SOIL PLATFORM PRIVACY POLICY

Introduction

This Privacy Policy describes how Soil Limited, a private limited liability company with its registered office in 115B, Suite 3, Old Mint Street, Valletta, Malta ("**Soil**", "**we**", "**our**" or "**us**") collects and uses your personal data and cookies in connection with your use of the Platform and the Services.

This Privacy Policy consists of two parts:

- **Privacy Notice** – which describes how we collect and use your personal data;
- **Cookie Notice** – which describes how cookies and similar technologies are used.

We provide the Platform and the Services subject to the [-] and [-]. Please read the Terms of Use before accessing or using the Platform and/or the Services.

Age restriction

The Platform and the Services are restricted to persons who are at least 18 years of age. We do not knowingly collect personal data from people who are less than 18 years of age in connection with the Platform or the Services. If you – the User – are below 18 years old, you may not use or interact with the Platform or the Services.

Your privacy and blockchain

Blockchain network is an application of a distributed ledger technology (DLT). A distributed ledger is an information repository that keeps records of certain actions (e.g. transactions) and that is shared across, and synchronized between, a set of DLT network nodes using a consensus mechanism. Blockchains are governed by their protocols, i.e. set of rules describing how a network operates (e.g. how a consensus is reached as regards validating a transaction). Such blockchains are intended to immutably record transactions across a wide network of computers and computer systems. Public blockchains are networks that are publicly accessible. Many blockchain networks are decentralized which means that we do not control or operate them.

When you use the Services, some of your data may be recorded on public blockchain networks, depending on the Service and the blockchain protocol. This means that your personal data could be determined directly, when combined with other data, or when anonymous data is de-anonymized. As a result, third parties may potentially access your personal data. For example, many public blockchain networks are open to forensic analysis or other blockchain analytics operations which can lead to the unintentional disclosure of your personal data such as financial data or information about your transactions.

This is due to the way blockchain technology works, where transparency and immutability of the data stored on the chain is one of the fundamental principles of the technology. Because blockchain networks are decentralized, we (or our Affiliates) are not able to delete or change your personal data from such blockchain networks. Please consult relevant information about the potential risks associated with using blockchain technology set out in the [-] and [-].

Definitions

All terms not defined in this Privacy Policy shall have the meaning as defined in the [-], the [-], or in the GDPR. The following terms used in this Privacy Policy shall have the meaning set forth below:

- **AML** – anti-money laundering.
- **AML Directive** – Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
- **Applicable Data Protection Law** – any applicable laws, statutes, regulations, orders, regulatory requirements, bylaws, and other similar legal instruments in force from time to time relating to data protection, data security, privacy, and/or the collection, use, disclosure and/or processing of Personal Data, including but not limited to the GDPR, local implementation of the ePrivacy Directive, or other EU or Member State law.
- **CDD** – customer due diligence.
- **CDD Verification** – CDD Verification as defined in the Terms of Use.
- **CFT** – counter terrorism financing.
- **controller**, **processor**, **processing,** and other terms relating to personal data not defined here – have the meaning as defined in Article 4 of the GDPR.
- **Cookie Notice** – part 2 of the Privacy Policy describing how cookies and similar technologies are used.
- **GDPR** – General Data Protection Regulation 2016/679 of 27 April 2016.
- **EEA** – European Economic Area.
- **Loan Agreement** – the Loan Agreement as defined in the Loan Terms.
- **Loan Terms** – means the document available for review prior to accessing the Vaults, which become accessible to the User solely upon successful Wallet connection and completion of the Online CDD Verification.
- **personal data** – information about identified or identifiable natural person as defined in Article 4(1) of the GDPR.
- **Platform** – Platform as defined in the Terms of Use.
- **Privacy Notice** – part 1 of the Privacy Policy describing how we collect and use your personal data.
- **Privacy Policy** – this Privacy Policy.
- **Soil** – Soil Limited, a private limited liability company established under the laws of Malta with its registered office in Malta, address: 115B, Suite 3, Old Mint Street, Valletta, Malta, entered in the Register under no. C106889, with share capital of EUR 1200.
- **Systems** – the ICT Systems as defined in the Terms of Use.
- **Terms of Use** – Terms of Use for the Platform available at [https://xrpl.soil.co/SOIL_terms-of-use.pdf]
- **you** – the User as defined in the Terms of Use, i.e. any natural person visiting the Platform or using one or more services or functionalities described in the Terms of Use.

