BT EXCHANGE (LT) UAB
Data Protection Policy

Version: 1.0
Updated: 06 February 2024

This Data Protection Policy (the **Data Protection Policy**) is the overarching policy for data security and protection for BT EXCHANGE (LT) UAB (the **Company** or **we**) designated to set forth the requirements for data processing at the Company.

The purpose of the Data Protection Policy is to support the requirements of the GDPR, the Law 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.

BT EXCHANGE (LT) UAB
Data Protection Policy

Version: 1.0
Updated: 06 February 2024

1. Definitions

In this Data Protection Policy, the following terms either in uppercase or in lowercase shall have the following meanings:

Definition	Meaning
Company	BT Exchange (LT) UAB, legal entity code 306321553, address Gedimino pr. 20, Vilnius, Lithuania.
Data Controller *or* Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of data.
Data Processing *or* Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data Processor *or* Processor	The natural or legal person, public authority, agency, or other body which processes data on behalf of the data controller.
Data Protection Impact Assessment *or* DPIA	Tools and assessments used to identify and reduce risks of a data processing activity as required by Article 35 of the GDPR. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the processing of personal data.
Data Subject	An identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
EEA	The 27 countries of the European Union (EU), and Iceland, Liechtenstein, Norway.
Staff *or* Staff Member	Employees of the Company and other staff members, for example, self-employed persons (e.g., service providers) who provide services to the Company and whose status is in essence equivalent to employees.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Law	The Law on Legal Protection of Personal Data of the Republic of Lithuania.
Laws	All applicable laws on data protection, including the GDPR, the Law and other national or international legal acts applicable to the Company.
Personal Data *or* Data	Any information relating to an identified or identifiable natural person (i.e., data subject).

Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Privacy by Design	Implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.
Recipient	A natural or legal person, public authority, agency or another body, to which the personal data is disclosed, whether a third party or not.
Responsible Person	Person responsible for handling matters related to data protection at the Company, i.e., Data Protection Officer and IT Manager (it@bullionz.com).
Supervisory Authority	An independent public authority which is established by EU Member State pursuant to Article 51 of the GDPR. Supervisory authority in Lithuania is the State Data Protection Inspectorate, L. Sapiegos str. 17, LT-10312 Vilnius, Lithuania, phone No: +370 5 271 2804 / 279 1445, fax +370 5 261 9494, e-mail ada@ada.lt.

2. Data Processing Principles

Personal data shall be processed at the Company following the Laws and other standards that regulate data protection, data processing and information security.

At the Company, the personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject ('*lawfulness, fairness and transparency*'),
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('*purpose limitation'*),
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('*data minimisation'*),
- accurate and, where necessary, kept up to date ('*accuracy*'),
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed ('*storage limitation'*),
- processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('*integrity and confidentiality'*).

The Company shall be responsible for and be able to demonstrate compliance with the above principles ('*accountability*').

If the Company violates at least one of the above data processing principles, such processing may be considered as non-compliant.

If any Staff Member have any doubts about the implementation of the above principles, they must immediately address them to the Responsible Person or line manager.

2.1. Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

The Company may only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR allows data processing in the presence of applicable legal basis for the processing, such as:

- the data subject has given a consent,
- the processing is necessary for the performance of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract,
- to comply with legal obligations of the Company,
- to protect the data subject's vital interests,
- to perform a task carried out in the public interest or in the exercise of official authority vested in the Company,
- to pursue legitimate interests of the Company where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

The Company may also process special category data if any of the abovementioned legal basis, as well as any of the exceptions listed in Article 9 of the GDPR, is applicable.

The Company must identify and document the legal ground being relied on for each processing activity.

Furthermore, the GDPR requires the Company to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. The information provided must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand it. The full list of information to be provided to the data subjects is established in Articles 13-14 of the GDPR, and the Company shall comply with this obligation.

In the event of (a) new processing activities, (b) changes in processing activities already carried out, or (c) termination of any processing activities, such changes shall be communicated to the Responsible Person and coordinated in advance (if this is not possible, as soon as it becomes possible).

