

Privacy Policy

Privacy policy of **BIOTRON FOUNDATION**, občianske združenie, a civil association founded under Slovak laws with registered seat at Staré Grunty 18, 841 04 Bratislava – m. č. Karlova Ves, Slovak Republic, ID No. (IČO): 51 191 857, registered with the Register of Civil Associations of the Ministry of Interior of the Slovak Republic (“**Biotron Foundation**”) and other companies belonging to “Biotron family” such as **Biotron Labs s.r.o.** with registered seat at Albina Brunovského 6, 841 05 Bratislava, Slovak Republic, ID No. (IČO): 52 010 988 (“**Biotron Labs**”) (Biotron Foundation and Biotron Labs hereinafter jointly referred to as “**Biotron**“, “**we**“ or “**us**“).

Biotron Foundation is a non-profit organization that exists to support and collectively lead the Foundation's vision - to make data available in a transparent and privacy-compliant way. Its goal is to provide companies with technical and legal framework that will help them stick to these principles, while having access to high-quality datasets at the same time. On the other hand, users providing data will be rewarded for sharing them.

Biotron Labs is a for-profit company that utilizes Biotron Foundation's frameworks and validate them in business. It is a taxable subsidiary that servers the non-profit, public benefit goals of its parent, the Biotron Foundation, and that will be responsible for product development, marketing and distribution of Biotron products. It also handles relationships with businesses, many of which generate income. Unlike the Biotron Foundation, the Biotron Labs is a tax-paying entity, which gives it much greater freedom in the revenue and business activities it can pursue. The subsidiary is 100% owned by Biotron Foundation. Biotron Foundation is funded by donations and license fees.

If you have any questions concerning how we process your personal data, you can contact our data protection officer either by email at: privacy@biotron.io or by post using the registered seat of Biotron Foundation mentioned above. We must comply with the EU general data protection regulation (the “**GDPR**“) and applicable sections of Slovak Act No. 18/2018 Coll., on protection of personal data as well as other Slovak and EU legislation. This privacy policy is primarily designed to ensure compliance with informational obligations pursuant to Articles 13 and 14 GDPR of Biotron and our business customers towards data subjects about whom we process personal data mainly when providing Biotron services defined in our terms of use as the “**Services**“. Our terms of use are available at https://docs.biotron.io/Biotron_Terms_of_Use.pdf (the “**Terms of Use**“). Typical data subjects about whom we process personal data are users of our mobile application “Biotron Data - share data & get rewards” (the “**App**“), our business customers or suppliers and their employees or our own employees.

We have tried to answer the required and most frequent privacy-related questions below:

Is there a “dummy” version of this policy so I don’t have to read everything?

Yes 😊 To put it very simply; if you use the App and its functionalities, we will provide your data to 3rd parties. These 3rd parties will pay us for such data. We will make a gift to you in a form of BTRN tokens when you participate in this scheme, as this is the non-profit goal of the Biotron Foundation. You will have basic control about what data and to whom can be provided.

What is our position when processing personal data?

Generally, we act as a **data controller** when processing your personal data for the below purposes. We have internally concluded a joint controllership agreement pursuant to the Article 26 of the GDPR between Biotron Foundation and Biotron Labs regarding the purposes related to the App as well as some other purposes mentioned below. The main parts of this Agreement provide, that:

- We have a single contact point for data subject being our “group” data protection officer mentioned above regardless of which entity processes your personal data in question;
- Biotron Foundation is non-profit organization that owns the vision and creates technical and legal frameworks;
- Biotron Foundation is the owner of the App and data engine that provides users with the Services;
- Biotron Foundation communicates, informs and deals with data subject request and the supervisory authorities on behalf of both joint controllers;
- Biotron Labs is a for-profit company that concludes business agreements with our business customers or suppliers and provides the Services in case such Services create profit (e.g. selling dataset or Labs report to our business customers).

We might also act as a **data processor** in certain scenarios. For example, when our partner provides us with its own data to conduct analysis of such data on its behalf or generally when we are contracted to process personal data on behalf of someone else, we act as a data processor of such partner or someone else that by virtue of determining the purpose and means of processing of personal data is regarded a data controller. In such a scenario, we suggest concluding a separate agreement pursuant to the Article 28 of the GDPR setting out in more detail our rights and obligations in relation to personal data processing. This agreement is not part of this privacy policy nor Terms of Use but is concluded separately, if required.