Please be advised that in this Privacy Policy we also use the definitions set out in the Terms of Use and Loan Terms. Please refer to this document to better understand the Privacy Policy.

Changes

The Privacy Policy shall be reviewed on an ongoing basis and updated as necessary, for example for legal reasons or to reflect changes in the Terms of Use. The current version of the Privacy Policy has been adopted and is effective as of [10 February 2026].

1. PRIVACY NOTICE

1.1. Controller and contact details

We, Soil, are the controller of your personal data to the extent this Privacy Policy applies. You can contact us by email at: contact@soil.co or in writing to our registered address: 115B, Old Mint Street, Valletta, Malta.

We may engage other entities to assist us in processing your personal data as processors. In such case we remain responsible for use of your personal data. However, in certain cases such entities may be separate controllers of your personal data. As such they are responsible for use of your personal data. You can find more information about recipients of your personal data in Section 1.6 below.

1.2. Sources of personal data

We collect your personal data from the following sources:

1.2.1. You

We collect your personal data from you in connection with your use of the Platform or the Services. For example, we collect your data when you file a complaint.

1.2.2. Automatic data collection

We collect your personal data from your devices or software in connection with your use of the Platform or the Services. For example, we may collect information about your device, its operating system or other software, hardware details, web browser settings and so on when you are browsing the Platform. We collect this information also when you visit our Platform without registration.

1.2.3. Blockchain networks

We collect data from blockchain networks in connection with providing the Services. Such information may include personal and/or anonymous data (please consult Section 1.3.3 for more details).

1.2.4. Public sources

We collect your personal data from public sources in connection with processing for CDD purposes. For example, we may collect information from public registers, sanction lists or lists of persons entrusted with prominent public functions (so-called "politically exposed persons"). We may also collect your personal data from sources such as public online databases, public registries, government, or public authorities when permitted under the Applicable Data Protection Law.

1.1.1. Third parties

We collect your personal data from third parties in connection with your use of the Platform or the Services. For example, when you interact with our profile on social media platforms such as Twitter (X), LinkedIn or via online communicators such as Telegram or Discord. We may also receive your personal data from our business partners. We also collect information from advertising networks, analytics providers, or search information providers in connection with tools such as Google Analytics. Please consult our Cookie Notice for more information.

1.2. Categories of personal data

We use your personal data only when it is lawful under the Applicable Data Protection Law and only to the extent it is necessary to achieve our purposes (please consult Section 1.4). We collect and use the following types of your personal data in connection with your use of the Platform and the Services.

1.2.1. CDD data

The CDD data includes your personal data processed by us or by our KYC service provider(s) acting on our behalf as well as the results of subsequent processing of such data by us in connection with the CDD Verification. For example, this may include information whether you have passed the CDD Verification, aggregated KYC reports with summary information, information whether you are listed on one of the sanction lists, our decisions as regards you in the context of the CDD Verification and so on. This also includes personal data obtained by our KYC service providers or by us from relevant publicly accessible sources, such as public registers, sanction lists or lists of persons entrusted with prominent public functions (so-called "politically exposed persons").

Please note that in certain cases our KYC service providers are independent data controllers. For example, if you enter into User Agreement with [Sum and Substance Ltd (UK)], provider of [Sumsub - KYC, KYB, AML & Fraud Detection provider], your use of its services is subject to the privacy policies and terms and conditions of that company. We encourage you to consult such documents before using such services. For example, you can consult the privacy policy of [Sumsub] (Section [https://sumsub.com/privacy-notice-service/]). We are not responsible for the privacy policies, terms of use and/or practices of such companies where they are independent data controllers.

1.2.2. Customer support data

The customer support data includes data collected and used in connection with customer support provided by us to you. For example, this may include your communication with us as regards your rights as a Consumer, your participation in our surveys or questionnaires or your other requests, questions, and queries.

1.2.3. Social media data

The social media data includes data collected and used in connection with your interactions or visits on our social media profiles. For example, this includes your nickname when you send us a direct message on Twitter, Discord or Telegram and the contents of such message. Please note that social media platforms are independent data controllers. Your use of such platforms is subject to the privacy policies and terms and conditions of such providers of such social media platforms. We encourage you to

consult such documents before using such services. We are not responsible for the privacy policies and practices of such social media platforms. For example, you can consult the privacy policy of Twitter, Discord and Telegram.