The Company shall assess the processing activities and make sure that the proper legal ground is being relied on for each processing activity.

If Staff Members have any doubts about the implementation of the above principle, they must immediately address them to the Responsible Person or line manager.

Where the Company seeks to process personal data on the basis of consent, it shall be freely given, specific, informed and unambiguously given in order to make the processing of personal data legitimate.

Data subject consents to processing of his/her personal data if he/she indicates such position clearly either by a statement or positive action. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are insufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data subjects must be able to easily withdraw consent at any time and withdrawal must be promptly honoured.

Consent may need to be refreshed if the Company intends to process personal data for a different and incompatible purpose which was not disclosed when the data subject first consented.

The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof.

The Company needs to keep records of all consents and have sufficient evidence thereof so that the Company can demonstrate its compliance with requirements on consent.

If personal data is processed on the basis of consent, the Company and its Staff Members must make sure that the consent has been obtained before performing any related processing activities.

Any processing activities on such basis are strictly prohibited until it is ascertained that the Company has obtained the consent that meets the abovementioned requirements.

2.2. Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

The Company cannot use personal data for new, different or incompatible purposes from that disclosed to data subjects when it was first obtained unless it has informed the data subjects of the new purposes and they have consented where necessary.

The Company and its Staff Members must make sure that the personal data collected for specified, explicit and legitimate purposes is not further processed in a manner that is incompatible with those purposes.

For instance, if personal data is collected in order to obtain services from a person, it may not be used in order to send marketing material to such person without a separate legal basis.

2.3. Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff Members may only process personal data when and to the extent the performance of their job duties requires it. They cannot process personal data for any reason unrelated to their particular job duties.

Staff Members may only collect personal data that they require for their job duties and business operations of the Company. Collecting excessive personal data is strictly prohibited. The Company and its Staff shall ensure any personal data collected is adequate and relevant for the intended purposes.

The Company and its Staff must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised.

The Company and its Staff must make sure that the Company does not collect excessive personal data.

For instance, if personal data is collected in order to conclude an agreement, the Company and its Staff shall not collect irrelevant, excessive personal data, e.g., photo, unless the other purpose requires to do so and there is a proper legal ground.

If Staff Members have any doubts about the necessity of particular personal data for the intended purpose, they must immediately address them to the Responsible Person or line manager.

2.4. Data Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccuracies are discovered.

The Company must ensure that the personal data it uses and holds is accurate, complete, kept up to date and relevant to the purpose for which the Company collected it.

The Company must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Also, the Company must take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Staff Members shall comply with the guidelines on data accuracy established in Section 6.4 of this Data Protection Policy.

If Staff Members believe that some of the personal data may be inaccurate (e.g., wrong email or address), they shall take all legitimate means to correct such personal data or confirm its accuracy. Also, they shall check the accuracy of any personal data as described above. Inaccurate personal data shall be destroyed or corrected immediately.

2.5. Storage Limitation

Personal data must not be kept for longer than is necessary for the purposes for which the personal data is processed.

The Company shall ensure that personal data is deleted after a reasonable time when its necessity for respective purposes expires, unless the Laws requires that personal data to be kept for a longer period, such as the Index of Retention Periods of General Documents of approved by the order No V-100 of the Chief Archivist of Lithuania on 9 March 2011.

The Company must not keep personal data in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which the Company originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Company shall take all reasonable steps to destroy or erase from its systems and all mediums all personal data that it no longer requires in accordance with the Data Protection Policy and Laws. This includes requiring third parties to delete that personal data where applicable.

The Company when acting as a data controller shall also ensure data subjects are informed of the period for which personal data is stored.

Staff Members shall strictly comply with the abovementioned requirements. While the Company takes all measures to ensure the full automatization of personal data deletion, Staff Members shall also be responsible for monitoring and deletion of personal data in accordance with the abovementioned standards, especially where the automatization is not possible.