For what purposes are your personal data processed?

If you use the App, the following are the typical purposes for which we are processing your personal data as a data controller:

Purpose	Legal basis	Description
1. Provision of Services	Performance of contract pursuant to the Article 6(1)(b) of the GDPR	This purpose involves all processing that is necessary to provide you with Services based on the Terms of Use. This includes processing necessary for administration and maintenance of your account, login to the App, related customer service as well as the core processing operations aimed at rewarding you with BTRNs for allowing us to leverage your personal data with our business customers.
	Consent pursuant to the Article 6(1)(a) of the GDPR	We specifically ask for your consent in order to access your location data within provision of the Services.
2. Development, improvement, testing	Legitimate interest of Biotron pursuant to the Article 6(1)(g) of the GDPR	As a software developer it is our aim and obligation to provide the best software solution possible. For that purpose, we continuously develop

and improve our software and conduct regular testing of its functionalities e.g. via analysis of application, removal of bugs, issuing new application versions and updates including security updates via performance and audience analysis or implementation of feedbacks of users. We consider aforementioned activities our legitimate interest.

3. Security	Compliance with legal obligation pursuant to the Article 6(1)(c) of the GDPR	Security is one of the cornerstones of our vision. We consider our obligation pursuant to the Article 32 GDPR to protect our assets including processed data (including personal data) against any potentially harmful conduct. This might include monitoring of user behavior within the App or our website to detect fraudulent, suspicious or otherwise harmful conduct of users, conduct of users that is in breach of Terms of Use or scanning of our systems against unauthorized bots.
4. Direct marketing (e.g. targeted advertising or newsletter)	<p>Consent pursuant to the Article 6(1) of the GDPR</p> <hr/> <p>Legitimate interest pursuant to the Article 6(1)(g) of the GDPR</p>	<p>If you subscribe to our newsletter, we rely on a legal ground of consent to send you any direct marketing communication or targeted advertisement.</p> <hr/> <p>If we focus our marketing newsletter on our existing clients whose e-mail addresses we obtained in connection with provision of similar services or products we rely on statutory consent exemption provisioned in Section 62 (3) of the Electronic Communications Act and we consider processing of personal data for such purpose our legitimate interest (direct marketing). We also process your personal data for other targeted advertising campaign purposes. In any case you have right to opt-out from any processing of your persona data for direct marketing purposes.</p>
5. Statistical purposes	Any other legal basis pursuant to the Article 89 GDPR, as explained in recital 50 GDPR (compatible purposes)	We generate anonymous aggregated statistics on the basis of personal data that we process for other purposes so that the resulting statistic are no longer personal data (e.g. number of users).
6. Scientific research purposes	Any other legal basis pursuant to the Article 89 GDPR, as explained in recital 50 GDPR (compatible purposes)	From time to time, we might process existing personal data for the scientific research purposes in the following areas: urban planning, transportation, health research & clinical trials.

Depending on our relationship, we as a data controller might also process your personal data for the following purposes:

Purpose	Legal basis	Description
7. Membership in the civil association	Compliance with legal obligation pursuant to the Article 6(1)(c) of the GDPR	We are obliged to process personal data about the members of our civil association (e.g. list of members, membership fees, elections, general meetings, etc.). This purpose is limited only to Biotron Foundation.
8. Accounting & Tax purposes	Compliance with legal obligation pursuant to the Article 6(1)(c) of the GDPR	To comply with Slovak accounting and tax legislation we must process the personal data included in the invoices and related documents and communication for statutory period of time. Both Biotron Foundation and Biotron Labs process personal data for this purpose individually.
9. Performance of contracts	Performance of contract pursuant to the Article 6(1)(b) of the GDPR if the party is an individual and legitimate interest pursuant the Article 6(1)(g) of the GDPR if the party is a legal person	In order to perform various different contract with our suppliers or customers we must process the personal data necessary to fulfil our obligations under such contracts. Both Biotron Foundation and Biotron Labs process personal data for this purpose individually.
10. Payroll & personnel purposes	Compliance with legal obligation pursuant to the Article 6(1)(c) of the GDPR	We are in an employment relationship with your or we discuss employment opportunities with potential candidates, we must process personal data in order to comply with employment, payroll, social contribution or similar legislation. We act as joint controllers.
12. Publication of photos of employees, team and supervisory board members	Consent pursuant to the Article 6(1)(a) of the GDPR	When we publish photographs of our employees, team members or supervisory board members on our website, we request your consent.
13. Increasing online awareness about Biotron (e.g. via social media)	Legitimate interest pursuant to the Article 6(1)(g) of the GDPR	If we maintain our business profiles on social networks (Facebook, Twitter, LinkedIn, Telegram, Medium), it is our legitimate interest to increase association / brand awareness in the online environment. We act as joint controllers.
14. Establishment, exercise or defense of legal claims	Legitimate interest pursuant to the Article 6(1)(g) of the GDPR	From time to time, we might need to pursue a legal claim, ask for compensation or off-court settlement or report certain facts to public authorities and aforementioned processing operations shall be considered as our legitimate interest. Both Biotron Foundation and

