Last updated: 23th September 2025

Privacy Policy

Welcome to the Privacy Policy (the "**Policy**").

The Website and Mobile Application are owned by the company Vault Fintech Solutions s.r.o., a company incorporated in Czech Republic with the company number 21627002, and a registered office at Frydlantská 1312/19, Kobylisy, 182 00 Praha 8, Czech Republic **("Vault")**.

Vault Fintech Solutions s.r.o., a legal entity duly registered in Czech Republic with No. 216 27 002 with a registered office at Frydlantská 1312/19, Kobylisy, 182 00 Praha 8, Czech Republic. (the "**Vault**")..

As a high-level summary, we are an evolving cryptocurrency-focused financial institution providing various cryptocurrency-related financial services (the "**Services**"). We provide all this employing the website https://vault.ist (the "**Website**") and the related mobile application and crypto-platforms that we may operate from time to time (each of which, is a "**Platform**") and which may be accessible via the Website or otherwise.

Accordingly, the purpose of this Policy is to set out the basis on which we will process your data when you:

1. visit and use a Website and/or Platform, regardless of where you visit or use them from;

2. apply for and register a customer account with us (your "**Account**");

3. apply for, receive, pay, and/or use any of our Services.

This also includes any data that you may provide to us for our events, newsletters, and other marketing items.

This Policy informs you about the items of Personal data that we may collect about you and how we will handle it, and in turn, also tells you about

(i) our obligations to process your data responsibly,

(ii) your data protection rights as a data subject, and (iii) how the law protects you. It should be read in conjunction with our Cookie Policy.

Please read the following information carefully to understand our practices regarding your data.

1. Important information and who we are

General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) regulations shall be implemented for EU users (the "**Regulation**" or the "**GDPR**").

This Policy aims to ensure that you are fully informed on how we will collect and process your Personal data in the circumstances and scenarios outlined in the **'Introduction'** (namely, through your token subscriptions and purchases, your use of the Website, and any of the related Services).

The Websites, the Platform, and the Services are not intended or in any way made available for minors, and we do not knowingly collect data relating to minors.

You must read this Policy together with any other privacy or fair processing notice we may provide on specific occasions when we are collecting or processing Personal data about you so that you are fully aware of how and why we are using your data. This Policy supplements the other notices and is not intended to override them.

The opening and registration of a customer account will give rise to the existence of a contractual relationship with us, as regulated by our Terms of Use, and all matters between you and us relating to Services will be deemed to fall within the subject matter of that same contractual relationship. Furthermore, the existence of this contract between you and us will also serve as the legal basis for a number of our processing activities involving your Personal data, as detailed below.

Controllers

Vault Fintech Solutions s.r.o. (as defined) above is the controller and is responsible for your Personal data. There may be other controllers of your Personal data, such as, for example, electronic identification verification service providers, or other service providers engaged by us for purposes of processing and storing your Personal data. They will be so-called "joint controllers" of your Personal data and as such, will share responsibility for such control with us.

Provider	Purpose	Privacy Policy
Vero	Email communications and marketing automation	https://www.getvero.com/privacy/
Fireblocks	Secure custody and transaction management of digital assets	https://www.fireblocks.com/privacy-policy/
Zendesk	Customer support ticketing system and live chat	https://www.zendesk.com/company/agreements-and-terms/privacy-policy/
Amazon Web Services (AWS)	Cloud infrastructure and hosting services	https://aws.amazon.com/privacy/
GitHub	Code hosting and software deployment infrastructure	https://docs.github.com/en/site-policy/privacy-policies/github-privacy-statement

SumSub	Identity verification and KYC/AML screening	https://sumsub.com/privacy-notice/
Reap Technologies Limited	Payment processing and account management	https://reap.global/privacy-policy

By agreeing to this Privacy Policy, you consent to the transfer of your personal data to Reap Technologies Limited and for the purposes outlined above. We ensure that such transfers are conducted in compliance with applicable data protection laws and regulations and that adequate safeguards are in place to protect your personal data.

