Torrum privacy policy (eSIM service)

Last updated: March 1, 2026

Version 1.0

At JSC "Telekom Baltija" ("we/us/our"), we take the security of personal information and privacy of our users very seriously. Please take a moment to read this Privacy Policy ("Policy") set forth how we collect, process and protect the information in connection with our website located at www.torrum.io and our services ("Services") available through our website.

This page informs you of our processing of your personal data when you:

1. visit our website,
2. subscribe to our marketing material (newsletters and special offers),
3. use our Services,
4. contact with us about our Service and partnership,

and the choices you have associated with that data.

Some terms that can be seen in this document:

Account is a personal page on the website accessible only to a registered user. In the Account, the user may perform various actions, such as managing their profile, obtaining a QR code, monitoring their balance, and other activities.
Automated decision-making is a decision that our system makes automatically due to its specific algorithm and without human participation.
Personal data means any information that is linked or reasonably linkable to an identified or identifiable individual, and does not include de-identified data or publicly available information.
Profiling means any form of automated processing performed on Personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, demographic characteristics, personal preferences, interests, reliability, behavior, location, or movements.
Services means E-SIM service provision.

ABOUT US

JSC Telekom Baltija acts as a controller of your Personal data and responsible for processing it.

Unified registration no. 40003454545
Postal address: K.Barona Street 32-14, Riga, LV-1011, phone: 67870123
Phone: 67870123

If you have any questions about the information detailed in this Policy or would like to exercise your data protection rights, please contact our data protection specialist at privacy@torrum.io. We will respond to your requests via the email address provided or in any other form of your choosing.

SOURCES OF YOUR PERSONAL DATA

We may receive your personal data:

- Directly from you (e.g., when you create an account or change your data, when you fill out our forms on the website, purchase the Services, sign up to receive communications from us, contact us, etc).
- Automatically from your device when you use the Services or our website. When you browse on our website, different cookies and other similar technologies may be installed on your device, as set out in our Cookies Policy.
- From third parties - where this has been authorised by you or is legally permitted, or where it is necessary for us to provide the Services to you in certain scenarios. For instance:
    - when you have purchased or been provided with the Services by a third party (such as an employer);
    - when have authorised a third party website to share your personal details with us (such as when you connect to your Account via Telegram or Google); and

    - when we collaborate with third parties for marketing purposes.
- We assign or generate it ourselves (e.g., we may assign you an unique service ID).

YOUR RIGHTS

Your personal data is subject to certain rights:

1. The right to access	1. Confirm whether your personal data is processed and access such personal data or obtain a copy of the personal data undergoing processing. 2. Obtain details of such processing.
2. The right to rectification	Correct the inaccurate personal data and complete incomplete personal data, taking into account the nature of the personal data and the purposes of the processing.
3. The right to delete or erasure (the "right to be forgotten")	Delete personal data provided by, or obtained about, you. You have the right to request the deletion of your personal data when one of the following conditions applies: • the personal data are no longer necessary for the purposes for which they were processed; • the consent on which the processing is based is withdrawn, and where there is no other legal ground for the processing; • you object to the processing and there are no overriding legitimate grounds for the processing; • the personal data have been unlawfully processed; • the personal data have to be erased for compliance with a legal obligation. We will not erase the personal data where the processing is necessary for any of the following reasons: • for exercising the right of freedom of expression and information; • for compliance with a legal obligation which requires processing; • for the establishment, exercise or defence of legal claims.

4. The right to restrict the processing	You have the right to obtain a restriction of processing where one of the following applies: • you contest the accuracy of the personal data. In this case the restriction applies for a period enabling us to verify the accuracy of the personal data; • the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead; • we no longer need the personal data for the purposes of the processing, but you require them for the establishment, exercise, or defence of legal claims; • you have objected to the processing. In this case the restriction applies for the period of the verification whether the our legitimate grounds override yours. Where processing has been restricted, such personal data will, with the exception of storage, only be processed with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or of a Member State. You will be informed before the restriction of processing is lifted.
5. The right to opt-out, to object to processing, to withdraw your consent	• processing based on legitimate interest or public interest (you can object based on your specific situation) • direct marketing (you can object at any time, and processing must stop immediately) When we process your personal data on the basis of our **legitimate interest** you have the right to object to that processing. If you wish to exercise this right, please contact us at privacy@torrum.io When we process your personal data on the basis of your consent, you have the right to withdraw your consent.
6. The right to data portability	Obtain a copy of your personal data processed by us as the controller, in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another controller without hindrance, where the processing is carried out by automated means, provided us shall not be required to reveal any trade secret.
7. The right not to be subjected to automated decision-making	<u>If you located in the European Union</u> You can opt out of the processing of the personal data for purposes of profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning you.

