

Dashboard Privacy Policy

Date Last Revised: April 1, 2025

This Dashboard Privacy Policy ("**Privacy Policy**") describes and summarizes the policies and procedures of Salt Edge Limited ("**Salt Edge**", "**we**", "**our**", "**us**") with respect to the processing of Personal Data in connection with the provision to You of the Services under the [Dashboard Terms and Conditions](#).

Salt Edge takes the privacy of individuals very seriously. We are committed to maintaining the security, confidentiality, availability and integrity of the Personal Data in our custody or control, and protecting such data in accordance with the applicable legislation. Salt Edge continually assesses the employed security measures, both technical and organizational, in order to determine the appropriate level of protection. We regularly review our privacy and security practices and adapt them as necessary to deal with new regulatory requirements, changes in legislation and/or security standards.

Please read this Privacy Policy carefully and refer to the [Dashboard Terms and Conditions](#) for a better understanding of the Services and for any key terms that we do not explicitly define here.

1. DEFINITIONS

For the purposes of this Privacy Policy, in addition to the capitalized terms defined elsewhere in this Privacy Policy and the Dashboard Terms and Conditions, the following terms shall have the meanings ascribed to them as follows:

1.1. "Account Provider" means the payment service provider that provides and maintains a Payment Account for You (e.g., bank, building society, electronic money institution) and is established in either the European Union/European Economic Area, or the United Kingdom of Great Britain and Northern Ireland ("**United Kingdom**").

1.2. "App Provider" means the third party, which supplies You with products and/or services through their website, mobile application or other electronic means (collectively, "**App**") and that redirects You to the Services and with whom You instruct and authorize Salt Edge to share Your Payment Account Data and/or Analytical Reports, based on your GDPR Consent.

1.3. "Controller" means a person, who, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

1.4. "Dashboard" means the online platform located at <https://www.saltedge.com/dashboard> accessed by You with your User Account credentials in order to use the Services, including without limitation any content, images, text and icons within such platform.

1.5. "Data Protection Laws" means the [UK GDPR](#), [EU GDPR](#), as well as the laws implementing or supplementing UK GDPR/ EU the GDPR in UK or each EU Member State, as well as the UK GDPR, and which are applicable to Salt Edge as regards the privacy, protection, processing, collection, use or disclosure of Your Personal Data, as amended, replaced or superseded from time to time.

1.6. "Data subject" means an identified or identifiable individual.

1.7. "GDPR Consent" means a freely given, specific, informed and unambiguous indication of Your wishes by which You, by a clear affirmative action, give explicit consent to Salt Edge to share Your Payment Account Data and/or Analytical Reports with Your App Provider.

1.8. "Payment Account Data" means the information made available from Your Account Provider relating to Your Payment Account, including without limitation account details (account name, number, balance, currency, etc.), transactions details (transaction amount, currency, date, description, etc.), account holder details (name, address, email, phone number), and features and benefits of Your Payment Account, that is accessed and automatically retrieved by Salt Edge through the Services.

1.9. "Personal Data" means any information relating to an identified or identifiable individual and includes, without limitation, Registration Information, Payment Account Data, Session Information, IT Identifiers and Identification and contact data.

1.10. "Processing" means 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.

1.11. "Processor" means a person who processes Personal Data on behalf of a Controller.

1.12. "Services" means the Account Information Services and, as applicable, the functionalities (including consent management functionalities), content, features, tools or services as made available by Salt Edge from time to time in the Dashboard.

1.13. "Special Categories of Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

1.14. "User Account" means the unique user account in the Dashboard set up with Salt Edge.