1.2.4. Tracking data

The tracking data includes data collected and used in connection with use of cookies and similar technologies, such as pixels, beacons, tags, device IDs, Local Shared Objects or tracking pixels. For example, this includes personal data used when we use cookies to check whether you accepted the Terms of Use and the Privacy Policy before accessing and using the Services. Please consult the Cookie Notice to learn more about cookies and similar technologies.

1.2.5. Technical data

The technical data includes data collected and used in connection with the ICT Systems. For example, this includes your IP address, information about your operating system or other software used by your device, hardware details, statistics derived from this data and so on. Most of this information is anonymous data. However, in some cases it may be used to identify you, for example in combination with other data. In general, if technical data allows for your identification, we treat it as personal data in compliance with the GDPR and other Applicable Data Protection Law.

1.2.6. Web3 data

The Web3 data includes anonymous data and, in some cases, your personal data that we receive in connection with your interactions with the with the Platform's blockchain-based functionalities, as well as our activity and the activity of third parties involved in enabling such functionalities. For example, this includes publicly accessible on-chain information (which can be personal data) and limited off-chain information of technical nature, such as a type of a device, browser version and so on (anonymous data, as a rule). This also includes wallet address which is a personal data when the wallet belongs to you, the User. In general, if Web3 data allows for your identification we treat it as personal data in compliance with the GDPR and Applicable Data Protection Law.

1.3. Purposes and legal grounds of processing

We collect and process your personal data in connection with your use of the Platform and the Services. As a rule, we collect your personal data directly from you and from your devices. We process your personal data to the extent necessary to provide the Services, ensure smooth operation of the Platform or for other legitimate purposes. You can find the description of such purposes and legal grounds for processing in greater detail below.

1.3.1. Analytics

We use your personal data for analytical and statistical purposes, such as monitoring efficiency and good performance of the Platform and Services. For example, this includes verifying certain metrics connected with the load of our ICT Systems or measuring Users' activity against certain metrics, such as monitoring click-through-rate and other parameters. The legal ground for processing your personal data is our legitimate interest (Article 6(1)(f) GDPR), which consists of having access to information about our products and services and their performance. Where required under statutory law, we will be conducting analytical activities only with your consent (Article 6(1)(a) GDPR).

1.3.2. Business operations

We use your personal data for the technical and administration purposes in connection with the maintenance and development of our business. For example, this includes internal assessments, audits, product and services development or improvement and so on. The legal ground for processing your personal data is our legitimate interest (Article 6(1)(f) GDPR), which consists of maintaining and developing our business operations and improving our products and services).

1.3.3. CDD

We use your personal data for CDD purposes, i.e. performing customer due diligence checks, in connection with your use of some of the Platform services. For example, this includes collecting data from you, either by us directly or by our KYC service provider(s), in connection with the CDD Verification to identify and verify Users before entering into Loan Agreement. This also includes fraud detection and/or prevention.

Use of your data for CDD purposes also includes processing for the purposes of detecting, monitoring, and preventing money laundering, terrorism financing, financial crime, and other illegal activities connected with use our Platform or Services. **Please note that Soil is not an obliged entity to which the AML Directive (as implemented in the local law) applies. We voluntarily adopted standards derived from the EU AML/CFT principles to ensure that use of our Platform is safe.**

The legal grounds for processing your personal data depend on a particular processing operation:

- necessity of processing for performance of a contract with you [Article 6(1)(b) GDPR] – as regards the CDD Verification to identify and verify Users before entering into Loan Agreement;
- our legitimate interest (Article 6(1)(f) GDPR), which consists of providing the Services safely and in compliance with our standards derived from the EU AML/CFT principles – detecting, monitoring, and preventing money laundering, terrorism financing, financial crime, and other illegal activities connected with use our Platform or Services;
- our legitimate interest (Article 6(1)(f) GDPR), which consists of preventing fraudulent activities on the Platform and/or fraudulent use of the Services – detecting, monitoring, and preventing fraud.