All related doubts shall be immediately addressed to the Responsible Person or line manager.

2.6. Integrity and Confidentiality

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

The Company shall develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). Requirements for Staff Members related to such safeguards are further listed in Section 6 of this Data Protection Policy.

The Company shall regularly evaluate and test the effectiveness of those safeguards to ensure security of its processing.

The Company may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place as requested.

The Company shall maintain the security of personal data by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people on a need-to-know principle are authorised to use the personal data and can access it,
- **Integrity** means that personal data is accurate and suitable for the purpose for which it is processed, and
- **Availability** means that authorised users should be able to access the personal data when they need it for authorised purposes.

Staff Members must comply with the data protection documents of the Company and not attempt to circumvent the administrative, physical and technical safeguards the Company implements and maintains in accordance with the GDPR and relevant standards to protect personal data.

Staff Members must comply with the safeguards listed in Section 6 of this Data Protection Policy.

3. Data Processors

The Company may authorise data processors – providers of technological and electronic communication services, advisers, auditors, consultants and other individuals that process personal data in the possession of the Company for the purposes identified by the Company and in line with its instructions – to process the personal data that the Company controls.

If the Company authorizes a data processor to process the personal data, the Company shall select the processor that will guarantee the required technical and organisational data protection measures and ensure that such measures will be enforced.

The Company and data processors shall always enter into written contracts (data processing agreements) that stipulate that data processors shall only process the personal data on the basis of instructions from the Company. Such contracts shall include all requirements imposed by the GDPR and the Laws.

Staff Members must ensure that the data processors are in compliance with the above requirements prior to the processing. All related doubts shall be immediately addressed to the Responsible Person or line manager.

4. Rights of Data Subjects

Data subjects have the following rights:

- right of access (*Article 15 of the GDPR*),
- right to rectification of personal data (*Article 16 of the GDPR*),
- right to erasure of personal data ("*right to be forgotten*") (*Article 17 of the GDPR*),
- right to restriction of processing (*Article 18 of the GDPR*),
- right to data portability (*Article 20 of the GDPR*),
- right to object to processing (*Article 21 of the GDPR*),
- right to lodge a complaint with a supervisory authority (*Article 77 of the GDPR*).

When the Company acts as a data controller, the Company will be responsible for compliance with the data subject rights.

4.1. Right to Access

The right to access encompasses two different aspects. First, upon a request, confirmation shall be given to data subject that the personal data relating to him or her is being processed. Second, access to the following information shall be granted:

- the purposes of processing,
- the categories of personal data concerned,
- the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organizations,
- the period for which the personal data will be stored or, if that is not possible, the criteria used to determine that period,
- the existence of the right to request access to and rectification or erasure or restriction of processing or a right to object to processing as well as the right to data portability,
- the existence of a right to lodge a complaint with a Supervisory Authority,
- where the personal data is not collected from the data subject, any available information as to its source,
- the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject (if necessary).

Where personal data is transferred to a third country or to an international organization, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

Upon a request of the data subject the Company shall provide him/her with a copy of the personal data undergoing the processing free of charge and in compliance with the rights of third parties. The provision of copies should not, for example, breach any business confidentiality or intellectual property rights (e.g., copyright, trademarks).

Should the data subject want several copies, a reasonable fee may be charged for this based on administrative costs. Where the request is made by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4.2. Right to Rectification of Personal Data

At the request of the data subject, inaccurate personal data must be rectified immediately, and incomplete personal data shall be supplemented.

All recipients of personal data that has been rectified shall be informed of the rectification unless this is impossible or can only be carried out at disproportionate expense. At the request of the data subject, he/she shall be informed of the recipients.

4.3. Right to Erasure of Personal Data ("*Right to be Forgotten*")

At the request of the data subject, personal data relating to him/her shall be erased immediately where one of the following grounds applies:

- personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed,
- data subject withdraws consent on which the processing was based and where there is no other legal ground for the processing,
- data subject objects to the processing and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing for the purposes of direct marketing,
- personal data has been unlawfully processed,
- personal data must be erased for compliance with a legal obligation in Laws,
- personal data has been collected in relation to services offered by the information society (consent of a child).