In any case, you can always ask us how we process your data and how you can exercise your rights.

Please note that in order to process and fulfil your requests regarding the exercise of your rights, we are required to verify your identity. For this purpose, we may request additional information necessary to confirm your identity. If such information is not provided and we are unable to verify your identity, we will be unable to process your request or exercise your rights.

If you are resident in the European Economic Area and you believe we are unlawfully processing your personal information, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here: https://ec.europa.eu/newsroom/article29/items/612080/en .

If you are resident in Switzerland, the contact details for the data protection authorities are available here: https://www.edoeb.admin.ch/edoeb/en/home.html .

HOW WE USE YOUR PERSONAL DATA

We use personal data collected through our sites only when we have a valid reason and the legal grounds to do so. We determine the legal grounds based on the purposes for which we have collected your personal data.

The list of personal data processing activities is set out in APPENDIX 1 PURPOSES AND LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA.

We process personal data only where there is a lawful purpose and an appropriate legal basis for doing so. The specific legal basis is determined by the purposes for which the personal data were collected. Personal data may be processed on one of the following legal bases:

- **Consent.**
  We process personal data where you have given your consent. Such consent may be withdrawn by you at any time.
- **Performance of a contract (or taking steps necessary to enter into a contract).**
  We process personal data where this is necessary for the conclusion or performance of a contract with you.
- **Compliance with legal obligations.**
  In certain cases, we are required to use or retain personal data in order to comply with applicable legal requirements.
- **Legitimate interests.**
  We may process personal data where such processing is necessary for the purposes of our legitimate interests, is reasonably expected in the course of our company's activities, and does not unduly prejudice your rights and freedoms.

ANALYTICS

For the purposes of further development, improvement, and optimisation of the Service and the Website, we analyse data related to their use, including information about where visitors (users) come from, as well as which devices and browsers are used. For these purposes, we use third-party analytics services such as Google Analytics 4.

In addition, analytics are used to maintain and improve the security of the Service and the Website, as well as to prevent, detect, and analyse unlawful or potentially harmful activities.

The categories of data processed as part of such analytics are specified in the **APPENDIX 1**. Where possible, such data is processed in an aggregated and/or anonymised form and is not used by us to directly identify individual users.

Analytics services may use cookies and other similar technologies to collect data about the operation of the Website and the Service, as well as user behaviour.

You may opt out of the use of Google Analytics at any time.

The following options are available:

- **Change cookie settings**
  You can disable the use of analytics cookies via the consent banner or in the cookie settings available on our website. After analytics cookies are disabled, Google Analytics will stop collecting data about your visits.
- **Use the "Do Not Track" mode or browser settings**
  Most browsers allow you to limit the collection of analytics data or completely block the use of third-party cookies.
- **Install the Google Analytics opt-out browser add-on**
  Google provides a special browser add-on that allows you to completely disable the transmission of data to Google Analytics. You can install it at: https://tools.google.com/dlpage/gaoptout?utm_source=chatgpt.com After installing this add-on, Google Analytics will no longer receive data about your visits.

We use the **Google Signals** feature in Google Analytics. This feature applies **only** to users who are signed in to their Google Account and have consented to ads personalization in their Google settings.
In such cases, Google Analytics associates visitation information from our website with information from the user's Google Account for ads personalization and aggregated analytics reporting.

This information may include approximate location data and aggregated information from Google services such as search history, YouTube viewing history, and interactions with websites that partner with Google. The data is used to provide aggregated and de-identified reporting, including demographics, interests, and cross-device analytics.