In certain cases, we may use automated decision-making processes in connection with the CDD purposes (please consult Section 1.10 for more details on such use of your data and its legal ground for processing).

1.3.4. Compliance

We use your personal data to ensure compliance with the applicable law. For example, this includes processing of your personal data to comply with consumer protection law. We also process your personal data to comply with the GDPR, for example when you submit your request as regards your privacy rights or for accountability purposes. This also includes compliance with applicable law introducing international or national sanctions targeting individuals or other entities. The legal ground for processing is the necessity of

processing for compliance with appropriate legal obligation under applicable law to which we are subject (Article6(1)(c) GDPR).

1.3.5. Contract performance

We use your personal data to perform contracts we have executed with you. For example, this includes rendering Services to you subject to the Terms of Use. The legal ground for such processing is the necessity of processing for performance of a contract with you (Article 6(1)(b) GDPR). For your convenience and to ensure that this Privacy Policy is intelligible, we have provided additional information on the selected Services below.

1.3.5.1. Blockchain-Based Services

We use your personal data and/or anonymous data to provide the blockchain-based services of the Platform, including the Vault service. For example, this includes processing your personal data for the purpose of allowing you access and use of the Vault service in connection with the Loan Agreement. The legal ground for processing your personal data is (depending on the circumstances and particular blockchain-based service of the Platform) appropriate legal obligation under applicable statutory law to which we are subject (Article6(1)(c) GDPR, performance of a contract with you (Article 6(1)(b) GDPR), or our legitimate interest (Article 6(1)(f) GDPR), which consists of providing our safe and high-performance of the blockchain-based services of the Platform to the Users.

1.3.5.2. Other Services

We use your personal data, such as your IP address or other online identifiers, for the purpose of rendering Access to the Platform, Wallet Connection and Dashboard Services. For example, this includes providing you access to the contents collected on the Platform in performance of the Access to the Platform Service. The legal ground for such processing is the necessity of processing for performance of a contract with you (Article 6(1)(b) GDPR).

1.3.6. Legal rights

We may process your personal data, if necessary, to establish and assert claims or to defend against claims. The legal ground for such processing is our legitimate interest (Article 6(1)(f) GDPR), which consist of the protection of our legal rights.

1.3.7. Marketing

We use your personal data for marketing purposes, such as sending you commercial information or direct marketing. For example, this includes providing you with our notifications, email, Newsletter or other messages containing commercial information about our brand, products, or services. This also includes processing your personal data when you visit our social media profiles for the purpose of promoting our brand, including informing you about activities, events and news concerning us. The legal ground for processing your personal data is our legitimate interest (Article 6(1)(f) GDPR), which consists of promoting our business or, if applicable, your consent (Article 6(1)(a) GDPR).

1.3.8. Security

We process your personal data to ensure the security and safety of the Platform and our ICT systems and to manage them. This includes detection of malware, bugs, possible exploits, virus screening, attacks, unlawful or malicious actions, IT security threats detection and prevention and so on. For example, we record some of your personal information in a system logs (special computer program used for storing a chronological record containing information about events and actions related to the ICT Systems used for rendering Services by us). The legal ground of the processing is our legitimate interest (Article 6(1)(f) GDPR), which consists of our need to ensure security and safety of our ICT systems used in connection with the Platform and the Services.

1.3.9. Social media interaction

We process your personal data for the communication and marketing purposes. For example, to inform you about our activity and promote various events, services, and products. We also process your personal data to communicate with you, to promote our brand and for direct marketing purposes, for example to collect your feedback on our products or services. The legal basis of the processing is our legitimate interest (Article 6(1)(f) GDPR), which consists of improving our services, communication with the Users, promotion, and marketing. Where required under statutory law, we will be conducting direct marketing activities only with your consent (Article 6(1)(a) GDPR).

1.4. Data storage

We store your personal data only as long as necessary for the purposes we collected it. This means that the duration of storage depends on the purpose of processing. For example, we store your personal data for the period when we provide you the Services in accordance with the agreement we have entered with you subject to the Terms of Use. We store personal data processed based on legitimate interest(s), our or those of a third party, until you lodge an effective objection to such processing. Similarly, when we process your personal data based on your consent, we store it until you withdraw your consent.

