

# BT EXCHANGE (LT) UAB

## Privacy Policy

Version: 1.0  
Updated: 23 January 2024

This privacy policy (the **Privacy Policy**) describes how BT Exchange (LT) UAB, registration code 306321553, registered address Gedimino pr. 20, Vilnius, Lithuania (the **Company** or **we**), processes personal data obtained from our suppliers, partners, candidates, or other persons when providing access and utility through our virtual asset trading platform via software, API (application program interface), technologies, products and / or functionalities (the **Services**).

This Privacy Policy describes what personal data we collect, how we obtain it, on what basis and for what purposes we use your personal data, how we use it, how long we store your personal data, who we share your personal data with, how we protect your personal data and your rights regarding your personal data.

### 1. Data controller

The Company is the data controller of your personal data listed in this Privacy Policy.

<b>Name</b>	BT Exchange (LT) UAB
<b>Legal entity code</b>	306321553
<b>Address</b>	Gedimino pr. 20, Vilnius, Lithuania
<b>E-mail</b>	<a href="mailto:majdi@bullionz.com">majdi@bullionz.com</a>
<b>Phone No</b>	[phone number]

We process your personal data listed below in accordance with the applicable legislation, including the Regulation (EU) 2016/679 (General Data Protection Regulation) (the **GDPR**) and other data protection laws. By using our Services, you become legally bound by this Privacy Policy.

By using any of the Services, or by providing the Company with any information about yourself, you understand that your personal data will be used as set out below. You are not allowed to use the Services if you do not fully agree to the Privacy Policy.

## 2. Personal data

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information which collected together can lead to the identification of the particular person also constitute personal data.

Please do not send to the Company any personal data, especially sensitive personal data, if you do not want such information to be used in this way.

The Services are available for individuals of 18 years of age or older.

## 3. Purposes for processing

The Company will collect and process your personal data for the following purposes:

### 3.1. Provision of the Services

<b>Purpose</b>	<p>Provision of the Services – providing access and utility through our virtual asset trading platform via software, API (application program interface), technologies, products and/or functionalities, i.e.:</p> <ul style="list-style-type: none"><li>■ enabling data subjects to create the account to access the Services,</li><li>■ enabling data subjects to manage the account details and information,</li><li>■ enabling data subjects to purchase / sell virtual assets,</li><li>■ enabling data subjects to transfer virtual assets,</li><li>■ enabling data subjects to perform other transactions with virtual assets.</li></ul>
<b>Data subjects</b>	<p>Users of the Services (if users are natural persons) / representatives of the users (if users are legal persons).</p>
<b>Personal data</b>	<ul style="list-style-type: none"><li>■ identification data (e.g., full name, position at the represented entity, name of the represented entity),</li><li>■ contact data (e.g., e-mail address, phone number),</li><li>■ usage data (information about your use of our Services, e.g., sign-up activity, virtual assets, bank details, payments),</li><li>■ other data related to the provision of our Services (e.g., communication with us regarding the use of our Services).</li></ul> <p>Please note that the Company may not process all the above data, and the scope of the processed data is determined on a case-by-case basis in accordance with the principle of data minimization.</p>
<b>Source</b>	<p>The user or the entity it represents, the use of the Services and / or third parties (e.g., payment service providers).</p>
<b>Legal ground(s) for processing</b>	<p>Such processing is necessary for the provision of our Services to our users (Article 6(1)(b) of the GDPR) and our legitimate interest to provide safe and reliable services, as well as to enter into contractual relations with the legal entity you represent (Article 6(1)(f) of the GDPR).</p> <p>If you do not provide this information, we may be unable to provide you with requested Services.</p>
<b>Data retention</b>	<p>Data will be stored for up to 10 years following the end of relations with the user.</p>