			Biotron Labs process personal data for this purpose individual unless individually agreed otherwise.
15.	Compliance with other legal obligations	Compliance with legal obligation pursuant to the Article 6(1)(c) of the GDPR	When we need to comply with legal obligation that requires us to process your personal data, we do so without your consent on the basis of complying with legal obligation. Both Biotron Foundation and Biotron Labs process personal data for this purpose individually.
16.	Archiving purposes	Any other legal basis pursuant to the Article 89 GDPR, as explained in recital 50 GDPR (compatible purposes) and in compliance with the Slovak Act on Archives and Registries	We are obliged to comply with mandatory obligations stemming from the Slovak Act on Archives and Registries. These obligations correspond with the archiving purposes (i.e. storing of selected documents for specified periods before their deletion or state archiving). We act as joint controllers.

Do we sell your personal data?

We do not sell your personal data in raw form. However, the core part of the Services is to reward users for allowing us to leverage their personal data by us or by our business customers. **Raw data is always analyzed and only aggregated anonymous or pseudonymous results or final analysis are sold to our business customers.** Whenever revenue is generated through the sales of Labs, insights, and processed datasets, it will be split between Biotron and those users that contributed their data to the respective deal.

You might ask: *“If we can link the aggregated anonymous report with specific users to reward them in BTRN tokens then the report is no longer anonymous, i.e. we sell personal data?”* The correct answer is no. We cannot establish such link because in order to allocate BTRN tokens we are using identifiers which are not provided to our clients. If, however any regulator or court comes to a different conclusion (e.g. that the above is only pseudonymized personal data), then we must regard it as necessary to fulfill our obligation to provide Services you requested under the Terms of Use. In general, you should read the notion of “Services” as an information society service provided by us encompassing processing your personal data for any purposes related to the App mentioned above also by our business customers including provision of your personal data to them by us.

What personal data we collect?

We process the following personal data about our users:

- E-mail address – Within the website registration process we collect e-mail address of Data Subjects in order to be able to communicate with registered users about products, services, offers, promotions, and events, and provide other news and information we think will be of interest to users.

- Information necessary in order to provide our Services - this includes e-mail address, Ethereum address, other Blockchain address where applicable and other information provided by you through email (such as your first name and surname might be disclosed, even though not directly requested by us).
- Other Information – you may choose to provide other information directly to us, e.g. with respect to the promotions and related services, your requests and notifications, customer support or other communication with us, such as:
 - Device and application information, such as the device name, device identification code (IMEI, ESN, MEID, and SN), device activation time, hardware model, OS version, application version, software identification code, and device and application settings (such as region, language, time zone, and font size).
 - Mobile network information, such as the public land mobile network (PLMN) provider ID and Internet Protocol (IP) address.
 - Log information. When you use Services, we will automatically collect and log some information, such as the time of access, access count, IP address, and information about incidents (such as errors, crashes, restarts, and upgrades).
 - Location information. We will collect, use, and process the approximate or precise location of your device. Location information can be obtained based on the GPS, WLAN, and service provider network ID. You are free to choose if you want to enable gathering of Location information. Please note that simply by installation of the applications on your devices, Location information is not gathered from you. Location information are gathered solely on your decision to enable collection of Location information in the settings menu of the installed application, what is rewarded by remuneration. In the same settings menu of the installed application, you can disable the location permissions to reject sharing your location information.