Please familiarize yourself with these providers and their privacy and liability policies. If you find any of these may not work for you, please do not access any of the Websites and do not use any of our Services.

As a general rule, we always seek to minimize the amount of your Personal data that we collect and store.

Contact details

Full name of legal entity: Vault Fintech Solutions s.r.o.

Email address: privacy@vault.ist

Please use the words 'Data Protection Matter' in the subject line.

Changes to the Policy and your duty to inform us of changes

It is imperative that the Personal data we hold about you is accurate and current at all times. Otherwise, this will impair our ability to process your token purchases and/or our ability to provide you with the Services that you may request from us (amongst other salient issues).

Please keep us informed if any of your Personal data changes during your relationship with us.

Third-party links

Our Website may include links to third-party websites, plug-ins, and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these third-party websites and are not responsible for their privacy notice or policies. We strongly encourage you to read the privacy notice of every website you visit, particularly when leaving our Website.

2. Glossary

Set out below are key definitions of certain data protection terms that appear in this Policy.

"**Consent Form**" refers to separate documents that we might from time to time provide you where we ask for your explicit consent for any processing that is not for purposes set out in this Policy.

"**Data subjects**" means living individuals (i.e. **natural persons**) about whom we collect and process Personal data.

"**Data controller**" or "**controller**" means any entity or individual who determines the purposes for which, and how, any Personal data is processed.

"**Data processor**" or "**processor**" means any entity or individual that processes data on our behalf and on our instructions (we being the data controller).

"**Personal data**" means data relating to a living individual (i.e. **natural person**) who can be identified from the data (information) we hold or possess. This includes but is not limited to, your name and surname (including maiden name where applicable), address, date of birth, nationality, gender, civil status, tax status, identity card number & passport number, contact details (including mobile and home phone number and personal email address), photographic image, bank account details, emergency contact information as well as online identifiers. The term "**personal information**", where and when used in this Policy, shall have taken the same meaning as Personal data.

"**Processing**" means any activity that involves the use of Personal data. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal data to third parties.

"**Sensitive Personal data**", "**sensitive data**" or "**special categories of Personal data**" includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offense committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. This type of sensitive data can only be processed under strict conditions.

Note that Personal data does not include information relating to a legal person (such as for example, a company). Therefore, information such as a company name, its company number, registered address, and VAT number, does not amount to Personal data in terms of both the Act and the GDPR. Naturally, we will still treat any such information confidentially and securely.

3. The data we collect about you

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (**anonymous data**).

We may collect, use, store, share, and disclose different kinds of Personal data about you which (**for purely indicative purposes**) we have grouped as follows. For the avoidance of doubt, categories marked in blue do not apply to non-customers (i.e. individuals who do not hold a registered customer account with us).

- **Identity Data** includes your first name, maiden name (where applicable), last name, username or similar identifier, marital status, title, nationality, date of birth, gender, identity card, and/or passport number.

- **Contact Data** includes address, billing address, email address, and contact number (telephone and/or mobile).

- **AML and KYC Data** includes the following due diligence documentation and information on you:

(i) copy of your national identity document, passport, and/or driver's license, (ii) proof of residence (for example, a recently issued utility bill), (iii) a 'selfie' (for identity verification), (iv) KYC database checks, (v) fraud database checks and (vi) any documentation or information which we may be from time to time:

1. required to collect to ensure compliance with any applicable legislation

(including applicable foreign laws) and global AML/KYC practices; and/or

2. otherwise mandated to collect by any competent authority, including, as applicable, any other documentation or information which may be mandated on us from time to time by applicable law and by any other competent authority or related legislation (including overseas authorities and applicable foreign laws).

- **Enhanced KYC Data** applies with respect to payments that exceed a set threshold and includes, at a minimum, the following enhanced customer due diligence documentation and information: source of funds and source of wealth.