Users can manage or delete this data through their Google Account settings, including **My Activity**.

WHO WE CAN SHARE YOUR PERSONAL DATA WITH

Third-party service providers we work with might handle your data on our behalf. You can view the list of such providers in the **APPENDIX 2**.

We may also share your information with third parties, such as:

- Mobile Operators: Service providers located in the appropriate jurisdiction for which the e-SIM service was purchased;
- Law enforcement agencies, government bodies, regulatory organisations (in particular in the electronic communications sector), courts or other public authorities if we have to, or are authorised to by law.

RETENTION OF PERSONAL DATA

The duration for which we are required or allowed to retain Personal data depends on the nature and the purposes for which the Personal data is processed.

The period during which we store your data may be determined by:

- Contractual or legal obligations applicable to us;
- The period necessary to provide you with services or information requested (e.g., to send newsletters or to provide information);
- Our legitimate business interests and the need to protect our rights and interests.

We keep personal data for marketing purposes for up to twelve (12) months or unless you have withdrawn your consent or unsubscribed from receiving newsletters.

Please be aware that we may not always be able to fulfill a request to erase personal data if it conflicts with our legal retention obligations. As we must demonstrate compliance with legitimate rights requests, we retain confirmation emails related to these requests for a period up to 5 years.

We take measures to delete or permanently deidentify Personal data once it is no longer required. In certain instances, we may opt to retain usage information in a depersonalized or anonymized format. Once Personal data has been anonymized and can no longer identify you, it no longer qualifies as Personal data and will not fall under our standard retention policies or be subject to the rights and choices outlined above.

INTERNATIONAL DATA TRANSFERS

Personal data is normally processed in the European Union / European Economic Area (EU / EEA), but in some cases it may be transferred and processed in non-EU / EEA countries. In some cases, your Personal data will be transferred to certain recipients (mainly our external service providers) who are located outside the European Economic Area in countries with laws and practices that do not contain equivalent data protection rights for your Personal Data (e.g. USA). Where such transfers occur, we ensure that appropriate safeguards are in place by ensuring that:

a) transfers do not occur without our prior written authority; and b) that an appropriate transfer mechanism, such as Standard Contractual Clauses (as approved by the European Commission) or

b) an adequacy decision of the European Commission, is in place to protect your Personal Data.

If you would like to find out more about any transfers which affect your Personal Data, please contact us by e-mailing privacy@torrum.oi

---

CHILDREN'S PERSONAL DATA

Our website and Services are not directed at children and we do not knowingly collect any personal information from anyone under the age of 18.

Information collected from devices or services purchased by adult users that are used by children without our knowledge will be treated as the adult's information under this Policy.

If you are a child and we learn that we have inadvertently obtained personal data from you from our website, or from any other source, then we will delete that information as soon as possible.

Please contact us at privacy@torrum.io if you are aware that we may have inadvertently collected personal data from a child.

SECURITY

We prioritize the security of your data and employ standard protection measures, ensuring that our partners also maintain an appropriate level of security.

Our goal is to protect user data by implementing all necessary and appropriate safeguards against loss, theft, misuse, unauthorized access, disclosure, alteration, or destruction. We maintain a

strong information security program with physical, technical, and administrative controls to keep your Personal data secure.

To ensure your Personal data is protected, we:

- Partner with reliable third parties who meet Personal data protection standards.
- Have established a comprehensive set of security policies across various areas.
- Control and differentiate access levels to your Personal data for our employees and third parties, and monitor data access and usage.
- Limit data access to only authorized employees who require it to fulfill their roles.
- Use encryption.

If you have any questions, please contact us.

PERSONAL DATA BREACH

Please note that no security system is perfect, and therefore we cannot fully guarantee the absolute security of the service or unauthorized access to personal data by third parties. In case of occurrence of such circumstances (events) we will take all reasonable measures to eliminate these circumstances (events) and their consequences.

If necessary, we will notify you of any violations related to your personal data breach and report such breach to the relevant authority for the supervision of compliance under the law.