All recipients of the personal data that has been erased shall be informed of the erasure unless this is impossible or can only be carried out at disproportionate expense. At the request of the data subject, he/she shall be informed of the recipients.

If the personal data to be erased has been published, the other data controllers who process the personal data shall be informed that the data subject has requested erasure of all links to the personal data to be erased or of copies or replications of the personal data.

The duty of erasure does not apply where the processing is necessary in the following cases:

- for exercise of the right of freedom of expression and information,
- for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company,
- for reasons of public interest in the area of public health,
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing, or
- for the establishment, exercise or defence of legal claims.

4.4. Right to Restriction of Processing

The data subject is entitled to demand the restriction of processing of their personal data. Restriction is the marking of stored personal data with the aim of restricting the future processing thereof.

Processing must be restricted if one of the following conditions has been met:

- accuracy is contested by the data subject (for a period enabling the accuracy of the personal data to be checked),
- processing is unlawful, but the data subject opposes the erasure of the personal data and requests the restriction of its use instead,
- personal data is no longer needed for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims,
- the data subject has objected to the processing (for a period pending verification of whether the legitimate grounds of the Company override those of the data subject).

If processing has been restricted, then this personal data (apart from the storage thereof) may only be processed with the consent of the data subject or for the establishment, exercise or defence of legal claims or for protection of the rights of another natural person or legal entity or for reasons of important public interest.

If the restriction is lifted, the data subject shall be informed thereof beforehand.

All recipients of the personal data that are subject to the restriction shall be informed of the restriction of processing unless this is impossible or can only be carried out at disproportionate expense. At the request of the data subject, he/she shall be informed of the recipients.

4.5. Right to Data Portability

Where the processing is based on contract or consent and carried out using automated means, at the request of the data subject, the personal data concerning them and provided by them shall be transmitted to them in a structured, commonly used and machine-readable format.

If the data subject requests, the personal data mentioned shall be transmitted to another data controller. This right shall not adversely affect the rights and freedoms of others.

4.6. Right to Object

The data subject shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data which is based on one of the following grounds:

- for processing carried out in the public interest or in the exercise of official authority or
- processing in the legitimate interest of the Company or of a third party without overriding interests of the data subject worthy of protection.

Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

4.7. Exercising the Rights of Data Subjects

The Company must exercise these rights within 1 month. If the request is very complex or the number of received requests is very high, this term may be extended for 2 months. In this case, the Company shall notify data subjects about this extension and reasons for it within 1 month of the receipt of request.

In order to ensure personal data protection and properly exercise rights of data subjects, the Company is entitled to ask data subjects to provide proof of their identity if the Company cannot identify the person making the request.

The Company is not entitled to ask for excessive information in this case, e.g., copy of ID card/passport may be asked only in highly exceptional and justifiable cases, for instance, if data subject asks for information about his/her special category data.

Staff Members must immediately forward all requests from data subjects concerning the abovementioned rights to it@bullionz.com.

5. Data Transfers

Generally, the Company is not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place, and unless the data subject has been made aware of such sharing in advance, in particular in accordance with this Data Protection Policy.

Generally, Staff Members may only share the personal data the Company holds with another Staff Member, if he or she has a job-related need to know the information.

The Company may also share the personal data it holds with third parties, such as service providers, if the following conditions are met:

- they have a need to know the information for the purposes of providing the contracted services,
- sharing the personal data complies with the information provided to the data subject and, if required, the consent has been obtained,
- the third party (data processor) has agreed to comply with the required personal data security standards, policies and procedures and put adequate security measures in place,
- the transfer complies with any applicable cross border transfer restrictions; and
- a fully executed written contract that contains GDPR approved third party clauses has been obtained (for processing relationships only).