2. WHAT PERSONAL DATA WE COLLECT ABOUT YOU AND HOW WE GET IT

2.1. In connection with the provision of the Services to You, we will generate or collect, and process the following Personal Data about You:

- a. Personal Data contained in Your **Payment Account Data**, which Salt Edge collects via our production systems when we access Your Payment Account(s) held by the respective Account Provider in read-only mode based on Your AIS Consent in order to retrieve, use, store and process Your Payment Account Data. This Personal Data is collected from Your Account Provider.
- b. **Registration Information** (such as, without limitation, email address, password, etc., as the same may be updated by You from time to time), which is provided by Your App Provider on Your behalf during registration process in order to automatically set up Your User Account when You start using the Services. Salt Edge may be required by law or regulation to collect

this information for identity verification during or subsequent to User Account registration. Under certain circumstances, some of the additional information (such as Your full name, date of birth, residence address, type of Payment Account – own, shared or legal, etc.) that we require for compliance with applicable anti-money laundering, terrorist financing and performing related customer identity, status and operations checks as prescribed by law in order to establish matters such as identity, affiliation, public exposure, ownership of Payment Accounts, purpose of transactions and origin of funds on Your Payment Accounts, may be provided to Salt Edge by Your App Provider during the registration of Your User Account.

- c. Identifiers (unique alphanumeric sequences) attributed in Your respect in our IT systems ("**IT identifiers**"). We generate IT identifiers ourselves in order to provide the Services to You.
- d. Personal Data contained in the technical information about the use of our systems in connection with the Services ("**Session Information**"). The Session Information we collect relates, generally to (i) the time of day when You access our systems and use their services, (ii) which components of our systems You access or use, (iii) actions You make when interacting with our systems and the outcome of these actions (such as errors), and (iv) Your browser type and version, operating system and version, user agent, device type and model, and internet protocol ("IP") address. We collect Session Information automatically when You use the Services.
- e. **Identification and contact data** (such as, without limitation, name, email address, phone number), which we may collect directly from You when You contact Salt Edge's support team or DPO (by email) with respect to any issues relating to the Services or communicate with Salt Edge in any other way. In some cases, Salt Edge may require additional information, including Personal Data, in order to identify You while processing Your enquiry or request. Salt Edge may also maintain records of such communications with You, including any follow-ups and subsequent feedback, for internal purposes.

2.2. Please note that we collect and use this Personal Data for the purposes described in Section 3 'How and why we use your Personal Data' below. We do not necessarily always collect and process all the above categories of Personal Data. Some of this data we collect and process only if required in the circumstances of our interaction with You.

2.3. We would like You to know that there is no statutory or contractual requirement or obligation that You provide any Personal Data to us. Nevertheless, if You do not provide Personal Data we require, it may delay or prevent us from providing the Services to You and/or addressing Your enquiries, requests, and complaints.

3. HOW AND WHY WE USE YOUR PERSONAL DATA

3.1. Salt Edge acts as Controller of Your Personal Data processed in connection with the provision of Services to You and, as applicable, the generation of Analytical Reports.

3.2. Salt Edge will adhere to the following general principles with respect to Personal Data processing:

- not collect more Personal Data than reasonably necessary for the purpose of providing the Services to You and, as applicable, generating Analytical Reports;

- not use Personal Data for any other purposes than those specified in this Privacy Policy;
- ensure that all personnel authorized by Salt Edge to process Personal Data have committed themselves to confidentiality obligations which are materially consistent with Salt Edge's obligations under this Privacy Policy, or are under an appropriate statutory or professional obligation of confidentiality; and
- not knowingly solicit, access, collect and/or process any Special Categories of Personal Data, except when required for compliance with applicable anti-money laundering, terrorist financing and performing related customer identity, status and operations checks as prescribed by law.

3.3. Under the applicable Data Protection Laws, we can only process Your Personal Data if we have a lawful basis, a proper reason for processing. Salt Edge's legal bases for processing the Personal Data collected, as described in this Privacy Policy, will depend on the type of Personal Data and the circumstances under which it is collected. We will collect and process Personal Data based on the following legal bases:

- processing is necessary for the performance of a contract to which You are a party;
- processing is based on Your GDPR Consent, pursuant to which Salt Edge discloses by sharing with Your App Provider Personal Data and/or Analytical Reports, as indicated in, and authorized by You through, such GDPR Consent;
- processing is necessary to comply with legal and regulatory obligations; and/or
- processing is necessary for the purposes of pursuing our own legitimate interests or those of a third party. We may process Your Personal Data based on legitimate interests whether we have a compelling justification for that or even when You should reasonably expect such processing to take place. In any case we can rely on legitimate interests as long as they are not overridden by Your own rights and interests and to ensure this, we carry out an assessment to balance our interests against Your own.