We do not intend to process special categories of data, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or a natural person's sex life or sexual orientation, unless the individual has given explicit consent to the processing of such data or other conditions under Article 9(2) of the GDPR are met.

How we collect your personal data?

Generally, **we collect your personal data directly from you**. Your provision of personal data to us is voluntary. You can provide your personal data to us by number of means such as by using the App; by visiting, registering or using Biotron website; in the process of concluding or negotiating the contract with us; by communicating with us; by subscribing to our newsletter; by activity on our profiles on social media.

However, we may also obtain your personal information from your employer or from the company in relation to which we process your personal data. This is typically the case when we conclude or negotiate a contractual relationship with the company where you work at. If the collection of personal data relates to a contractual relationship it is often a contractual requirement or a requirement that is required for the conclusion of a contract. Failure to provide personal data (whether yours or your colleagues) may have negative consequences for the company you represent, as this may result in failure to conclude or

performance of a contractual relationship. If you are a member of a statutory body of a legal person that is a contracting party to us or with whom we are negotiating a contractual relationship, we may obtain your personal data from publicly available sources and registers.

In some cases, **we collect data (including personal data) from other third-party data vendors** acting as separate controllers who are responsible for ensuring that collection and provision of your personal data to us is done in compliance with the GDPR. We actively cooperate with our data vendors to ensure such provision of data to us is as transparent, fair and legal as possible.

We also **collect your personal data via our data collection SDK / script when placed in a third-party mobile or web application**. Similarly, as with the data vendors, we actively cooperate with third-party applications' owners to ensure such provision of data to us is as transparent, fair and legal as possible.

How we share your data?

We take the confidentiality of your personal data very seriously and have policies in place to ensure that your data is only shared with authorized personnel at Biotron or a verified third-party services provider. Our staff might have access to your personal data on a strictly need-to-know basis typically governed and limited by function, role and department of the particular employee. Personal data of our employees, business customers or other natural persons are provided to the extent necessary to following categories of recipients:

- to our business customers that in line with this privacy policy and/or Terms of Use get access to your personal data;
- payroll, accounting professionals or our professional advisors (e.g. accountants, attorneys or auditors);
- providers of standard software and cloud services (e.g. Microsoft One Drive or Amazon Web Services);
- hosting providers (Amazon, EU);
- providers of technical (IT) support;
- social insurance company, pension insurance management company, supplementary pension insurance company, health insurance company, office of social affairs and family;
- postal couriers and courier services;
- employees of the above recipients.

We also use sub-contractors to support us in providing services who might process personal data for us. We ensure that selection of our sub-contractors and any processing of personal data by them is compliant with the GDPR in terms of technical and organizational security of processing operations. If we use our own recipients to process personal data (Biotron's internal staff), your personal data are always processed on the basis of authorizations and instructions that inform our recipients about not only our internal privacy policies but also about their legal responsibility for their violations. If we are requested by the public authorities to provide your personal data we examine the conditions laid down in the legislation to accept the request and to ensure that if conditions are not met, we do not adhere to the request. In case that you have a question about our current processors, do not hesitate to contact us for further information.

What countries do we transfer your personal data to?

By default, we seek not to transfer your personal data outside the EU and/or European Economic Area where not necessary, as our servers are located in Germany (EU). However, some of our business customers, sub-contractors or the above-mentioned recipients of personal data might be based or their servers might be located in the United States of America (U.S.) or elsewhere outside the EU/EEA (e.g. Canada). As such, US is regarded a third party not ensuring adequate level of protection. However, companies certified under the EU-US Privacy Shield mechanism according to the Commission (EU) are regarded as ensuring adequate level of protection. Any transfer of personal data outside the European Economic Area is done by us only under strict compliance with the GDPR. We ensure the third-party recipients are either certified under the EU-US Privacy Shield, concluded EU model clauses with us or follow equivalent safeguards in place. Please note that even when such safeguards are not in place, pursuant to Article 49(1)(b) of the GDPR we are entitled to transfer your personal data if it necessary for performance of contract with the data subject. This may encompass transfer that is necessary to provide you with the Services pursuant to the Terms of Use. Regardless of where your personal data is physically processed, we apply the same protections as described in this privacy policy.