The duration of storage or use of your data may be extended in certain situations. For example, we may store your personal data after you terminate the agreement with us when required by law. We may also continue to store and use the same dataset if we use it for a different purpose and on a different legal basis, if admissible by law. For example, if you terminate the agreement with us, we may continue to use personal data provided by you in connection with your use of the Services when necessary to establish and assert possible claims or to defend against claims (if we have a legitimate interest to do so).

After the end of the period of data storage, we permanently delete or anonymize your personal data.

Please note that use of the blockchain networks in connection with the Services, depending on the blockchain protocol, may result in recording some of your personal data (e.g. Web3 data) on the blockchain. This means that your personal data could be determined directly, when combined with other data, or when anonymous data is de-anonymized. As a result, third parties may potentially access your personal data. For example, many public blockchain networks are open to forensic analysis or other blockchain analytics operation which can lead to the unintentional disclosure of your personal data such as financial data or information about your transactions. This is due to the way blockchain technology works, where transparency and

immutability of the data stored on the chain is one of the fundamental principles of the technology. Please consult relevant information about the potential risks associated with using blockchain technology set out in the Terms of Use and Loan Terms.

1.5. Data recipients

As a rule, we do not share your personal data unless it is necessary. For example, we may share your personal data for example in connection with the provision of the Services under the Terms of Use. We may disclose your personal data to the following categories of recipients:

- KYC services providers;
- Web3 wallet services providers;
- Web3 decentralized cryptocurrency exchanges;
- external developers or software solution providers;
- marketing and advertising services providers;
- analytical tools providers;
- data storage providers;
- professional advisors, such as lawyers, accountants, and tax advisors.

We require our partners to keep your data secure and confidential under the terms that ensure level of protection essentially equivalent to that described in this Privacy Notice. Please note that some of them act on our behalf as our processors and some act as independent controllers of your personal data. If they are controllers of your data, relevant privacy policies and terms and conditions of such controllers may apply. We encourage you to consult such documents before using such services. We are not responsible for the privacy policies and practices of the third parties.

As a rule, our partners are in the European Economic Area. However, some of them may be located outside of the EEA, for example in the United States. Please consult Section 1.7 of the Privacy Notice for more details on transfers of your personal data outside of the EEA.

Below you can find additional information on selected categories of recipients of your data.

1.5.1. Data storage and hosting providers

We share with and receive your personal data with data storage and hosting providers. For example, we can store your personal data on AWS cloud servers located in the EEA. You can find more details about the data sharing in the summary below:

- **Name(s) and link(s) to privacy policy**: Amazon Web Services (https://aws.amazon.com/compliance/data-privacy/); Global Cloud Infrastructure LTD (https://www.vpsserver.com/privacy-policy/)
- **Country(ies) of processing**: EEA (Amazon Web Services), Gibraltar (Global Cloud Infrastructure LTD)
- **Type of personal data shared**: Technical data, Web3 data
- **Legal grounds of data sharing**: performance of a contract with you (Article 6(1)(b) GDPR)

1.5.2. KYC services providers

We share your personal data with our KYC services providers. For example, we may exchange personal data related to your KYC Procedure results. You can find more details about the data sharing in the summary below:

- **Name(s) and link(s) to privacy policy**: Sum and Substance Ltd (UK), (https://sumsub.com/privacy-notice-service/)
- **Country(ies) of processing**: Germany (Standard central storage location on AWS GDPR-compliant servers)
- **Type of personal data shared**: CDD data
- **Legal grounds of data sharing**: performance of a contract with you (Article 6(1)(b) GDPR); our legitimate interest (Article 6(1)(f) GDPR), which consists of our interest of preventing fraudulent activities on the Platform and/or fraudulent use of our Services.

1.5.3. Web3 wallet services providers

We share your personal data with our partners who provide wallet services to you. For example, when you connect your MetaMask wallet using the Wallet Connection Service, we exchange certain data to enable such connection. You can find more details about the data sharing in the summary below:

- **Name(s) and link(s) to privacy policy**:
  Consensys (MetaMask): Privacy Notice (MetaMask XRPL Snap - developed by Peersyst - Privacy policy).
  Crossmark: Privacy Policy.
  Xaman (earlier XUMM): Privacy Policy (XRPL Labs).
  WalletConnect: Privacy Notice.
- **Country(ies) of processing**:
  USA i UE: (MetaMask/Consensys).
  Netherlands / EU: (Xaman).
  The Cayman Islands: (WalletConnect).
  Global (including EU): (Crossmark)
- **Type of personal data shared**: Web3 data, Technical data
- **Legal grounds of data sharing**: performance of a contract with you (Article 6(1)(b) GDPR)

1.5.4. Blockchain network participants

Please note that your use of the blockchain networks in connection with the Services, depending on the blockchain protocol, may result in recording some of your personal data on the blockchain. This means that your personal data could be identified directly, when combined with other data, or when anonymous data is de-anonymized. As a result, third parties may potentially access your personal data.