If there is another legal basis for us to collect and process Personal Data, we will provide the required notification to You at or before the time the Personal Data is collected.

3.4. If You voluntarily submit or provide Personal Data to Salt Edge when contacting us with an enquiry or request relating to the Services or otherwise, You will be deemed to have given Your consent to the collection, use and processing of Personal Data by Salt Edge as reasonably necessary to carry out the specific purpose(s) for which You have provided the Personal Data. Salt Edge will rely on such implied consent as if it were given to Salt Edge under normal circumstances.

3.5. The table below explains in detail what we use Your Personal Data for and why:

Personal Data we process	Purposes of processing	Lawful basis for processing
<p>Personal Data that is part of Payment Account Data</p>	<ul style="list-style-type: none"> - to provide the Services, including Analytical Reports; - to enable Your App Provider to provide the services and related support to you; - to troubleshoot, investigate and fix service-related errors, to provide support to Your App Provider; - to provide customer support; - to handle and process enquiries submitted by You. 	<p>Performance of contract with You under the Dashboard Terms and Conditions.</p> <p>Our legitimate interest to ensure that our contractual arrangements with Your App Provider are complied with.</p> <p>Our legitimate interest to ensure continuity and availability of our services, including in accordance with our contractual obligations.</p>
<p>Registration Information</p>	<ul style="list-style-type: none"> - to provide the Services. 	<p>Performance of contract with You under the Dashboard Terms and Conditions.</p>
<p>IT Identifiers and Session Information</p>	<ul style="list-style-type: none"> - to ensure precise and adequate separation and structuring of records relating to You and Your Payment Account(s) in our systems, including for the purpose of sharing Payment Account Data with Your App Provider; - to provide the Services; - to improve the Services and user experience; - to enable identification to address Your enquiries, complaints and data subject requests; - to keep count of the usage of our systems by Your App Provider under our business arrangements with them; - to compile statutory reports on our activity; 	<p>Performance of contract with You under the Dashboard Terms and Conditions.</p> <p>Compliance with our legal obligations to prevent Personal Data Breaches; to provide statutory reports on our activity to regulators; to facilitate supervision by competent authorities; to prevent, detect, report and minimise fraud incidents; to ensure due management of operational and security risks and to demonstrate compliance with statutory requirements; to ensure the security of the Services.</p> <p>Our legitimate interests to ensure that we keep due track of the use of our systems and services; to ensure that we adequately perform our</p>

	<ul style="list-style-type: none"> - to prevent and detect unauthorised access and fraudulent activity; - to protect security of our systems and data; - to assess and manage operational and security risks relating to the Services; - to monitor and report operational and security incidents regarding the Services; - to investigate illegal activity in connection with the Services; - to address and resolve complaints received from You; - to enforce legal rights or defend or undertake legal proceedings in relation to the Services provided. 	<p>obligations towards Your App Provider(s); to ensure that we are billing and getting paid for our products and services; to prevent and detect damaging and prejudicial activity; to ensure that we carry out a customer-friendly business; to ensure that we adequately maintain the Services at adequate standards of service provision and improve them overtime; to ensure that we carry out a customer-friendly business and that complaints and other requests are adequately addressed; to protect our business, interests and rights against unfunded claims or breaches of our legal or contractual rights.</p>
<p>Identification and contact data</p>	<ul style="list-style-type: none"> - to properly handle enquiries, complaints and requests (including data subject requests) submitted to us or in our respect; - to demonstrate compliance with the applicable legal provisions regarding addressing complaints and data subject requests; - to enforce legal rights or defend or undertake legal proceedings in relation to the Services provided. 	<p>Compliance with our legal obligations to respond to complaints and data subject requests.</p> <p>Our legitimate interest to ensure that we carry out a customer-friendly business and that complaints and other requests are adequately addressed.</p> <p>Our legitimate interest to demonstrate compliance with our legal obligations and protect our business against unfunded claims and allegations.</p>

4. NO AUTOMATED DECISION-MAKING; ANONYMIZATION

4.1. We do not engage in automated decision-making in Your respect as a result of processing Your Personal Data in accordance with the Dashboard Terms and Conditions and this Privacy Policy.