### 3.2. Compliance with legal requirements (e.g., AML / KYC)

<b>Purpose</b>	Compliance with legal requirements applicable to the Company, including anti-money laundering (AML) and <i>Know Your Customer</i> (KYC) regulations.
<b>Data subjects</b>	Users of the Services (if users are natural persons) / representatives, shareholders, managers, ultimate beneficial owners (UBOs) of the users (if users are legal persons).
<b>Personal data</b>	<ul style="list-style-type: none"> <li>■ identification data (e.g., full name (including former name), position at the represented entity, name of the represented entity, nationality, passport number or any government issued ID number, date of birth, proof of identity (e.g., passport)),</li> <li>■ contact data (e.g., address, e-mail address, phone number),</li> <li>■ AML / KYC data (e.g., date of birth, citizenship, address, country of residence, country of tax residence, activities, sources of income, copy of identification document (and personal data included therein), bank details, information about applied international sanctions, politically exposed person (PEP) status),</li> <li>■ payment data (e.g., information about payments via the Services, including recipients),</li> <li>■ other personal data as may be required for the Company to comply with applicable legal acts).</li> </ul> <p>Please note that the Company may not process all the above data, and the scope of the processed data is determined on a case-by-case basis in accordance with the principle of data minimization.</p> <p>The Company may also use profiling in order to enable the fulfilment of the requirements of the abovementioned legal obligations on anti-money laundering and countering the financing of terrorism (AML/CFT). Please see Section 7 of this Privacy Policy for more information.</p>
<b>Source</b>	The user or the entity it represents, the use of the Services and / or third parties (e.g., identification service providers, public registers, state and / or municipality institutions).
<b>Legal ground(s) for processing</b>	<p>Such processing is necessary for the Company to comply with legal requirements (e.g., AML / KYC obligations) (Article 6(1)(c) of the GDPR).</p> <p>Personal data of special categories, if any, will be processed in order for us to comply with AML / KYC legal requirements (Articles 6(1)(c) and 9(2)(g) of the GDPR), and, if required in particular cases, upon your consent (Articles 6(1)(a) and 9(2)(a) of the GDPR).</p> <p>Data on convictions and criminal offenses will only be processed when and to the extent required by applicable law.</p> <p>If you do not provide this information, we may be unable to provide you with requested Services.</p>
<b>Data retention</b>	Data will be stored for up to 8 years following the end of relations with the user. If the supervisory authority adopts a respective decision, such personal data may be stored for 2 additional years.

### 3.3. Recruiting

<b>Purpose</b>	Processing personal data in relation with recruitment procedures.
<b>Data subjects</b>	Candidates to work at the Company.
<b>Personal data</b>	<ul style="list-style-type: none"> <li>■ identification data (e.g., full name),</li> </ul>

	<ul style="list-style-type: none"> <li>■ contact data (e.g., e-mail address, phone number),</li> <li>■ information about your experience, education and other information provided by you in your CV and (or) other documents or communication with the Company,</li> <li>■ information required to verify whether candidate is in line with the legal requirements applicable to the Company (e.g., impeccable reputation), where applicable,</li> <li>■ information obtained from current (only upon receiving your explicit consent) or previous (only upon informing you thereof) employers,</li> <li>■ information about the results of the recruitment procedures (e.g., results of tests, interviews).</li> </ul> <p>Please note that the Company may not process all the above data, and the scope of the processed data is determined on a case-by-case basis in accordance with the principle of data minimization.</p>
<b>Source</b>	The candidate himself / herself, or his / her current or previous employers.
<b>Legal ground(s) for processing</b>	<p>Such processing is necessary for the Company in order to take steps at the request of the data subject prior to entering into an employment contract (Article 6(1)(b) of the GDPR), for the legitimate interest of the Company to carry out the recruitment procedures (Article 6(1)(f) of the GDPR), in order to comply with the applicable legal obligations (e.g., requirements on impeccable reputation) (Article 6(1)(c) of the GDPR) or your consent (Article 6(1)(a) of the GDPR).</p> <p>Data on convictions and criminal offenses will only be processed when and to the extent required by applicable law.</p> <p>If you do not provide the information required by the Company to enter into contractual relations with you or to comply with our legal obligations, we may refuse to enter into employment relations.</p>
<b>Data retention</b>	The Company will store the personal data about the candidate for as long as the selection to the specific position is taking place. Based on your consent such personal data may be stored longer.

### 3.4. Relations with suppliers & partners

<b>Purpose</b>	Commercial relations with our suppliers & partners, e.g., day-to-day business communication related to the services and (or) goods provided.
<b>Data subjects</b>	Our suppliers & partners or their representatives.
<b>Personal data</b>	<ul style="list-style-type: none"> <li>■ identification data (e.g., full name, position at the represented entity, name of the represented entity),</li> <li>■ contact data (e.g., address, e-mail address, phone number),</li> <li>■ payment data (e.g., bank account number, information about payments to or from our suppliers &amp; partners),</li> <li>■ subject matter and text of the communication with us.</li> </ul> <p>Please note that the Company may not process all the above data, and the scope of the processed data is determined on a case-by-case basis in accordance with the principle of data minimization.</p>
<b>Source</b>	Our suppliers & partners or their representatives and / or third parties (e.g., banks).

