Data Protection Policy

1. Introduction

1.1 This Data Protection Policy is the overarching policy for data security and protection for **BT Exchange LT (Lithuania) and BT Exchange CZ (Czech Republic)** (hereafter referred to as "us", "we", or "our"). The policy ensures compliance with **General Data Protection Regulation (GDPR - EU Regulation 2016/679)**, the **Lithuanian Law on Legal Protection of Personal Data**, and the **Czech Act on Personal Data Processing (Act No. 110/2019 Coll.)**.

2. Purpose

2.1 This GDPR Privacy Policy explains how the Company uses client's Personal Data (defined below) company provides access and utility through our digital platform via software, API (application program interface), technologies, products and/or functionalities ("Service").

2.2 In the course of providing Service, this GDPR is made to abide by the laws in the jurisdictions that the company operates, and to improve services, company needs to collect and maintain personal information about the client.

2.3 The purpose of the Data Protection Policy is to support the 10 Data Security Standards, the General Data Protection Regulation (2016), the Data Protection Act (2018), the common law duty of confidentiality, and all other relevant national legislation. We recognize data protection as a fundamental right and embrace the principles of data protection by design and by default.

2.4 This policy covers:

- Our data protection principles and commitment to common law and legislative compliance.
- procedures for data protection by design and by default.

3. Collection of Personal Data

3.1 Company collects, processes, and stores Personal Data collected from you via client's use of the Service or where client has given consent.

3.2 This Personal Data may include contact details, copies of identification documentation provided by client or derived from publicly accessible databases, government identification number as well as information relating to devices or internet service (such as an IP address and a MAC number).Company collects information provided during the onboarding process, which may be a completed, incomplete, or abandoned process.

3.3 Company collects data on the client for the purpose of processing orders, managing and verifying accounts, and promotion offers.

3.4 Company collects, uses, stores, and transfers Personal Data, which may include the following:

(i) Operating within the European Economic Area ("EEA").

(ii) Company collects, stores, and processes personal information in accordance with the Best Practices of the Data Collection in the EU and GDPR [General Data Protection Regulation- (EU) REGULATION 679/2016].

(iii) Types of client defined in APPENDIX A.

3.5 Right to Data Portability- Client has a right to receive his/ her Data in a coherent, structured and readable manner.

4. Collection and Storing of Data Outside the EU

4.1 As outlined above, company may collect Personal Data from customers located in the EEA. To facilitate the services company provides to customers located in the EEA, company requests explicit consent for the transfer of Personal Data from the EEA to outside of the area. If client is an individual located in the EEA and declines to consent to such transfer, client will no longer be able to use company services.

4.2 Client will have the ability to withdraw all digital assets; however, all other functionalities will be disabled.

- BT EXCHANGE (LT) UAB & BT EXCHANGE CZ need to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees, and other people the organization has a relationship with or may need to contact.

- This policy describes how this personal data must be collected, handled, and stored to meet the company's data protection standards- and to comply with the law.

- This policy includes in its scope all data that we process either in hardcopy or digital copy, this includes special categories of data.

This data protection policy ensures BT EXCHANGE (LT) UAB & BT EXCHANGE CZ:

- Comply with data protection law and follows good practice.
- Protects the rights of staff, customers, and partners.
- Is open about how it stores and processes individuals's data
- Protects itself from the risks of a data breach.

5. Data Protection Law

The Data Protection Act 1998 describes how organizations- including BT EXCHANGE (LT) UAB & BT EXCHANGE CZ - must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.

The Data protection Act is underpinned by eight important principles. These say that personal data must:

- ✓ Be processed fairly and lawfully.
- ✓ Be obtained only for specific, lawful purposes.
- ✓ Be adequate, relevant, and not excessive.
- ✓ Be accurate and kept up to date.
- ✓ Not be held any longer than necessary.
- ✓ Processed in accordance with the rights of data subjects.
- ✓ Be protected in appropriate ways.
- ✓ Not to be transferred outside the European Economic Ares (EEA), unless that country or territory also ensures an adequate level of protection.

6. Definitions

Personal Data: Any information relating to an identified or identifiable natural person, as defined in the Lithuanian Law on Legal Protection of Personal Data and the GDPR.