How long do we store your personal data?

We must not and we do not want to store your personal data for longer than necessary for the given purpose of processing. Due to this legal requirement but also due to technical and financial aspects of data storage we actively delete data where no longer necessary. Retention periods are either provisioned in respective laws or are set out by us in our internal policies or procedures. When processing of your personal data is based on a consent and you decide to withdraw your consent, we do not further process your personal data for the specific purpose. However, it does not exclude the possibility that we process your personal data on different legal basis especially due to our legal obligations. General retention periods for our purposes are as follows:

Purpose	General retention period
Provision Services	Duration of the contract (Terms of Use), i.e. until you use the Services
Development, improvement, testing	Duration of the contract (Terms of Use), i.e. until you use the Services
Security purposes	Duration of the contract (Terms of Use), i.e. until you use the Services
Direct marketing purposes (e.g. targeted advertising or newsletter)	Until the acceptance of the objection against processing or sign-out from the newsletter performed by data subject
Statistical purposes	Duration of any other purposes
Scientific research purposes	Duration of any other purposes
Membership in the civil association	Duration of the membership in the civil association
Accounting & Tax purposes	10 years
Performance of contracts	Duration of the contract plus 3 years

Payroll & personnel purposes	Duration of the employment contract, unless longer period is required by law for employee file or records (e.g. 70 years of employee's age)
Employment monitoring mechanisms	Duration of the monitoring mechanism
Publication of photos of employees, team and supervisory board members	Duration of the relationship with the employee, team or supervisory board member until the consent is revoked prior to that
Increasing online awareness about Biotron (e.g. via social media)	Generally during the term we use social network or media.
Establishment, exercise or defense of legal claims	Duration of the court or off-court processing or settlement until the legal claim is settled or ceases to exist
Compliance with other legal obligations	As required to comply with various legal obligations (in Slovakia typically 2-10 years)
Archiving purposes	Duration of any other purposes or longer period if required by the Slovak act on archives or registries

The above retention periods only specify the general periods during which personal data are processed for the specific purposes. However, we proceed to erasure or anonymization of personal data before the expiry of these general periods if we consider the personal data to be unnecessary in view of the above-mentioned purposes. Conversely, in some specific situations, we may keep your personal data longer than stated above if it is required by law or our legitimate interest.

What rights do you have?

„You have the right to withdraw your consent at any time. You also have a right to object to any direct marketing processing of your personal data including profiling. You have right to object to any processing that is based on legitimate interest we rely on as described above. The same right is applicable on processing on legal ground of public interest that we do not currently rely on.“

In case of exercising the right, we will gladly demonstrate to you how we have evaluated these legitimate interests (including on behalf of our business customers) as compelling over the rights and freedoms of data subjects. The GDPR lays down general conditions for the exercise of your individual rights. However, their existence does not automatically mean that they will be accepted by us because in a particular case exception may apply. Some rights are linked to specific conditions that do not have to be met in every case. Your request for an enforcing specific right will always be dealt with and examined in terms of legal regulations and applicable exemptions.

Among others, you have:

- Right to request access to your personal data according to Article 15 of the GDPR. This right includes the right to confirm whether we process personal data about you, the right to access to personal data and the right to obtain a copy of the personal data we process about you if it is technically feasible.

- Right to rectification according to Article 16 of the GDPR, if we process incomplete or inaccurate personal data about you.
- Right to erasure of personal data according to the Article 17 GDPR;
- Right to restriction of processing according to the Article 18 GDPR;
- Right to data portability according to the Article 20 GDPR;
- Right to object according to the Article 21 GDPR;
- Right not to be subject to the automated individual decision making according to the Article 22 GDPR.

If you feel that we are processing incorrect personal data about you given the purpose and circumstances, you can request rectification of incorrect or incomplete personal data using our general contact details mentioned above.

You have a right to lodge a complaint related to personal data to the relevant data protection supervisory authority or apply for judicial remedy. Please note that our competent data protection authority is **the Office for Protection of Personal Data of the Slovak Republic** (<https://dataprotection.gov.sk/uouu/>).