Here are some key rules to prevent data theft on personal devices:

- *use strong passwords*: set strong, unique passwords for all your accounts and devices. Avoid using easily guessable information like birthdays or common words;
- *keep software updated*: regularly update your operating system, antivirus software, and applications to patch security vulnerabilities and protect against potential threats;
- *use secure wi-fi networks:* avoid connecting to public Wi-Fi networks for sensitive activities. If you must use public Wi-Fi, consider using a virtual private network (VPN) to encrypt your internet traffic;
- *be wary of phishing*: be cautious of unsolicited emails, messages, or phone calls asking for personal or financial information. Verify the sender's identity before responding or clicking on any links;
- *secure physical access*: keep your devices physically secure by using locks or biometric authentication methods. Avoid leaving your devices unattended in public places;
- *practice safe browsing habits*: avoid visiting suspicious websites or clicking on unfamiliar links. Install ad-blockers and browser security plugins to mitigate potential risks.

COOKIE AND SIMILAR TECHNOLOGIES

We use cookies and other similar technologies (such as pixels, pings, local storage elements, and other similar technologies) allowing us to store or gain access to information on your device. This help us to ensure the stable operation of our website, enhance user experience, perform analytics, and — where applicable — provide personalized advertising. For simplicity, all such technologies are referred to as "cookies."

We use both our own cookies and cookies placed by trusted third-party partners. Depending on their functional purpose, different categories of cookies may be used, including Necessary, Functional, Analytics, Performance, Advertisement, and Uncategorized cookies. A complete description of these categories, their purposes, storage periods, and relevant providers is available in our Cookie Policy, which forms part of this Privacy Policy.

You can manage your cookie preferences through the consent management interface on our website or via your browser settings. Most browsers let you remove or reject cookies in their settings. To do this, follow the instructions provided by your browser. These options are available in the "Privacy", "Security" or "Site settings" sections of your browser. The European Interactive Digital Advertising Alliance website – https://youronlinechoices.eu – allows you to install opt-out cookies across different advertising networks.

Please note that disabling certain categories of cookies may limit the functionality of some features.

Where the use of cookies relies on your consent, you may modify or withdraw it at any time.

CHANGES TO THE PRIVACY POLICY

This Policy may change periodically. We may update this Privacy Policy from time to time in response to changing legal, technical, or business developments.

Periodically reviewing our website is a good idea to stay informed about our privacy policies relating to your personal data.

The invalidation of certain provisions of the Privacy Policy for any reason does not entail the invalidity of the Privacy Policy as a whole or its other provisions.

APPENDIX 1 PURPOSES AND LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA

	Processing activity and purpose	Categories of processed data	Legal Basis
	Account creation and management	Unique identifiers Contact data Location data Technical data	Contract with You
	Order processing, E-sim service provision and payments	Unique identifiers Financial data Transaction data Service related user data	Contract with You
	Technical support	Unique identifiers Location data Technical data Communication / interaction data	Contract with You
	Referral program operation	Unique identifiers Referral link Referral reward	Contract with You
	Communicate developments, updates and news	Unique identifiers Contact data Communication / interaction data Company data	Your consent

	Obtain feedback from You and conduct analysis	Unique identifiers Contact data Company data Employment and work data Communication / interaction data Electronic communications data and metadata	Your consent
	Maintaining a database of our current customers, clients	Unique identifiers Employment and work data Company data	Our legitimate interest in maintaining business relationships and carry out interaction with clients
	Personalize and target marketing activities	Unique identifiers Contact data Company data Employment and work data Electronic communications data and metadata Communication / interaction data Metadata	Your consent

	Development, improvement and optimisation of our Service and Website	Unique identifiers Location data Technical data Behavioral data Web browsing data Electronic communications data and metadata Metadata Communication / interaction data	Our legitimate interests to enhance your user experience; improv and develop our service and website and their features
	Maintaining and improving Service and Website security and preventing unlawful activities	Unique identifiers Location data Behavioral data	Our legitimate interests to ensure and enhance security of our website and service

---

APPENDIX 2 LIST OF THIRD-PARTY PROVIDERS

Name of processor	**Processing activities**	**Country**
Stripe	Payment services	USA