1.5.5. Our affiliates and subsidiaries

We share your personal data with our affiliates and subsidiaries. All such entities adhere to the same level of personal data protection as described in this Privacy Notice. In addition, in case of a merger, acquisition or reorganization, we may share your personal data with an involved party. We will ensure that such Third-Party is obligated to keep

your data secure and confidential under the terms that ensure level of protection essentially equivalent to that described in this Privacy Notice.

1.5.6. Public authorities

We may share your personal data with public authorities where required by law and subject to the statutory conditions and limitations.

1.6. Data transfers outside the EEA

The level of protection for the Personal Data outside the European Economic Area (EEA) differs from that provided by the EU law. For this reason, we transfer your personal outside the EEA only when necessary and with an adequate level of protection, primarily by cooperating with processors of the personal data in countries for which there has been a relevant European Commission decision finding an adequate level of protection for the Personal Data. Alternatively, we may use the standard contractual clauses issued by the European Commission. If you want to learn more about these safeguards, obtain a copy of them or learn where they have been made available, contact us (please consult Section 1.1 above).

1.7. Requirement to provide personal data

In some cases, provision of your personal data is mandatory by law or necessary to carry out your request or to perform a contract we have with you. If you fail to provide us with your personal data in such situations, we may not be able to carry out your request, perform a contract with you (or enter into it) or comply with the law. In some cases, this may mean that we will terminate the contract or stop our engagement with you. For example, if you do not provide your personal data necessary for the consumer complaint procedure, we may not be able to handle your complaint.

In other cases, provision of your personal data is voluntary. If you fail to provide us with your personal data in such situations, we may not be able to carry out your request or achieve our goal. For example, if you do not share your contact details with us, we may not be able to contact you.

1.8. Your rights

To exercise your right(s) contact us (please consult Section 1.1 above).

Depending on where you live, you may have different privacy rights. If the EU law applies to you, you have the following rights under the GDPR.

Please note that it may be technically impossible, depending on a blockchain protocol, to delete or change any information recorded on-chain in a public blockchain network due to the nature of the blockchain technology. Most blockchain networks are decentralized which means that we do not control or operate them. Because of that, we (or our affiliates) are not able to delete or change your personal data from such blockchain networks. Please consult relevant information about the potential risks associated with using blockchain technology set out in the Terms of Use or Loan Terms.

1.8.1. Right to access information

You can request from us information about the processing of your personal data. You can also request a copy of your personal data that we process from us free of charge. However, under certain conditions set out by privacy law, we may charge a fee for that.

1.8.2. Right to correct your data

You can request that we rectify your personal data that we use, for example, when it is inaccurate. You can also complete your data if it is incomplete.

1.8.3. Right to be forgotten

You can request that we erase your personal data under certain conditions prescribed by law. However, this is not an absolute right, and it does not apply in certain conditions, for example, when use of your data is necessary for the establishment, exercise or defense of legal claims by us.

1.8.4. Right to restrict

You can request that we stop processing your personal data, except for storage, under certain conditions prescribed by law. However, this is not an absolute right, and it does not apply in certain conditions, for example when use of your data is necessary for the protection of the rights of another natural or legal person.

1.8.5. Right to data portability

You can request that some of your personal data is provided to you, or to another controller, in a commonly used and machine-readable format. This right applies where we use your data based on your consent or a contract and if the processing of your data is carried out by automated means.

1.8.6. Right to withdraw consent

You have the right to withdraw your consent to the processing of your personal data. You can do this at any time. If you withdraw consent, we will stop using your personal data where the basis for processing is consent. Withdrawal of consent does not affect the lawfulness of processing your data based on consent before withdrawal. The right to withdraw consent applies only to the extent that your personal data is processed based on consent.