A transfer of personal data to a third country (outside the EEA) or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection (*adequacy decision*).

In the absence of an adequacy decision, the Company may transfer personal data to a third country or an international organisation only if the appropriate safeguards are provided, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. This should be assessed on a case-by-case basis in the absence of adequacy decision. **All and any transfers of personal data to third countries without an adequacy decision may only take place after prior consultation with your line manager.**

Furthermore, in the absence of an adequacy decision, for transfers without requiring any specific authorisation from a supervisory authority, one of the following tools shall be employed:

- binding corporate rules in accordance with Article 47 of the GDPR,
- standard data protection clauses adopted by the European Commission pursuant to the procedure indicated in the GDPR,
- standard personal data protection clauses adopted by the Supervisory Authority and approved by the European Commission pursuant to the procedure indicated in the GDPR,

- an approved code of conduct pursuant to Article 40 of the GDPR together with binding and enforceable commitments of the data controller or data processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights,
- an approved certification mechanism pursuant to Article 42 of the GDPR together with binding and enforceable commitments of the data controller or data processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

In special cases the Company may also rely on derogations established in Article 49 of the GDPR, however, they may not be used for regular and systematic transfers of personal data.

Staff Members must make sure that the above conditions are met prior to personal data transfers.

If Staff Members have any doubts about the implementation of the above guidance, they must address them to the Responsible Person or line manager.

6. Technical and Organizational Data Protection Measures

The Company strives to ensure the security of personal data. Thus, all Staff Members shall follow the guidelines established in the following Sections of this Data Protection Policy.

6.1. General Staff Guidelines

Each Staff Member must comply with the following requirements:

- the only people able to access personal data controller by the Company should be those who need it for their work,
- data should not be shared informally. When access to confidential information is required, Staff Members can request it from their line managers,
- Staff Members should keep all data secure, by taking sensible precautions and following the guidelines set forth 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,
- Staff Members should request help from their line manager or the Responsible Person if they are unsure about any aspect of data protection.

6.2. Guidelines on Data Storage

This Section describes how and where data should be safely stored. Questions about storing data safely can be directed to the Responsible Person.

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,

- Staff Members 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 standard backup procedures of the Company,
- 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.

6.3. Guidelines on Data Use

When personal data is accessed and used it can be at the greatest risk of loss, corruption, or theft:

- when working with personal data, Staff Members should ensure the screens of their computers are always locked when left unattended,
- personal data should not be shared informally. In particular, it should never be sent by email, as this form of communication is not secure,
- data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorized external contacts,
- personal data should never be transferred outside of the EEA, except where and to the extent permitted by this Data Protection Policy,
- Staff Members should not save copies of personal data to their own computers. Always access and update the central copy of any data.

6.4. Guidelines on Data Accuracy

As discussed in Section 2.4, data accuracy is one of key principles on data protection. It is the responsibility of all Staff Members who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible:

- data must 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 customer's details when they call him/her,

- the Company will make it easy for data subjects to update the information the Company holds about them. For instance, via the website,
- data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached via his/her 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 6 months.

7. Personal Data Breaches

The GDPR requires the Company to notify personal data breaches to the Supervisory Authority and, in certain instances, the data subject. For example, any of the following could result in a personal data breach for the Company:

- suffering a computer system hack or phishing attack,
- emailing personal information to the wrong recipient,
- the loss or theft of a device or records containing personal data.

The Company will deal with any suspected personal data breach and will notify data subjects or the Supervisory Authority where we are legally required to do so.

7.1. Identification of Personal Data Beaches

Personal data breach, generally, may involve such incidents:

- **destruction** - this is where the personal data no longer exists, or no longer exists in a form that is of any use to the Company,
- **damage** - this is where personal data has been altered, corrupted, or is no longer complete,
- **loss** - this should be interpreted as the personal data may still exist, but the Company has lost control or access to it, or no longer has it in its possession,
- **unauthorised or unlawful processing** – this may include disclosure of the personal data (or access by) to recipients who are not authorised to receive (or access) the personal data, or any other form of processing which violates the GDPR.