Data Subject: An identified or identifiable natural person to whom the personal data relates.

Data Controller: The natural or legal person, public authority, agency, or other body that determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the Data Controller.

Data recipient shall mean a legal or a natural person to whom personal data are disclosed.

Disclosure of data shall mean disclosure of personal data by transmission or making them available by any other means.

The consent shall mean an indication of will be given freely by a data subject indicating his agreement to the processing of his personal data for the purposes known to him. His consent with regard to special categories of personal data must be expressed clearly, in a written or equivalent form or any other form giving unambiguous evidence of the data subject's free will.

A third party shall mean a legal or a natural person, with the exception of the data subject, the data controller, the data processor, and persons who have been directly authorized by the data controller or the data processor to process data.

7. Lawful Bases for Processing Personal Data

BT EXCHANGE (LT) UAB & BT EXCHANGE CZ will only process personal data if at least one of the following lawful bases is met:

Consent: The Data Subject has given explicit consent for the processing of their personal data for one or more specific purposes.
Contractual Obligations: The processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract.

Legal Obligations: The processing is necessary for compliance with a legal obligation to which the Company is subject.

Legitimate Interests: The processing is necessary for the legitimate interests pursued by the Company or a third party, except where such interests are overridden by the interests, rights, or freedoms of the Data Subject.

8. Rights of Data Subject

Company would like to assure its clients with their privacy rights under GDPR [General Data Protection Regulation- (EU) REGULATION 679/2016] by informing them on their rights under the mandated EU Legislation:

8.1 Right to Access- Clients have a right to request copies of their personal data.

8.2 Right to Rectification- Client has a right to request that Company corrects any information that Client believes to be incorrect, or complete information that is incorrect in the Client's opinion.

8.3 Right to Erasure- Client has a right to request deleting his/her personal data, under conditions mandated in Art. 17 GDPR [General Data Protection Regulation- (EU) REGULATION 679/2016].

8.4 Right to Restrict Processing- Client has a right to request restriction on his/her personal data processing, under conditions mandated in Art. 18 GDPR [General Data Protection Regulation- (EU) REGULATION 679/2016].

8.5 Right to Object to Processing- Client has a right to object his/her personal data processing, under conditions mandated in Art. 19 GDPR [General Data Protection Regulation- (EU) REGULATION 679/2016].

9. People, risks, and responsibilities

This policy applies to:

- The head office of BT EXCHANGE (LT) UAB & BT EXCHANGE CZ
- All branches if any of BT EXCHANGE (LT) UAB & BT EXCHANGE CZ
- All staff and volunteers of BT EXCHANGE (LT) UAB & BT EXCHANGE CZ
- All contractors, suppliers and other people working on behalf of BT EXCHANGE (LT) UAB & BT EXCHANGE CZ

It applies to all data that the company hold relating to identifiable individuals, even if that information technically falls of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

10. Data Protection Risks

This policy helps to protect BT EXCHANGE (LT) UAB & BT EXCHANGE CZ from dome very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational change.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

11. Responsibilities

Everyone who works for or with BT EXCHANGE (LT) UAB & BT EXCHANGE CZ has some responsibilities for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The **board of directors** is ultimately responsible for ensuring that BT EXCHANGE (LT) UAB & BT EXCHANGE CZ meets its legal obligations.

- The **Data Protection Officer, ,** is responsible for:
    - Keeping the board updated about data protection responsibilities, risks, and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.

- Dealing with requests from individuals to see the data BT EXCHANGE (LT) UAB & BT EXCHANGE CZ hold about them (also called "subject access requests").
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

- The **IT Manager, ,** is responsible for:
  - Ensuring all systems, services, and equipment used for data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

- The **Marketing Manager,** is responsible for:
  - Approving any data protection statements attached to communication such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

12. Marketing

12.1 Company may communicate company news, promotions, and information relating to our products and services provided. Company may share Personal Data with third parties to help with marketing and promotional projects, or sending marketing communications. By using our services, client accepts this Privacy Policy and agrees to receive such marketing communications.

12.2 Customers can opt out from these marketing communications at any moment. If you do not want to receive these communications, please send an email to support@bullionz.com

12.3 For product related communications, such as policy/terms updates and operational notifications, client will not be able to opt out of receiving such information.

