular employment, will be considered as a controller of your personal data. However, if you send your application to BENU Vaistinė Lietuva, UAB, another company – UAB „TAMRO“ will be the data controller as well. If you provide your personal data on your own decision (but not to the particular recruitment process), the data controllers will be both companies - UAB „Tamro“ and BENU Vaistinė Lietuva, UAB.

### 3. Data Collection during the visit of the website [www.benu.lt](http://www.benu.lt) (hereinafter – the Website)

(1) When using the website for information purposes only, i.e. if you do not register or otherwise provide us with information, we only collect the personal data that your browser transmits to our server. If you wish to view our website, we collect the following data, which is technically necessary for us to display our website to you and to ensure its stability

- IP address
- date and time of the request

- Time zone difference to Greenwich Mean Time (GMT)
- Content of the request (specific page)
- Access status/HTTP status code
- amount of transferred data
- Referrer URL
- Browser Type
- Operating system and its interface
- Language and version of the browser software

(2) In addition to the aforementioned data, cookies are stored on your computer when you use our website. Cookies are small text files that are stored on your hard disk in the browser you use and through which certain information flows to the institution that sets the cookie. Cookies cannot run programs or transmit viruses to your computer. They serve to make the Internet offer more user-friendly and effective overall.

(3) Use of cookies:

a) This website uses the following types of cookies, the scope and functioning of which are explained below:

- Transient cookies (see b)
- Persistent cookies (see c).

b) Transient cookies are automatically deleted when you close your browser. This includes in particular the session cookies. These store a so-called session ID, with which different requests of your browser can be assigned to the common session. This will allow your computer to be recognized when you return to our website. Session cookies are deleted when you log out or close your browser.

c) Persistent cookies are automatically deleted after a specified period, which may vary depending on the cookie. You can delete cookies at any time in the security settings of your browser.

d) You can configure your browser settings according to your wishes and, for example, refuse the acceptance of third party cookies or all cookies. Please note that you may not be able to use all functions of this website.

e) We use cookies to identify you for follow-up visits if you have an account with us. Otherwise you would have to log in again for each visit.

f) The Flash cookies used are not collected by your browser, but by your Flash plug-in. We also use HTML5 storage objects that are stored on your mobile device. These objects store the required data independently of your browser and do not have an automatic expiry date. If you do not wish the Flash cookies to be processed, you must install an appropriate add-on, e.g. "Better Privacy" for Mozilla Firefox (<https://addons.mozilla.org/de/firefox/addon/betterprivacy/>) or the Adobe Flash killer cookie for Google Chrome. You can prevent the use of HTML5 storage objects by using private mode in your browser. We also recommend that you regularly delete your cookies and browser history manually.

(g) Of course, you can also view our website without cookies. Internet browsers are regularly set to accept cookies. In general, you can deactivate the use of cookies at any time via the settings of your browser. Please use the help functions of your Internet browser to find out how you can change these settings. Please note that some features of our website may not work properly or at all if you have disabled the use of cookies.

(4) We use cookies for the sake of ensuring the stability of operation of the website as well as for the purposes of statistics, marketing and for improvement of your browsing experience. The legal basis for the processing of cookies is your consent (paragraph 1(a) of Art 6 of the GDPR), except cookies that even without your consent due to performance of our services are necessary for the purpose of functioning of the website (paragraph 1(b) of Art 6 of the GDPR). Unless specifically stated, we only store cookies for 30 days from the day of their collection.

(5) If we make use of contracted service providers for individual functions of our offer or would like to use your data for advertising purposes, we will inform you in detail about the respective processes below.

(6) A company that has the status of data controller in relation to the selection of candidates is the company you are contacting when sending your data.

(7) If you want to make purchases on the [www.benu.lt](http://www.benu.lt) e – shop (hereinafter – E-shop), you will be requested to provide the data, which is necessary for implementation of your purchase order: name, surname, e-mail address, phone number, full address (including state, city, street, apartment number, post code). You can make a purchase without a registration, just by providing the above mentioned data, or you can register. If you decide to register to E-shop, your E-shop account will be created and automatically connected with BENU loyalty program. If you are not a BENU loyalty program client, the loyalty program account will be created automatically after your registration to E-shop. More information about purchases on E-shop may be found on the [www.benu.lt](http://www.benu.lt).

(8) You can amend or supplement the data on the E-shop as well as cancel your E-shop registration by a written request provided to the E-shop administrator.

(9) Your personal data on the E-shop will be stored for 2(two) years period from the last purchase, if you are the client of the loyalty program. The invoice data will be stored as long as requested by the law on accounting. If pharmaceutical consultation is provided to you by phone or live chat, as described in the E-shop rules, the record of such conversation will be stored for 1 (one) year period from the date of the pharmaceutical consultation.