In practice personal data breaches may include, but are not limited to the following:

- access by an unauthorised party,
- deliberate or accidental action (or inaction) by partner or third party,
- sending personal data to an incorrect recipient,
- computing devices containing personal data being lost or stolen,
- personal data becoming lost, destroyed, corrupted or disclosed,
- alteration of personal data without permission,
- loss of availability of personal data (e.g., encrypted by ransomware).

Personal data breaches are categorised according to the following 3 information security principles:

- "**Confidentiality personal data breach**" - an unauthorised or accidental disclosure of, or access to, personal data,
- "**Integrity personal data breach**" - unauthorised or accidental alteration of personal data,
- "**Availability personal data breach**" - accidental or unauthorised loss of access to, or destruction of, personal data.

Depending on the circumstances, a personal data breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

Whereas determining if there has been a personal data breach of confidentiality or integrity is relatively clear, an availability personal data breach may be less obvious. A personal data breach will always be regarded as an availability personal data breach when there has been a permanent loss of, or destruction of, personal data.

Upon discovery of a (potential) personal data breach, the Staff Member shall immediately inform the Responsible Person via email (it@bullionz.com) about such personal data breach and provide all information known to him/her which may affect the investigation of the personal data breach.

The fact that the Staff Member does not know some of the information about the personal data breach is not a justifiable reason for the delayed notification to the Company. In this case, the Staff Member must immediately inform the Responsible Person of the fact itself and provide the missing information at a later stage upon the request from the Responsible Person.

When the information about a personal data breach is found out outside of operational functions (for example, information about the personal data breach appears in the press), Staff Member shall also notify the Responsible Person of such information received.

If Staff Members have any doubts on whether a particular incident is actually a personal data breach, they shall contact the Responsible Person immediately and provide all available information which may be useful for identification purposes.

Quick reaction is a key - the sooner you notify the Company of the personal data breach, the sooner we will be able to protect the rights of data subjects and properly fulfil our obligations. **Therefore, the fact of the personal data breach itself must be communicated to the Company immediately, but in any case, no later than within 2 hours upon acknowledgment of such personal data breach.** Please note that this deadline also applies in cases where the personal data breach is acknowledged on the weekend, public holidays, or less than 2 hours before the end of working hours.

This is very important since the Company has only 72 hours to inform the Supervisory Authority about the personal data breach. You should preserve all evidence relating to the potential personal data breach.

7.2. Risk Assessment

There is a duty without undue delay and where feasible, to report a personal data breach not later than 72 hours after having become aware of it, notify the Supervisory Authority. An assessment will also need to be made as to whether to notify the data subjects concerned, and when required, notify them without undue delay (Article 34 of the GDPR). Not all personal data breaches have to be reported.

Upon receipt of information personal data breach, the responsible person needs to establish the likelihood and severity of the resulting risk to people's rights and freedoms in order to determine if the personal data breach has to be reported to the data subjects and/or Supervisory Authority.

- if there are likely consequences to individuals → the personal data breach must be reported to the Supervisory Authority,
- when the personal data breach is likely to result in a high risk to the rights and freedoms of individuals → the personal data breach must be reported to both the Supervisory Authority and data subjects.

Notification of the personal data breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a personal data breach to data subjects is where it is likely to result in a high risk to the rights and freedoms of individuals. This risk exists when the personal data breach may lead to physical, material or non-material damage for the individuals whose personal data have been breached, e.g., discrimination, identity theft or fraud, financial loss, damage to reputation and others.

When the personal data breach involves special category data, such damage should be considered likely to occur.