- **Financial Data** includes your wallet and private key details.

- **Transaction Data** includes details about:

    1. your subscriptions, purchases, and transactional activity;

    2. your transactional history on the Platform;

    3. your use of the Services (including your service requests);

    4. the payments made to and from you.

- **Portfolio Data** includes details about the tokens credited to your account.

- **Usage Data** includes details about how you use our Platform and the Websites.

- **Technical Data** includes internet protocol (IP) address, 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 which you (whether a client or otherwise) use to access and browse the Websites.

- **Website Visit Data** includes the full Uniform Resource Locators (URL), clickstream to, through, and from the Website (including date and time), products you viewed or searched for, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), methods used to browse away from the page.

- **Marketing and Communications Data** includes your preferences in receiving marketing from us or our third parties and your communication preferences. This may include information on whether you have subscribed or unsubscribed from any of our mailing lists, attended any of our events, or accepted any of our invitations.

We will also collect, use, and process any other information that you voluntarily choose to provide or disclose to us where relevant for processing your token requests and/or providing you with your requested Services. Any such information that we receive from you would fall under the '**Transaction Data**' category.

We also collect, use, and share Aggregated Data such as statistical or demographic data for any purpose. Aggregated Data may be derived from your Personal data but is not considered Personal data in law as this data does not directly or indirectly reveal your identity. For example, we may aggregate your Website Visit Data to calculate the percentage of users accessing a specific feature of the Website. However, if we combine or connect Aggregated Data with your Personal data so that it can directly or indirectly identify you, we treat the combined data as Personal data which will be used following this Policy.

If you fail to provide Personal data

Where we need to collect Personal data about you:

- by law, or

- under the terms of, or in connection with, the contract that we have with you (as discussed above); or

- as part of our legitimate (business) interests to verify the identity of our applicants and customers, mitigate against risks (such as potential or suspected fraud), and, in particular, assess and take a decision on whether we want to enter into a customer relationship with you (as subject to our customer acceptance criteria and policies),

and you either fail to provide that data when requested, or else provide incomplete or insufficient data, we may not be able to perform or conclude the contract that we have or are otherwise trying to enter into with you (namely regarding your account opening, token subscriptions and purchases, and provision of the Services).

In certain cases, particularly where it relates to KYC due diligence data (both standard and enhanced), we may even need to exercise our prerogative to terminate our contract with you following the terms thereof, or else, if still at the application stage, we may have to decline to enter into a customer relationship with you.

We will however notify you if this is the case at the time.

Special categories of Personal data

We do not knowingly collect Special Categories of Personal data (or Sensitive Personal data) about you. Should we receive sensitive Personal data about you, we will only process that data when there is a legitimate basis to do so and, in all circumstances, in accordance with our obligations at law and under the appropriate safeguards.

As set out below in **Section 5**, we collect and process **AML** and **KYC Data** and, if applicable, **Enhanced KYC Data** in order to (i) conduct our AML and KYC checks, and other due diligence checks, on you, (ii) verify your identity or claimed identity and, in those instance of enhanced due diligence, your source of funds and source of wealth, (iii) take an informed decision on whether we want to enter into a customer relationship with you, and, if positive, to conduct initial and ongoing screening and monitoring and (iv) to comply with any legal or regulatory obligation that we may have and/or any Court, regulatory or enforcement order that may be issued upon us.

4. How is your Personal data collected?

We generally use different methods to collect data from and about you including through:

Account Registration. We will ask you to provide us with your Identity, Contact AML, and Risk Data when you apply to open a customer account with us. You provide this information, which will then be collected and processed when you fill in and submit your account application form (together with other related forms) and complete the required application steps.