Do we process your personal data via automated means which produces legal effects concerning you?

No. We do not currently conduct processing operations that would lead to the decision which produces legal effects or similarly significantly affects concerning you based solely on automated processing of your personal data in light of Article 22 GDPR. However, we cannot rule out that such decisions are made by our business customers which remain responsible complying with Article 22 of the GDPR as a separate data controllers from us.

How we protect your personal data?

It is our obligation to protect your personal data in an appropriate manner and for this reason we focus on the questions related to protection of personal data. Biotron has implemented generally accepted technical and organizational standards to preserve the security of the processed personal data, especially taking into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. Where appropriate, we use encryption.

Social networks

Please read relevant privacy policies to better understand processing of your personal data by providers of social media platforms. We only have a typical admin control over the personal data processed by us via our own Biotron profile. We assume that by using these social media platforms, you understand that your personal data might be processed for other purposes and that your personal data might be transferred to other third countries and third parties by

providers of social media platforms. We are not responsible for conduct of social networks providers but we do acknowledge our responsibility for protection of personal data when managing our accounts.

Minimum age

It does not fit into our goals and vision to provide our Services to children and users younger than 16 years of age. In order to use our Services you must be at least 21 years of age. From this reason, we do not give an option for younger users to provide us with their parent emails for verification.

Cookies Policy

What are cookies?

Cookies are small pieces of text sent by your web browser by a website you visit. A cookie file is stored in your web browser and allows the Service or a third-party to recognize you and make your next visit easier and the Service more useful to you. Cookies can be "persistent" or "session" cookies.

How we use cookies?

We use cookies and similar technologies on our website, within the App or generally when providing the Services for the following purposes:

- to enable certain functions of the Service including storing your preferences;
- to provide analytics;
- to enable advertisements delivery, including behavioral advertising.

We use both session and persistent cookies on the Service and we use different types of cookies to run the Service: Essential cookies. We may use essential cookies to authenticate users and prevent fraudulent use of user accounts. We will ask you to consent to our use of cookies in accordance with the terms of this policy where such consent is required.

When the “cookies” consent is not required?

We think it is useful to clarify the legal regime applicable to cookies under e-Privacy Directive, as amended in 2009, to those who are interested. Article 5(3) of the e-Privacy Directive states: *“Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the*

terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.”

The fact, that “cookies consent” is generally required is often overlooked by two very important exceptions from this rule. Your consent is not required for: (a) technical storage or access (i.e. session cookies) and most importantly for; (b) provision of information society services. In our case, the Services we provide to you fall within the second category (b) and thus not requiring your consent. When the Services encompass provision and use of your data by our business customers, these business customers are entitled to rely on this exemption and (for example) display you a targeted advertising on their websites without additional consent because it is *strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*. Please note, that such conduct is necessary for mutual performance of Services as requested by you and you can always opt-out from direct marketing processing on the basis of your right to object pursuant to the Article 21 of the GDPR. If you object to us, we ensure our business customer are notified about this and on the basis of the Terms of Use, they are obliged to stop such processing immediately.

Third-party cookies

In addition to our own cookies, we may also use various third-parties cookies to report usage statistics of the Service, deliver advertisements on and through the Service, and so on. The third parties cookies, which we may use, are namely Google Analytics, Sendinblue, MailGun, MailChimp. Details of the third party cookies used by us may be found on the webpages of the respective third parties.

What are your choices regarding cookies

If you'd like to delete cookies or instruct your web browser to delete or refuse cookies, please visit the help pages of your web browser. Please note, however, that if you delete cookies or refuse to accept them, you might not be able to use all of the features we offer, you may not be able to store your preferences, and some of our pages might not display properly. We will use cookies only for a time of the validity of your consent to our use of cookies.

Changes to this privacy (and cookies) policy

Privacy is not a one-time issue for us. The information we give you with regard processing of personal data may change or cease to be up to date. From these reasons we may change this privacy policy from time to time by posting the most current privacy policy and its effective date on our website. In case we

change this privacy policy substantially, we may bring such changes to your attention by explicit notice, on our websites or by email. We encourage you to review the privacy policy whenever you access or use the Services or otherwise interact with us to help protect your privacy.

Biotron, Bratislava

Last Updated: November 2018