The risks shall be also assessed by taking into account the following criteria:

- **type of personal data breach**. This criterion is described in Section 6.1 of this Data Protection Policy and it may affect the level of risk presented to individuals.
- **nature, sensitivity, and volume of personal data**. Usually, the more sensitive the personal data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. Also, a combination of personal data is typically more sensitive than a single piece of personal data.
- **ease of identification of individuals**. An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals or match the personal data with other information to identify individuals.
- **severity of consequences for individuals**. Depending on the nature of the personal data involved in a personal data breach, for example, special category data, the potential damage to individuals that could result can be especially severe, in particular where the personal data breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation.
- **special characteristics of the individual**. A personal data breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the personal data breach on them.
- **special characteristics of the Company**. The nature and role of the Company and its activities may affect the level of risk to individuals as a result of a personal data breach.
- **number of affected individuals**. Generally, the higher the number of individuals affected, the greater the impact of a personal data breach can have.

The notification to the data subject is not required if any of the following conditions are met:

- the Company has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption,
- the Company has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise,
- it would involve disproportionate effort (provided there is a public communication or similar measure).

7.3. Notification

Once the Responsible Person made the assessment and concluded that the personal data breach must reported to the data subjects and/or Supervisory Authority, he/she shall:

Reporting to the Supervisory Authority	The Responsible Person shall fill in the personal data breach form provided by the Supervisory Authority. The form can be accessed here: https://www.ada.lt/go.php/lit/Pranesimas-apie-duomenu-saugumo-pazeidima-bdar/4/1. The Company shall report a personal data breach to the Supervisory Authority without undue delay and where feasible, not later than 72 hours after having become aware of it. The Company should be regarded as having become "aware" when the Company has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. Where the notification to the Supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay. Depending on the circumstances of the personal data breach, the Company shall consider the necessity to notify other state or municipal institutions and/or other public bodies.
Reporting to the data subjects	Data subjects should be informed of the personal data breach directly, for example by sending them a notification by e mail, mail, SMS, etc. This notification should be separated from other information sent, such as regular updates. Where direct notification to the data subject would require a disproportionate effort, the notification may instead be made public or by similar measures whereby the data subjects are informed in an equally effective manner, such as prominent website banners or notification and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective mean of communicating a personal data breach to an individual. The Company should choose the means that maximize the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean that the Company shall employ several methods of communication, as opposed to using a single contact channel. At least the following information shall be provided to data subjects: ■ the name and contact details of the responsible person, ■ the likely consequences of the personal data breach, ■ the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.4. Registry of Personal Data Breaches

All personal data breaches, whether reported to the Supervisory Authority/data subjects or not, should be recorded. Based on the information provided in the personal data breach registry, the Supervisory Authority must be able to verify the implementation of the obligation to report personal data breaches. The personal data breach registry shall include facts relating to the personal data breach, its effects and the remedial action taken.

Information on personal data breach should be entered in the personal data breach registry as soon as the personal data breach is identified and the risks – assessed. If necessary, the information in the personal data breach log should be supplemented and/or corrected later on.

The Responsible Person shall be responsible for filing and keeping up to date the personal data breach registry. The personal data breach registry shall be filled and stored in electronic format.

8. Privacy by Design and Data Protection Impact Assessment (DPIA)

8.1. Privacy by Design

The Company is required to implement Privacy by Design measures by implementing appropriate technical and organisational measures in an effective manner, to ensure compliance with personal data privacy principles.

The Company must assess what Privacy by Design measures can be implemented on all programmes, systems or processes that process personal data by taking into account the following:

- the state of the art,
- the cost of implementation,
- the nature, scope, context and purposes of processing, and
- the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

Please see Section 6 to learn more about data security measures mandatory at the Company.

8.2. DPIA

DPIA is a way for the Company when acting as a data controller to systematically and comprehensively analyse personal data processing and help to identify and minimise personal data protection risks. While performing DPIA focus should be not only on compliance risks, but also on broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The Company should evaluate potential harm – to individuals or to society at large, whether it is physical, material or non-material. DPIA does not have to indicate that all risks have been eradicated. But it should help the Company to document them and assess whether or not any remaining risks are justified.

Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data. DPIA should begin early in the life of a project, before the Company starts the processing, and run alongside the planning and development process.