Direct Interactions. You may give us your Identity, Contact AML and Risk Data, Enhanced KYC Data, and Marketing and Communications Data by filling in our forms (such as our 'Contact Form') or by corresponding with us by post, phone, email, or otherwise. This includes Personal data you provide when you:

- contact us in the context of opening and registering a customer account;
- apply to open a customer account;
- subscribe to, purchase, and/or use our Services;
- discuss with us the particular Services that you require;
- request and receive our Services;
- contact us with complaints or queries;
- complete an inquiry form;
- contact us for further information about our products and services;
- submit the AML and KYC Data and/or Enhanced KYC Data that we request;

- request marketing to be sent to you;
- express interest and/or attend any of our seminars or other hosted events;
- participate in a survey or our webinars;
- subscribe to our newsletters;
- give us some feedback.

Through our provision of the Services. This may encompass all of the data categories listed in Clause 3 (namely, Identity, Contact, AML and Risk Data, Enhanced KYC Data, and Transaction Data).

Automated technologies or interactions. When you interact with our Website, we may automatically collect Technical and Usage Data about your equipment, browsing actions, and patterns. We may collect this Personal data by using cookies, server logs, and other similar technologies.

Please see our Cookie Policy for further details.

Third parties or publicly available sources. We may receive Personal data about you from various third parties and public sources as set out below:

Technical Data from the following parties:

(a) analytics providers;

(b) advertising networks; and

(c) search information providers.

Identity, Contact, AML, and Risk Data and Enhanced KYC Data from publicly available sources such as public court documents, the RoC, and the company houses and registers of other jurisdictions, and from electronic data searches, online KYC search tools (which may be subscription or license-based), anti-fraud databases and other third party databases, sanctions lists, outsourced third-party KYC providers and from general searches carried out via online search engines (e.g. Google).

We may also receive customer due diligence reports about our applicants from our outsourced third-party KYC provider. These reports may encompass identity checks, document integrity checks, checks against global sanctions lists, and related screening and monitoring measures. In such cases, this third-party provider will conduct the requested customer due diligence checks **autonomously** and will generally amount to a controller of the Personal data that it collects in connection with those checks. It also has its data policies and practices, which will be duly notified and communicated to the applicant.

5. How we use your Personal data

We will only use your Personal data when the law allows us to. Most commonly, we will use your Personal data in the following circumstances:

Where you wish to enter into a customer relationship with us.

Where we need to perform the contract we have or which are about to enter into with you as a customer (including in respect of your token purchases and subscriptions, and use of the Services).

Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.

Where we need to comply with a legal or regulatory obligation.

You have the right to withdraw consent to such marketing at any time by contacting us, as indicated above under '**Contact Details**'.

6. Purposes for which we will use your Personal data

We have set out below, in a table format, a description of all the ways we plan to use your Personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate.

Note that we may process your Personal data according to more than one lawful ground or basis, depending on the specific purpose for which we are using your data. Please contact us at privacy@vault.ist if you need details about the specific lawful basis we are relying on to process your Personal data where more than one lawful basis has been set out in the table below.

Purpose/Activity	**Type of data**	**Lawful basis for processing including basis of legitimate interest**
(a) To conduct customer due diligence measures on you (following your application to enter into a customer relationship with us). (b) To determine whether we want to enter into a customer relationship with you and, if positive, to register your customer account and onboard you as a customer.	(a) Identity; (b) Contact; (c) AML and KYC.	(a) Performance of a contract with you or to take steps at your request before entering into such a contract. (b) Necessary for our legitimate interests (to verify your identity, conduct initial screening and monitoring (sanctions lists, fraud databases, and other KYC checks), determine whether you present any risks as a prospective customer, and ultimately enable us to take an informed decision on whether we want to enter into a customer relationship with you).
(a) To establish and verify your identity. (b) To fulfill our other internal KYC policies and requirements.	(a) Identity; (b) Contact; (c) AML and KYC; (d) Enhanced KYC Data (for payments over a certain threshold); and (e) Transaction.	Necessary for our legitimate interests (for risk assessment purposes, to prevent and mitigate against fraud, to safeguard the reputation of our business).