1.8.7. Right to object

You have the right to object to the processing of your personal data based on legitimate interest(s), our or those of a third party. You can do this at any time. If you raise an objection, we will stop using your personal data where the basis for processing is our legitimate interest. In exceptional circumstances, we may continue to use your data despite your objection. This exception does not apply when you object to the processing of data for direct marketing purposes, i.e. if you object to it, we will stop processing your personal data on this basis.

1.8.8. Right to lodge a complaint

You can lodge a complaint with the supervisory authority dealing with the protection of personal data. You can lodge such complaint with your local data protection authority or

with the Information and Data Protection Commissioner, a Maltese data protection authority based in Sliema, Malta (https://idpc.org.mt/).

1.8.9. Rights connected with automated decision-making

You have the following rights connected with automated decision-making process in used for the purpose of the KYC Procedure:

- right to contest the automated decision(s) made in connection with the KYC Procedure;
- right to express your point of view in connection with such automated decision(s);
- right to obtain human intervention as regards the automated decision-making process used for the purpose of the KYC Procedure.

These rights are limited to decisions based solely on automated processing. This means that in some cases, for example when the specific KYC process is not fully automated, you are not entitled to these rights. Please contact us for more details (consult Section 1.1 of the Privacy Policy for our contact details).

1.9. Automated decision-making

We may use automated decision-making. This means that certain decisions about you which may produce legal effects concerning you or similarly significantly impact you (i.e. determine if you can use our Services) will be made solely by technological means without human involvement. Apart from such fully automated decisions, we may also use semi-automated decisions (i.e. made by us based on results of an automated data collection and analysis).

1.9.1. How automated decisions are made?

The CDD Verification involves collecting your personal data from you and other sources (consult Section 1.2 of the Privacy Policy for more details on sources of your data). For example, we or our service providers may:

- make automated checks of your personal data against the information in multiple databases, including sanction lists or lists of persons entrusted with prominent public functions (so-called "politically exposed persons") to verify your presence in such databases and the authenticity of uploaded documents;
- use geo-blocking to ensure that the Users from restricted countries under our internal CDD procedure aligned with the EU AML/CFT standards cannot access our Website and/or the Services;
- use fraud detection and prevention systems, including systems detecting suspicious or malicious activity;
- use so-called wallet screening to ensure that funds in the cryptocurrency wallet of a User are not restricted funds under our internal CDD procedure aligned with the EU AML/CFT standards (for example, do not originate and/or are not related to any restricted person or any other suspicious activity under our internal CDD procedure aligned with the EU AML/CFT standards).

The results of such processing are then automatically checked against preset thresholds, conditions or other reasoning mechanisms implemented in our Systems by us or our service providers acting on our behalf. If the results of such checks do not meet such thresholds or other requirements, your CDD Verification result will be negative. For example, if you are listed on an international sanction list, you will not pass the CDD Verification with positive result.

1.9.2. What are the consequences of automated decisions?

The results of the CDD Verification determine whether you can access and/or use the blockchain-based Platform services, such as Vault service.

If the results are positive, you will be able to access and/or use the blockchain-based Platform services, such as Vault service.

If the results are negative, depending on a particular system employed by us or our service providers, you will be either:

- automatically blocked from accessing and/or using the blockchain-based Platform services, such as Vault service (for example, when we detect that you are trying to circumvent our requirements on restricted countries or restricted individuals);
- flagged for manual review by us; depending on the result of the manual review, you may or may not be able to access and/or use the blockchain-based Platform services, such as Vault service. Such manual review does not constitute an automated decision-making as the decision is made by a human.

1.9.3. What are the grounds of processing?

Our use of automated individual decision-making is necessary for entering into, or performance of, a contract between you (the User) as we require our Users to comply with our internal CDD procedure aligned with the EU AML/CFT standards. This means that use of such automated decision-making tools is a contractual requirement under the Terms of Use in order for you to access and/or use blockchain-based Platform services, such as Vault service. The legal ground of processing for the purpose of the automated individual decision-making is a necessity of processing for performance of a contract with you [Article 6(1)(b) GDPR].

1.9.4. Your rights

To exercise your right(s) contact us (please consult Section 1.1).