#### 4. Administration of complaints, inquiries and feedback

(1) If you contact us (e.g., via contact form, in writing or by e-mail), we store your details for processing the complaint, inquiry or feedback (hereinafter - inquiry) and for any follow-up questions. We delete the data arising in this context after the storage is no longer necessary. Your inquiry and related data is being processed and stored for 1 (one) year from the day the reply to the inquiry was provided to you. If your inquiry relates to a potential dispute, your personal data will be stored for a period of 1 (one) year from the end of the prescribed by law limitation statute for the particular claim and (or) from the day of coming into force of the final court decision.

(2) The company that will have the status of data controller for your personal data processed for this purpose is the company to which you provide the contact details. If you submit your data to BENU Vaistinė Lietuva, UAB, UAB TAMRO will also be the data controller.

#### 5. E-mail communication

(1) Based on the GDPR Regulation, content of correspondence by e-mail is considered as personal data and this applies even for the correspondence of employees of legal entities. In this respect, we will apply the rules for the processing of personal data in accordance with the GDPR Regulation to the content of communication as well as to the email addresses.

(2) The basis for the processing of your personal data is the free will expression to engage communication by email and provision of certain details in it, i.e. the consent. Moreover, the processing of your data may also be based on the performance of a contract and statutory obligations.

(3) Your email address, correspondence content and related data will be processed in accordance with the principle of proportionality. This data will primarily be visible to the person whom you will be directly contacting by email. However, in certain cases, your correspondence may also be accessible to other employees, for example, in the course of internal administration, investigation of potential violations of legal acts or internal rules of procedure, replacement of the employee and related purposes, and in similar situations.

(4) The data controller responsible for the processing of personal data for this purpose is the company with whom you are communicating with your employee or other representative.

#### 6. Customer card account

(1) You can login the customer account on the [www.benu.lt](http://www.benu.lt) website. Data in this account is stored for no longer than the validity of the Customer card as defined in the terms of the Customer card program.

(2) The Data controller responsible for the processing of personal data for this purpose is UAB Tamro.

## 7. Video Surveillance

(1) Video surveillance is carried out for the purpose of ensuring the safety of persons. Video records are stored for a maximum of 30 days and are destroyed at the end of this term

(2) The data controller responsible for the processing of personal data for this purpose is the company in whose premises or territory the video surveillance is carried out.

## 8 Plugins

### Google Analytics

a) The website uses Google Analytics, a web analytics service provided by Google, LLC. ("Google"). Google Analytics also uses cookies, i.e. text files that are stored on your computer and allow an analysis of your use of the website. The information generated by the cookie about your use of this website is usually transferred to a Google server in the U.S.A. and stored there. Through the activation of IP anonymization on the website, however, your IP address will be truncated by Google within Member States of the European Union or other parties to the Agreement on the European Economic Area. Only in exceptional cases is the complete IP address transmitted to a Google server in the U.S.A. and truncated there.

b) On behalf of us Google will use this information for the purpose of analyzing your use of the website, compiling reports on website activity and providing us with other services relating to website activity and internet usage.

c) Google will not associate the IP address transmitted by your browser with any other data held by Google. Google may also transfer this information to third parties where required to do so by law, or where such third parties process this information on Google's behalf.

d) At any time you may delete cookies placed on your computer by calling up the relevant menu item in your internet browser or deleting the cookies on your hard drive. For details, see the Help menu of your internet browser.

e) You may refuse the use of cookies by selecting the appropriate settings on your browser; we advises, however, that if you do this you may not be able to use the full functionality of this website. You can also prevent the data generated by the cookie about your use of the website (incl. your IP address) being sent to Google as well as the processing of this data by Google by downloading and installing the browser plugin available at the following link: <http://tools.google.com/dlpage/gaoptout?hl=en>

f) Further information is available at <http://tools.google.com/dlpage/gaoptout?hl=en>. We want to point out that the code "`_anonymizeIp();`" has been added to Google Analytics on the website to guarantee the anonymous collection of IP addresses (so-called IP masking).

### Google Maps

This website uses Google Maps API to display geographical information visually. When using Google Maps, Google also collects, processes and uses data about the use of map functions by visitors. You can find more information about Google's data processing in the Google Privacy Policy. There you can also change your personal data protection settings in the Data Protection Center.

### Google Web Fonts

Google Fonts are used to improve the visual presentation of various information on this website. The web fonts are transferred to the cache of the browser when the page is called up so that they can be used for display. If your browser does not support Google Web Fonts or does not allow access, the text will be displayed in a default font.

Data submitted in connection with the page visit is sent to resource-specific domains such as fonts.googleapis.com or fonts.gstatic.com. They are not associated with data that may be collected or used in connection with the parallel use of authenticated Google services.

You can set your browser so that the fonts are not loaded from Google servers (e.g. by installing add-ons like NoScript or Ghostery for Firefox.) If your browser does not support Google Fonts or if you block access to the Google servers, the text will be displayed in the system's default font.