(a) To enable your use of the Platform, process your token subscriptions, purchases, and trading activity, and provide you with the Services that you have requested from us. (b) To keep your account portfolio accurate and updated. (c) Manage transactions and generate transaction reports and records.	(a) Identity; (b) Contact; (c) Financial; (d) Transaction; and (e) Portfolio.	(a) Performance of a contract with you. (b) Necessary to comply with our contractual obligations. (c) Necessary to comply with a legal obligation.
For tax and accounting purposes (e.g. reporting to tax authorities, and accounting and reporting requirements).	(a) Identity; (b) Contact; (c) Financial; and (d) Transaction.	Necessary to comply with a legal obligation.

(a) For billing and invoice purposes; (b) To collect and recover money which is owed to us (debt recovery); (c) Internal record keeping (including files).	(a) Identity; (b) Contact; (c) Financial; (d) Transaction; and (e) Portfolio.	(a) Performance of a contract with you. (b) Necessary to comply with a legal obligation. (c) Necessary for our legitimate interests (to recover debts due to us, to keep track of your token subscriptions and purchases and the provision of the Services to you (including any developments that took place), and to then be able to review such information should an issue arise).

To manage our customer relationship with you, which may include to: (a) notify you about changes to our terms of service or privacy notices; (b) set up, manage and administer your customer account on the Website; (c) distribute and account your funds; (d) deal with your enquiries, requests, complaints or reported issues; (e) contact you in the course of providing the requested services; (f) ask you to participate in a survey; (g) request feedback from you; (h) advise you of industry and legislative updates, (i) inform you about our events and seminars (including webinars); (j) provide you with information about our products and services; (k) provide you with any other information or materials which you have requested from us.	(a) Identity; (b) Contact; (c) Financial; (d) Transaction; (e) Usage; (f) Portfolio; and (g) Marketing and Communications.	(a) Performance of a contract with you. (b) Necessary for our legitimate interests (for customer relationship handling and management, to study business growth and possible trends regarding our products and service areas, to enable a review and assessment of our products and service provision, to develop and grow our business).

(a) To detect, prevent, and/or report fraud or any other potentially illegal or prohibited activity that comes to our attention (b) To assist and cooperate in any criminal or regulatory investigations against you, as may be required of us. (c) To enforce our service terms. (d) To protect the rights and property of ourselves and others.	(a) Identity; (b) Contact; (c) AML and KYC; (d) Enhanced KYC; (e) Data; (f) Financial; (g) Transaction; and (h) Payment.	(a) Necessary to comply with a legal obligation. (b) Necessary for our legitimate interests (including, to protect the reputation of our business).
To administer and protect our business, the Website, and our Platform (including troubleshooting, data analysis, testing, system maintenance, support, reporting, and hosting of data).	(a) Identity; (b) Contact; (c) Usage; (d) Technical; and (e) Website Visit.	(a) Necessary for our legitimate interests (for running and administering our business (including IT support), systems administration, network security, preventing fraud and to maintain the confidentiality of communications, and in the context of a business reorganization or group restructuring exercise). (b) Necessary to comply with a legal obligation.
(a) To carry out market research campaigns; (b) To market our products and services to you by email or other means if you have subscribed to one of our mailing lists (where you are not a customer); (c) To deliver relevant Website content and advertisements to you, and measure or understand the effectiveness of the advertising that we serve to you.	(a) Identity; (b) Contact; (c) Technical; (d) Usage; (e) Website Visit; and (f) Marketing and Communications.	(a) Necessary for our legitimate interests (to develop our products and services and grow our business, to define our customers, to keep our products, services, and the Website updated and relevant, and to inform our marketing strategy). (b) Based on your consent, in the absence of a customer relationship.