<b>Legal ground(s) for processing</b>	<p>Such processing is necessary for the performance of the agreement between the Company and the respective supplier or partner (Article 6(1)(b) of the GDPR), for the legitimate interest of the Company to maintain the respective contractual relations with the legal entity the data subject represents (Article 6(1)(f) of the GDPR) or to comply with legal requirements (e.g., accounting) (Article 6(1)(c) of the GDPR).</p> <p>If you do not provide the information required by the Company to comply with legal requirements (e.g., accounting) or maintain contractual relations, we may be unable to carry out our contractual obligations.</p>
<b>Data retention</b>	Data will be stored for up to 10 years following the receipt of such data or termination of the respective agreement.

### 3.5. Direct interactions

<b>Purpose</b>	Managing and answering the inquiries sent / provided to the Company via e-mail, phone or other means.
<b>Data subjects</b>	Persons submitting / providing the abovementioned inquiries to the Company.
<b>Personal data</b>	<ul style="list-style-type: none"> <li>■ identification data (e.g., full name, position at the represented entity, name of the represented entity),</li> <li>■ contact data (e.g., e-mail address, phone number),</li> <li>■ subject matter and text of the communication with us.</li> </ul> <p>Please note that the Company may not process all the above data, and the scope of the processed data is determined on a case-by-case basis in accordance with the principle of data minimization.</p>
<b>Source</b>	Persons submitting / providing the abovementioned inquiries to the Company themselves.
<b>Legal ground(s) for processing</b>	Such processing is necessary for the legitimate interest of the Company to answer such inquiries (Article 6(1)(f) of the GDPR) or in order to comply with the respective legal obligation where the Company has a legal obligation to submit a reply (Article 6(1)(c) of the GDPR).
<b>Data retention</b>	Data will be stored for 2 years following the receipt of your query.

### 3.6. Direct marketing

<b>Purpose</b>	Informing you about special offers, news or providing other information about the services of the Company.
<b>Data subjects</b>	Persons receiving the abovementioned communications from the Company.
<b>Personal data</b>	<ul style="list-style-type: none"> <li>■ identification data (e.g., full name, position at the represented entity, name of the represented entity),</li> <li>■ contact data (e.g., e-mail address, phone number),</li> <li>■ information about purchased or otherwise used Services.</li> </ul> <p>Please note that the Company may not process all the above data, and the scope of the processed data is determined on a case-by-case basis in accordance with the principle of data minimization.</p>

<b>Source</b>	Persons receiving the abovementioned communications from the Company themselves and the use of the Services.
<b>Legal ground(s) for processing</b>	<ul style="list-style-type: none"> <li>■ your consent to the processing of personal data for direct marketing purposes (Article 6(1)(a) of the GDPR), or</li> <li>■ our legitimate interest to inform our users about similar services of the Company (Article 6(1)(f) of the GDPR).</li> </ul> <p>Based on our legitimate interest to inform our customers about our similar services, the Company will process your e-mail address for direct marketing purposes only if all the following conditions are met:</p> <ul style="list-style-type: none"> <li>■ by using service from the Company, you do not initially object to the direct marketing communications,</li> <li>■ each time we send a direct marketing message, you will be given the option to opt out from such direct marketing messages, and</li> <li>■ on this basis, your personal data will only be processed for the marketing of similar services of the Company itself.</li> </ul> <p>You can unsubscribe from marketing messages at any time.</p>
<b>Data retention</b>	Your personal data will be processed for this purpose for 2 years from the date of its collection, or until you object to such processing of your personal data, or until your consent to process personal data for this purpose is revoked, whichever occurs first.

### 3.7. Improving the Services and ensuring their proper operation and security, ensuring fraud prevention

<b>Purpose</b>	Improving the Services and ensuring their proper operation and security, ensuring fraud prevention.
<b>Data subjects</b>	Users of the Services.
<b>Personal data</b>	<ul style="list-style-type: none"> <li>■ device data (e.g., internet protocol (IP) addresses, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access the Services),</li> <li>■ information about your use of the Services.</li> </ul> <p>Please note that the Company may not process all the above data, and the scope of the processed data is determined on a case-by-case basis in accordance with the principle of data minimization.</p>
<b>Source</b>	Your use of the Services.
<b>Legal ground(s) for processing</b>	Our legitimate interest to improve our Services, ensure their proper operation and security, also our legitimate interest to prevent fraud (Article 6(1)(f) of the GDPR).
<b>Data retention</b>	Your personal data will be processed for this purpose for 5 years.