## Vimeo

This website uses plug-ins from the American company Vimeo, LLC, 555 West 18th Street, New York, New York 10011, USA. As a consequence, log information may be transmitted from our website to Vimeo. Vimeo's server in the United States thus automatically stores information ("log data"), such as the information that your browser sends to a website when you visit, or the information that your mobile app sends when you use it. This log data may contain your IP address, the address of the website you visited that uses Vimeo features, the browser type and settings, the date and time of your request, information about your use of Vimeo, and cookies.

You can find out more information about data collection, how your data is evaluated and processed by Vimeo, and your rights relating to this in Vimeo's Privacy Policy: <http://vimeo.com/privacy>.

## Social Plugins

On our website social plugins ("plugins") are used by social networks.

In order to increase the protection of your data when visiting our website, the plugins are not unrestricted, but only integrated into the page using an HTML link (so-called "Shariff solution" from c't). This integration ensures that no connection is established with the servers of the provider of the respective social network when a page of our website containing such plug-ins is called up. Click on one of the buttons, a new window of your browser opens and calls up the page of the respective service provider, on which you can (if necessary after entering your login data) e.g. press the Share button.

The purpose and scope of data collection and the further processing and use of the data by the providers on their pages as well as your relevant rights and setting options for the protection of your privacy can be found in the data protection information of the following providers:

XING AG (Dammtorstr. 30 - 20354 Hamburg - Germany)

LinkedIn Corporation (2029 Stierlin Court - Mountain View - CA 94043 - USA)

facebook Inc. (1601 p. California Ave, Palo Alto, CA 94304, USA)

Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043 USA)

Twitter Inc. (795 Folsom St., Suite 600, San Francisco, CA 94107, USA)

## 9. Data transmission to recipients

(1) In some cases, we will use external IT, server, mail, archiving, bookkeeping, auditing, or other suppliers or contractors to process your data. We carefully select such contractors or service providers, request them to comply with our instructions, and regularly inspect them.

(2) If necessary, we may transfer your personal data to companies belonging to the same group; notaries, bailiffs, lawyers, consultants, auditors; law enforcement and supervisory authorities, courts and other dispute settlement bodies; potential or existing successors of our business or part thereof, or their authorized consultants or individuals.

(3) If our service providers or partners are located outside of the European Economic Area, we will inform you of the consequences of such circumstances in the description of the offer.

## 10. Your Data Subject Rights

We gladly want to you inform you regarding your rights according to the General Data Protection Regulation:

#### Right of Access

You have the right to request confirmation whether data concerning you are being processed and to request information regarding these data according to Art. 15 GDPR

#### Right to rectification

In accordance with Article 16 of the GDPR, you have the right to request the completion or correction of inaccurate data concerning you.

#### Right to erasure

In accordance with Art. 17 GDPR, under the presence of other circumstances provided for in this article, you have the right to demand that relevant data may be deleted in case there are no legal obligations preventing the deletion.

#### Right to restriction of processing

You may demand a restriction of the processing in accordance with Art. 18

#### Right of data portability

You have the right to request to receive the data provided to us in accordance with Art. 20 GDPR and additionally to request its transmission to other processors

#### Right to object

You may object to the future processing according to Art. 21 GDPR at any time.

#### Right to revocation

You have the right to revoke consent anytime according to Art. 7 Par. 3 GDPR valid for the future.

#### Right to submit a claim to the supervisory authority

In accordance with Art. 77 GDPR you have the right to file a complaint with the competent supervisory authority – the State Data Protection Inspectorate.

### 11. Reporting System

The PHOENIX group, i.e. the PHOENIX Pharmahandel GmbH & Co KG as well as its affiliated companies, including UAB "Tamro" and BENU Vaistinė Lietuva, UAB, according to § 15ff AktG, has established a web based reporting system which is designed to enable employees, business partners, customers and third parties an easy system by which to report data incidents or concerns. These reports are taken seriously and are reviewed and actioned regularly and are used to improve the protection of personal data.

You can access this reporting tool at any time via:

<https://phoenixgroup-databreach.integrityplatform.org/>

In order to explain the background to the reporting system in more detail, we have also answered a number of frequently asked questions below:

#### *When should I report an incident?*

PHOENIX group has an obligation to notify the supervisory authority within 72 hours of becoming aware of an incident, due to this, all incidents must be reported without delay via the online reporting tool.

#### *What data incidents should be reported and how?*

All personal data incidents are to be reported to the Data Protection team via the online reporting tool.

#### *What is a data protection incident?*

Data Protection incidents are any event which has, or could have, resulted in the accidental or

deliberate loss of personal data (electronic or paper) or destruction of data, or unauthorised access to data (e.g. loss or theft of laptop, smartphone, paper record, prescriptions).

*What happens after I submit a report?*

The Data Protection team will review the incident report and will contact you for further information or, where necessary, will assist you with the post incident actions.

## 12. General Comments

We retain the right to change our data privacy statement. This may be necessary as a result of technical developments. We therefore ask you to consult the data privacy statement from time to time and to apply the current version. If you have do have any further questions or concerns regarding you personal data, please contact the designated data protection officer.

Date of last review and update: March 2020