You have the following rights connected with automated decision-making:

- right to contest the automated decision(s);
- right to express your point of view in connection with such automated decision(s);
- right to obtain human intervention as regards the automated decision-making process.

These rights are limited to decisions based solely on automated processing. This means you are not entitled to execute these rights in connection with semi-automated decision-making or where decisions are made solely by humans. You may use your other rights under the GDPR listed in Section 1.10 in such case.

2. COOKIE NOTICE

2.1. What are cookies?

Cookies are small text files installed on your device that collect information which, as a rule, facilitates use of the Platform and the Services. For example, cookies may remember whether you accepted the Terms of Use and the Privacy Policy before accessing and using the Services. In most cases information used in connection with cookies is personal data. In such cases, the Privacy Notice applies to such personal data.

We mainly use our own cookies. We may also use other technologies similar to cookies, for example HTML5 local storage, Local Shared Objects or tracking pixels. Where we refer to cookies in this Cookie Notice, we also mean such technologies.

2.2. What about personal data?

We may use your personal data in connection with the use of cookies or similar technologies for purposes described in Sections 1.4.1–1.4.8 of the Privacy Notice. The legal grounds for processing your personal data are (depending on the type of cookies) your consent (Article6(1)(a) GDPR) or necessity of processing for performance of a contract with you (Article 6(1)(b) GDPR).

2.3. What cookies are used?

The following types of cookies are used in connection with your use of the Platform and the Services.

2.3.1. Necessary cookies

The necessary cookies are the type of cookies that are required by the Platform and the Services to function properly. For example, we use cookie(s) to remember whether you accepted the Terms of Use and the Privacy Policy before accessing and using the Services. These cookies are set by us. They are mandatory because they are necessary for the provision of the Platform and the Services.

2.3.2. Analytical cookies (optional)

The analytical cookies are a type of cookies that enable collecting information such as number of visits and traffic on the Platform for statistical purposes. For example, these types of cookies may be installed to analyse how you navigate the Platform and/or the performance of the Platform. They may be set by us or by third-party providers engaged by us. They are optional, so we use them only with your consent.

2.4. Description of the cookies

Each cookie has a specific provider responsible for the cookie (e.g. us or a third party), a specific purpose of use, and a maximum functioning period. If the provider of a cookies is a third party, such third party has access to such cookies. The duration of the operation of cookies depends on their type and purpose. In general, there are two types of cookies: session cookies and persistent cookies. Session cookies expire at the end of a given session. Persistent cookies are stored on the device for a longer period. They do not expire

after the end of a given session. The maximum period after which our cookies expire is 12 months.

The following cookies are used in connection with your use of the Platform or the Services:

NECESSARY COOKIES

Cookie name	Purpose	Provider	Duration
cookieyes-consent	CookieYes sets this cookie to remember users' consent preferences so that their preferences are respected on subsequent visits to this site. It does not collect or store any personal information about the site visitors.	CookieYes	1 year

ANALYTICAL COOKIES

Cookie name	Purpose	Provider	Duration
_ga_*	Google Analytics sets this cookie to store and count page views.	Google Analytics	1 year 1 month 4 days
_ga	Google Analytics sets this cookie to calculate visitor, session and campaign data and track site usage for the site's analytics report. The cookie stores information anonymously and assigns a randomly generated number to recognise unique visitors.	Google Analytics	1 year 1 month 4 days

2.5. Your cookie rights

There are several ways in which you can manage cookies.

2.5.1. Your consent

Optional cookies, for example advertising cookies, are used only with your consent. You can withdraw your consent at any time. You can do this through your cookie settings (Section 2.5.2) or through your browser settings (Section 2.5.3).

2.5.2. Web browser

You can also manage cookies through your web browser. For example, you can delete all or some cookies from your device or block them.

Please note that deleting or blocking cookies may cause the Platform or the Services to not function properly or to stop functioning altogether.

To manage cookies through your web browser, refer to the instructions provided by your browser provider. For example, some of such instructions for the relevant web browsers can be found on the websites of their operators: Microsoft (Internet Explorer, Edge), Google (Chrome), Apple (Safari), Mozilla (Firefox), Opera (Opera).

2.5.3. Your rights related to personal data

You have rights related to your personal data as set forth in the Privacy Notice (Section 1.9).