### 3.8. Legal claims and dispute resolution

The Company may process all the above personal data for the purpose of presenting, enforcing, or defending against legal claims. For this purpose, we will process personal data based on our legitimate interest of presenting,

enforcing, or defending against legal claims (Article 6(1)(f) of the GDPR). We will process it for this purpose for 1 year following the end of the relevant legal proceedings (for example, the final decision of a court or arbitration).

#### 4. Data recipients

Any information that you provide may be shared with third parties (data processors), which provide the Company with services and act on its behalf (e.g., companies providing marketing / advertising services, IT service providers, accounting service providers, etc.). The Company ensures that processing of personal data by such third parties will be based on legitimate legal grounds and will be performed in accordance with lawful instructions of the Company and in compliance with the GDPR and other legal requirements.

Specifically, the Company may share personal data with the following categories of third parties (data processors or individual data controllers) as necessary:

- payment service and your cryptocurrency wallet providers (if needed and to the extent required for proper provision of the Services),
- our affiliates, i.e., subsidiaries, joint venture partners or parent companies (if needed for proper internal administration of the group (e.g., accountability) or where we obtain services from other group companies),
- courts, arbitrators, mediators, opposing party and their lawyers (if needed for the legal proceedings),
- police, law enforcement authorities, tax authorities, other government, or municipal institutions,
- our professional advisers such as lawyers or accountants (if needed for the protection of our legitimate interests),
- service providers who provide information technology and system administration services, marketing, accounting, postal or courier or other services,
- other natural or legal persons where this is related to and necessary for the organizational changes of the Company, e.g., in the event of merger, acquisition, or sale of our assets (as a whole or in part), your personal data could be shared with auditors or other representatives of the potential acquirers and transferred to the final acquirer. Please note that in the latter situation the data controller of your personal data could become the final acquirer. You would be informed about such organizational changes,
- other persons or entities (if needed to provide you with the Services as effectively as possible).

#### 5. Third countries

The Company will not transfer your personal data to third countries (countries outside the EU/EEA), unless this is deemed necessary. This may be the case if the Company must involve external parties, e.g., IT providers. The Company makes every effort to ensure that such data transfers comply with the requirements of the GDPR and implements appropriate measures to ensure that your personal data remains protected and secure. You may find out more about such measures by contacting us directly via phone or e-mail as indicated above.

#### 6. Your rights

##### Right of access

You have the right to obtain from the Company the confirmation as to whether your personal data is being processed and to access the information about how the Company processes your personal data, as well as to receive the copy of your personal data.

##### Right to rectification

You have the right to obtain from the Company the rectification of your inaccurate personal data. You also have the right to have incomplete personal data completed by providing a supplementary statement.



<b>Right to erasure ('right to erasure')</b>	<p>You have the right to obtain from the Company the erasure of your personal data, if conditions established in Article 17 of the GDPR are met.</p> <p>Please note that Article 17(3) of the GDPR establishes some exceptions for such cases where processing is necessary. If they are applied in your case, we will inform you about them accordingly.</p>
<b>Right to restriction of processing</b>	<p>You have the right to obtain from the Company restriction of processing if conditions established in Article 18 of the GDPR are met.</p> <p>Where processing has been restricted, such personal data shall, except for 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.</p>
<b>Right to data portability</b>	<p>You have the right to receive your personal data, which you have provided to the Company, in a structured, commonly used, and machine-readable format and have the right to transfer this data to another controller, if:</p> <ul style="list-style-type: none"><li>■ the processing is based on a consent or on a contract, and</li><li>■ the processing is carried out by automated means.</li></ul> <p>You also have the right to have the personal data transferred directly from the Company to such another controller, where technically feasible.</p>
<b>Right to object</b>	<p>You have the right to object at any time to processing of your personal data for the purposes of the legitimate interests of the Company, including profiling based on those provisions.</p> <p>The Company will no longer process the personal data unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights, and freedoms, or for the establishment, exercise, or defence of legal claims.</p> <p>Where you object to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.</p>
<b>Right to withdraw the consent</b>	<p>If the processing of your personal data is based on your consent, you have the right to withdraw this consent at any time. Your withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.</p>
<b>Right to lodge a complaint with a supervisory authority</b>	<p>You have the right to lodge a complaint with a supervisory authority in the EU member state of your habitual residence, place of work or place of the alleged infringement if you consider that the processing of your personal data infringes the GDPR.</p> <p>Lithuanian supervisory authority is Lithuanian State Data Protection Inspectorate, address L. Sapiegos str. 17, 10312 Vilnius, Lithuania, e-mail <a href="mailto:ada@ada.lt">ada@ada.lt</a>, website <a href="https://vdai.lrv.lt/">https://vdai.lrv.lt/</a>.</p> <p>The Company would recommend and be grateful if you contact us before lodging a complaint to the relevant supervisory authority and express your concerns or questions to us. We will do our best to assist you with all your queries.</p>