To permit us to pursue available remedies or limit any damages which we may sustain.	(a) Identity; (b) Contact; (c) AML and KYC; (d) Enhanced KYC; (e) Data; (f) Financial; (g) Transaction; (h) Portfolio; and (i) Marketing and Communications.	(a) Performance of a contract with you. (b) Necessary for our legitimate interests.

"Legitimate Interest" means our interest to conduct and manage our business affairs appropriately and responsibly, to protect the reputation of our business, and to provide our customers with the best possible service and the users of the Websites with a secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before your Personal data is processed for our legitimate interests. We do not use your Personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted to by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us at the following email address: privacy@vault.ist.

"Performance of Contract" means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract. This includes our Terms of Service or other applicable terms of business.

"Comply with a legal obligation" means processing your Personal data where it is necessary for compliance with a legal or regulatory obligation to which we are subject.

7. Marketing

We strive to provide you with choices regarding certain Personal data uses, particularly around advertising and marketing. Through your Identity, Contact, Usage, Technical, and Website Visit Data, we can form a view of what we think you may want or need. This is how we then decide which of our products and/or services may be relevant or of interest to you (our **marketing communications**).

You may **receive marketing communications** from us (which may consist of newsletters, industry and legislative updates, mailshots, publications, and/or information about our events, seminars, and webinars) where:

- you have entered into an ongoing commercial or contractual relationship with us; and
- provided you have not opted out of receiving marketing from us (see **Your right to object** below).

Where the above does not apply to you, we will only send you our marketing

communications if you have expressly consented to receive them from us.

Third-Party Marketing

We will get your express opt-in consent before we share your Personal data with any third parties (including our affiliated entities) for marketing purposes.

Opting out

You can ask us to stop sending you marketing communications (unsubscribe) at any time by following the opt-out (unsubscribe) links on any marketing communication sent to you.

Cookies

You can set your browser to refuse all or some browser cookies or to alert you when the Website sets or accesses cookies. If you disable or refuse cookies, please note that some parts of the Website may become inaccessible or not function properly.

Change of purpose

We will only use your Personal data for the purposes for which we collected it unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose, or we are obliged to process your data by applicable laws or court / enforceable orders.

If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us at privacy@vault.ist.

If we need to use your Personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your Personal data without the need to obtain your consent, in compliance with the above rules, where this is required or permitted by law.

8. Disclosures of your Personal data

We may have to grant access to, disclose, or share your Personal data with the parties set out below (which may be in or outside your jurisdiction) for the purposes set out in the table in **Clause 6** above

Third-party service providers, including platform integration and infrastructure hosting providers (to store data), KYC providers and identity and customer verification service providers (to facilitate the set-up and opening of your account and from whom we may receive customer due diligence reports on you), payment services and payment gateways (to process payments), and token accounting services (to verify, monitor and secure token subscriptions, purchases and trading activity).

Our affiliated entity, such as partner firms involved in the provision of certain Services.

Affiliated group entities. We share information with these entities to

a) help, detect, and prevent potentially illegal acts and violations of our policies;

b) allow you to use the products and services they provide that are supplied in connection with, or using our products and services; and

c) guide decisions about our products, services and communications.

Suppliers and external agencies that we engage to process information on our or your behalf, including to provide you with the information and/or materials that you may have requested.

Professional advisers such as consultants, bankers, professional indemnity insurers, brokers, and auditors.

Law enforcement agencies, public authorities, and judicial bodies (local and overseas).

Other organizations where the exchange of information is for the purpose of fraud protection or credit risk reduction.

Debt recovery agencies assist us with the recovery of debts owed to us.

Third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets (**successors in title**). Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use your data in the same way as set out in this Policy.

We require all affiliated entities and third-party service providers to respect the security of your Personal data and to treat it following the law. We do not allow them to use your Personal data for their own purposes and only permit them to process your Personal data for specified purposes and following our documented instructions. Our service providers currently store your Personal data in Germany. We will update this Privacy Policy if their data storage location changes.