DPIA shall be required in the case of:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person,
- processing on a large scale of special category data or of personal data relating to criminal convictions and offences referred to in Article 10 of the GDPR, or
- a systematic monitoring of a publicly accessible area on a large scale.

DPIA shall also be performed at least in the following cases (a specific list is published by Supervisory Authority alongside with its recommendations, therefore in case of any concerns please refer to the Company):

- processing of personal data for the purposes of scientific or historical research: (1) where special category data is processed without the consent of the data subject or where the processing is carried out by linking or combining personal data sets; (2) when processing personal data of minors; (3) when processing a personal code,

- processing of personal data is carried out on a large scale where the personal data is received indirectly and the provision of information is in some cases impossible or would require a disproportionate effort, or where such provision of information may make it impossible or significantly impede the purposes of the processing,
- processing of personal data where it is not possible or would require a disproportionate effort to inform the recipients to whom the personal data has been disclosed of the rectification, erasure or restriction of the processing,
- processing of biometric personal data for the specific purpose of identifying a natural person for the purposes of monitoring or controlling natural persons or when processing personal data relating to vulnerable persons,
- processing of genetic data for personal assessment or scoring, including profiling and forecasting,
- processing of video data when video surveillance is carried out in premises and/or territories that are not owned by the Company or on other lawful grounds; in health care, social care, prisons and other institutions where services are provided to vulnerable persons; together with sound recording,
- phone call recording,
- processing of personal data using innovative technologies or a new way of using existing technologies to process personal data of vulnerable data subjects,
- processing of children's personal data for direct marketing purposes, assessment of children's personal aspects based on automated processing, including profiling, or where information society services are offered directly to children,
- processing of personal data of employees for monitoring or control purposes: processing of video and/or audio data of such persons at the workplace and/or at the premises or areas of the Company where its employees work; processing of personal data relating to the monitoring of employees, communication, behaviour, location or movement.

DPIA must include:

- a description of the processing, its purposes and the legitimate interests pursued by the Company, if appropriate,
- an assessment of the necessity and proportionality of the processing in relation to its purpose,
- an assessment of the risk to individuals, and
- the risk mitigation measures in place and demonstration of compliance.

Where appropriate, the Company shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

DPIA shall be carried out in accordance with the Laws, recommendations of the Supervisory Authority and Working Party of Directive 95/46/EC, and other relevant and up-to-date documents adopted by competent authorities.

DPIAs are carried out jointly by the Responsible Person and Staff Members of the team introducing the new processing activity. If intended processing activities correspond to the above criteria, they must be immediately addressed to the Responsible Person.

9. Training and Audit

The Company is required to ensure that all Staff Members have undergone adequate training to enable them to comply with the Laws. The Company must also regularly test its systems and processes to assess compliance.

Staff Members must undergo privacy-related training.

Staff Members must regularly review all the systems and processes under their control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of personal data.

The Company carries out Staff Members' trainings before they start handling personal data and on a regular basis later on (at least once per year).

However, if Staff Member believes that his/her data privacy related training is insufficient or he/she needs any information or clarifications related to processing, he/she shall immediately contact his/her line manager and address such concerns.

10. Responsibilities

Everyone who works for or with the Company 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 Data Protection Policy and data protection principles.

However, these people have key areas of responsibility:

- the **board of directors** is ultimately responsible for ensuring that the Company 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 Data Protection Policy,
  - dealing with requests from individuals to access the data the Company holds about them,
  - checking and approving any contracts or agreements with third parties that may handle the sensitive data of the Company.
- the **IT manager officer** 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 Member to ensure marketing initiatives abide by data protection principles.

11. Changes to this Data Protection Policy

The Company reserves the right to change this Data Protection Policy at any time, in cases of amendments to any legal acts regulating the processing of personal data.

This Data Protection Policy shall be reviewed at least once per year to verify its accuracy and compliance.

This Data Protection Policy does not override any applicable Laws and regulations.