All abovementioned requests shall be sent via e-mail address as provided above in the Privacy Policy. The Company will examine your request to exercise the rights of the data subject within 1 month. This period may be extended, if necessary, for a further period of 2 months, considering the complexity and number of requests. In this case, the Company will notify you of any such extension within 1 month of receipt of the request, together with the reasons for the delay.



If, upon the receipt of a request, we have suspicions regarding your identity, we have the right to request additional information necessary to confirm your identity.

### 7. Profiling

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

The Company uses profiling to monitor risks related to the anti-money laundering and countering the financing of terrorism (AML/CFT) as required by legal obligations applicable to the Company. For this purpose, the Company uses an automated screening service and a risk matrix. The system may trigger potential alerts ("red flags"), e.g., status of politically exposed person (PEP) or adverse media relevant to our legal obligations, which will be further analyzed by our compliance agents. In order to investigate or address the alert generated by the system, our compliance agents may contact you to obtain more information or place you under the appropriate risk category.

The Company will not make decisions based solely on automated processing, including profiling, which produce legal effects concerning you or similarly significantly affect you as all such situations will be subject to verification of our employees.

### 8. Security of your personal data

Your personal data will be processed in accordance with the GDPR requirements, the Law on Legal Protection of Personal Data of the Republic of Lithuania, and other applicable legal acts. When processing your personal data, we implement organizational and technical measures that ensure the protection of personal data against accidental or unlawful destruction, alteration, disclosure, and any other unlawful processing. The Company takes various measures to ensure information security, including encryption of the communications with SSL, required two-factor authentication for all sessions, periodic review of our personal data collection, storage, and processing practices, and restricted access to client's personal data on a need-to-know bases for our employees and vendors who are subject to strict contractual confidentiality obligations.

The Company is committed to responsible data practices, user rights, and data protection principles against security breaches, including:

- Unauthorized access – the Company prevents unauthorized access to user data. This includes implementing secure login procedures, access controls, and encryption techniques to protect data from being accessed by unauthorized individuals,
- Data breaches – the Company prevents data breaches by implementing security measures such as firewalls and encryption protocols and outlining the process in the event of a breach, ensuring prompt communication to affected users and relevant authorities,
- Employee training and awareness – the Company emphasizes the importance of employee training and awareness regarding data security practices by providing regular training sessions, establishing data protection policies, and enforcing strict confidentiality obligations for employees handling sensitive data,
- Secure data transfers – where the user data is transferred to third parties, the Privacy Policy outlines the measures taken to ensure the security of such transfers,
- Security audits and assessments – the Company conducts periodic security audits and assessments to identify vulnerabilities and ensure compliance with industry best practices.

The Company may generate anonymized data based on personal data from which your identity cannot be determined. Fully anonymized data does not meet the criteria necessary to qualify as personal data and is not subject to this Privacy Policy.

Although we aim to protect your personal data, the transfer of data via the internet is not 100% secure, so we cannot fully guarantee secure transfer of data via the internet.

### 9. Changes

The Company may, at its sole discretion, change, modify, add, or remove any portion of this Privacy Policy, in part or in its entirety, at any time based on new functions or regulations.

Any changes to this Privacy Policy are effective from the date of their publication and (or) communication via contact details, where possible. You undertake to review this Privacy Policy periodically to become aware of any changes. If we have your contact details, we will inform you about such changes separately.