Some of our service providers (including those providing cloud infrastructure, such as Amazon Web Services) may be located or store data in the United States. Where such transfers occur, we ensure that adequate safeguards are in place to protect your personal data in accordance with GDPR requirements.Certain service providers utilized by our organization, including those responsible for cloud infrastructure such as Amazon Web Services, may operate from or maintain data storage facilities within the United States. In instances where such data transfers are conducted, we implement appropriate protective measures to guarantee the safeguarding of your personal data in alignment with the General Data Protection Regulation (GDPR) standards.

6. International transfers

We do not generally transfer your Personal data outside the European Economic Area ("**EEA**") except

as may be necessary to: (i) process your transactions, subscriptions, purchases, and/or trading activity, (ii) provide the requested services, (iii) fulfill our contractual obligations to you, (iv) exercise and enforce our contractual rights and terms of services, (v) comply with our legal and/or regulatory obligations or (vi) assert, file or exercise a legal claim.

Where we do need to transfer your Personal data to outside the EEA (whether for these stated purposes or any other purpose listed in **Clause 5** above), we will ensure a similar degree of protection is afforded to that Personal data by ensuring at least one of the following safeguards applies or is otherwise implemented:

- We will only transfer your Personal data to countries that have been deemed to provide an adequate level of protection for Personal data by the European Commission.

- In the absence of an adequacy decision, we will use specific contracts approved by the European Commission which give Personal data the same protection it has in Europe.

- Where we use providers based in the U.S., we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to Personal data shared between Europe and the US.

Please contact us at privacy@vault.ist if you want further information on the specific mechanism used by us when transferring your Personal data out of the EEA.

7. Data security

We have put in place appropriate security measures to prevent your Personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed (i.e. to safeguard its integrity and confidentiality). We also regularly review and, where practicable, improve upon these security measures.

We also limit access to your Personal data to strictly those employees, agents, contractors, and third parties that have a professional 'need-to-know'. They will only process your Personal data on our instructions and they are subject to a duty of confidentiality. All our employees and agents have received appropriate training on data protection.

We have put in place procedures to deal with any suspected Personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

8. Data retention

Please note that we consider our relationship with customers to be an ongoing and continuous customer relationship, until such time that either we or the customer terminates it in accordance with our Terms of Use.

We will only retain your Personal data for as long as necessary to fulfill the purposes for which we collected it (see **Clause 6** above) and, **thereafter**:

for the purpose of satisfying any legal, accounting, tax, anti-money laundering, and regulatory obligations or reporting requirements to which we may be subject (including as an issuer of a virtual financial asset in terms of applicable Czech Republic law); and/or

to the extent that we may also need to retain your Personal data to be able to assert, exercise or defend possible future legal claims against you or that otherwise involve you.

By and large, our retention of your Personal data shall not exceed the period of **six (6) years** from the termination of your customer relationship with us (which would typically arise from the closure or termination of your customer account). This retention period enables us to make use of your Personal data for any applicable AML retention and reporting obligations and for the filing, exercise, or defense of possible future legal claims (taking into account applicable prescriptive periods and statutes of limitation). In certain cases, we may need to retain your Personal data for a period of up to **ten (10) years** in order to comply with applicable accounting and tax laws (this will primarily consist of your Transaction Data). There may also be instances where the need to retain Personal Data for longer periods, as dictated by the nature of the products and services provided.

In some circumstances, you can ask us to delete your data. See **Request erasure** below for further information.

Kindly contact us at privacy@vault.ist for further details about the retention periods that we apply.

Data Minimization

To the extent possible, we may anonymize the data that we hold about you when it is no longer necessary to identify you from the data that we hold about you. In some

circumstances, we may even pseudonymize your Personal data (so that it can no longer be associated with you) for research or statistical purposes, in which case we may use this information indefinitely without further notice to you.