13. General Staff Guidelines

- The only people able to access data covered by this policy should be those who **need it for their work.**

- Data **should not be shared informally.** When access to confidential information is required, employees can request it from their line managers.

- **BT EXCHANGE (LT) UAB & BT EXCHANGE CZ will provide training** to all employees to help them understand their responsibilities when handling data.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

- In particular, **strong passwords must be used,** and they should never be shared.

- Personal data **should not be disclosed** to unauthorized people, either within the company or externally.

- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

- Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

14. Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper**, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet.**

- Employees should make sure paper and printouts are **not left where unauthorized people could see them,** like on a printer.

- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion, and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.

- If data is **stored on removable media** (like CD or DVD), these should be kept locked away securely when not being used.

- Data should only be stored on **designated drives and servers** and should only be uploaded to approved cloud computing services.

- Servers containing personal data should be **sited in a secure location**, away from general office space.

- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.

- Data should **never be saved directly** to laptops or other mobile devices like tablets or smartphones.

- All servers and computers containing data should be protected by **approved security software and a firewall**.

14. Personal Data Usage

14.1 Company uses Personal Data to communicate with the client and to administer, deliver, improve, and personalize the Service. Company might also generate generic data out of any Personal Data collected and use it for company purposes.

14.2 Company may also use such data to communicate with you in relation to other products or services offered by company and/or its partners. Company does not share Personal Data with third parties (other than partners in connection with their services) except where client have given consent and further detailed below.

14.3 **Company may share Client Personal Data with third parties:**

14.3.1 If company deems that sharing it is necessary to enforce the Terms of Service；

14.3.2 To comply with government agencies, including regulators, law enforcement and/or justice departments

14.3.3 To third parties who provide services to the company (such as administration or technical services) ;

14.3.4 In connection with the sale or transfer of our business or any part thereof.

14.3.5 Additionally, company has implemented international standards to prevent money laundering, terrorist financing and circumventing trade and economic sanctions and will implement final Virtual Financial Asset rules and regulations when effective, which will likely require us to undertake due diligence on our customers. This may include the use of third-party data and service providers which we will cross-reference with your personal information.

-

15 Data Accuracy

The law requires BT EXCHANGE (LT) UAB & BT EXCHANGE CZ to take responsible steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort BT EXCHANGE (LT) UAB & BT EXCHANGE CZ should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up-to-date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.

- Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call.

- BT EXCHANGE (LT) UAB & BT EXCHANGE CZ will make it **easy for data subjects to update the information** BT EXCHANGE (LT) UAB & BT EXCHANGE CZ hold about them. For instance, via the company website.

- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

16 Subject Access Requests

All individuals who are the subject of personal data held by BT EXCHANGE (LT) UAB & BT EXCHANGE CZ are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed on **how to keep it up to date**.
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individual should be made by mail. Addressed to the data controller at majdi@bullionz.com. The data controller cam supply a standard request form, although individuals do not have to use this.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

17 Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, BT EXCHANGE (LT) UAB & BT EXCHANGE CZ will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

APPENDIX "A"

Definition of Clients

Individual clients:

1. Email address
2. Mobile phone number
3. Full legal name (including former name, and names in local language)
4. Nationality
5. Passport number, or any government issued ID number
6. Date of birth ("DOB")
7. Proof of identity (e.g. passport, driver's license, or government-issued ID)
8. Residential address
9. Proof of residency
10. Additional Personal Data or documentation at the discretion of our Compliance Team

Corporate clients:

1. Corporate legal name (including the legal name in local language)
2. Incorporation/registration Information
3. Full legal name of all beneficial owners, directors, and legal representatives
4. Address (principal place of business and/or other physical locations)
5. Proof of legal existence
6. Description of the business
7. Percentage of ownership for Individual/corporate owners
8. Contact information of owners, principals, and executive management (as applicable)
9. Proof of identity (e.g., passport, driver's license, or government-issued ID) for significant individual beneficial owner of the institutional customer entity
10. Personal Data for each entity's significant beneficial owner of the institutional customer entity (see the "Individual Customer" section above for details on what Personal Data we collect for individuals)
11. Source of wealth