9. Your legal rights

Under certain circumstances, you have rights under data protection laws in relation to your Personal data. Please click on the links below to find out more about these rights:

Request access to your Personal data.

*Request correction (**rectification**) of your Personal data.*

Request the erasure of your Personal data.

Object to processing of your Personal data.

Request restriction of processing your Personal data.

Request transfer of your Personal data.

Right to withdraw consent.

If you wish to exercise any of the rights set out above, please contact us at privacy@vault.ist.

No fee is usually charged

You will not have to pay a fee to access your Personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive, or excessive. Alternatively, we may simply refuse to comply with your request in such circumstances.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your Personal data (or to exercise any of your other rights). This is a security measure to ensure that Personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

We try to respond to all legitimate requests within a period of one month from the date of receiving your request. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

You have the right to

(i) **Request access** to your Personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the Personal data we hold about you and to check that we are lawfully processing it.

You may send an email to privacy@vault.ist requesting information on the Personal data that we process. You shall receive one copy free of charge via email of the Personal data that is undergoing processing. Any further copies of the information processed shall incur a charge of €10.00.

(ii) **Right to information** when collecting and processing Personal data about you from publicly accessible or third-party sources. When this take place, we will inform you, within a reasonable and practicable timeframe, about the third party or publicly accessible source from whom we have collected your Personal data.

(iii) **Request correction or rectification** of the Personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected and/or updated, though we may need to verify the accuracy of the new data you provide to us. As mentioned, it is in your interest to keep us informed of any changes or updates to your Personal data that may occur during the course of your relationship with us.

(iv) **Request erasure** of your Personal data. This enables you to ask us to delete or remove Personal data where:

- there is no good reason for us to continue to process it;
- you have successfully exercised your right to object to processing (see below);
- we may have processed your information unlawfully; or
- we are required to erase your Personal data to comply with local law.

Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request. These may include instances where the retention of your Personal data is necessary to:

- comply with a legal or regulatory obligation to which we are subject; or
- establish, exercise, or defend a legal claim.

(v) **Object to processing** of your Personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your Personal data for direct marketing purposes (as under the '**Marketing'** in **Section 5** above).

In some cases, we may demonstrate that we have compelling legitimate grounds to process your personal information that override your rights and freedoms.

(vi) **Request restriction of processing** of your Personal data. This enables you to ask us to suspend the processing of your Personal data in the following scenarios:

- if you want us to establish the data's accuracy;
- where our use of the data is unlawful but you do not want us to erase it;
- where you need us to hold onto the data even if we no longer require it, as you need it to establish, exercise or defend legal claims; or
- where you have objected to our use of your Personal data, but we need to verify whether we have to override legitimate grounds to use it.

(vii) **Request the transfer (data portability)** of your Personal data to you or to a third party. We will provide to you, or a third party you have chosen, your Personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information that you initially provided consent for us to use or where we used the information to perform a contract with you.

(viii) **Withdraw your consent at any time** where we are relying on consent to

process your Personal data (which will generally not be the case). This will **not** however affect the lawfulness of any processing which we carried out before you withdraw your consent. Any processing activities that are not based on your consent will remain unaffected.

Kindly note that none of these data subject rights are absolute, and must generally be weighed against our own legal obligations and legitimate interests. If a decision is taken to override your data subject request, you will be informed of this by our data protection team along with the reasons for our decision.

Complaints

You have the right to complain at any time to a competent supervisory authority on data protection matters, such as (in particular) the supervisory authority in the place of your habitual residence or your place of work.

We would, however, appreciate the opportunity to deal with your concerns before you approach the supervisory authority, so please contact us in the first instance at privacy@vault.ist.

10. Conclusion

We reserve the right to make changes to this Policy in the future, which will be duly notified to you. If you have any questions regarding this Policy, or if you would like to send us your comments, please contact us today or alternatively write to our data protection team using the details indicated in this Policy.