4.2. Salt Edge may generate anonymous data derived from or based on Personal Data collected from You or acquired from Your use of the Services, which anonymous data can no longer be used to identify, directly or indirectly, a natural person ("**Anonymized Data**"), and may combine or incorporate such Anonymized Data with or into other similar data or information collected from other users or derived from other users' use of the Services ("**Anonymized Aggregated Data**"). Salt Edge may use such Anonymized Data and Anonymized Aggregated Data for various business purposes, including, but not limited to:

- providing, maintaining, supporting and improving the Services;
- conducting analytical research, compiling statistical reports and performance tracking;
- developing and/or improving other Salt Edge's services and products; and
- sharing such Anonymized Data and Anonymized Aggregated Data with Salt Edge's affiliates, agents and/or Subcontractors.

Anonymized Data and Anonymized Aggregated Data are not Personal Data, and consequently the provisions in this Privacy Policy are not applicable to such data. For the avoidance of doubt, we will not sell Anonymized Data and Anonymized Aggregated Data.

5. CHILDREN'S PRIVACY

Protecting the privacy of children is especially important to Salt Edge. The Services are not directed to children under the age of eighteen (18) years and Salt Edge does not knowingly solicit, collect or process Personal Data from persons under eighteen (18) years of age. If we become aware of the fact that Personal Data of persons less than eighteen (18) years of age has been collected via the Services, we will take the appropriate steps to delete such information without undue delay.

6. PERSONAL DATA DISCLOSURES

6.1. We routinely share Personal Data with:

- App Providers.** We will share Your Payment Account Data (after processing, including without limitation data enrichment, carried out by Salt Edge on such data) and/or Analytical Reports with Your App Provider based on Your GDPR Consent. By sharing Your Payment Account Data and/or Analytical Reports with Your App Provider designated in GDPR Consent, such App Provider, as the receiving party, will act as an independent Controller with respect to Personal Data so shared. Therefore, Your App Provider is solely responsible for complying with its obligations as Controller as set forth in the applicable Data Protection Laws, including, without limitation, with respect to the processing, confidentiality and security of Your Personal Data by Your App Provider after Salt Edge shares such data with Your App Provider. Salt Edge will not be responsible for any subsequent processing carried out by Your App Provider. Salt Edge will only be responsible for the sharing of Your Personal Data and ensuring that it is shared securely and with the intended recipient.
- Salt Edge Inc.,** who is our parent company and, as a subcontractor and data Processor, provides us with the technology, facilities and personnel required to provide the Services to

You. Salt Edge Inc. is a Canadian corporation with its registered office at 150 Elgin Street, Floor 10, Ottawa, ON, K2P 1L4, Canada, registered under number 874389-4. The sharing of Your Personal Data with Salt Edge Inc. takes place mainly as automatic collection and processing of Your Personal Data on servers located within the European Economic Area, where we host our software solutions that enable us to provide the Services.

6.2. We may occasionally also share Your Personal Data:

- with regulatory bodies, competent authorities, courts, tribunals and law enforcement agencies, to comply with our legal and regulatory obligations or with any subpoena, enforceable request or other legal process.
- with third parties, such as Your App Provider(s), Gateway Partner(s), Your Account Providers, professional advisers (such as lawyers), law enforcement agencies, courts, tribunals, and regulatory authorities, to investigate any potential violations of the Dashboard Terms and Conditions, or of applicable laws, and/or to enforce our legal rights or to undertake or defend legal proceedings.
- with members of our group or third parties that have or may acquire control or ownership of our business (and with our or their professional advisers), if necessary in connection with a significant corporate transaction or restructuring, including a merger, acquisition, asset sale, initial public offering or in the event of our insolvency. Any such recipient of any of Your Personal Data will be bound by appropriate confidentiality obligations. Our legal basis for such transmission resides in the need to comply with applicable legal and regulatory obligations as well as our legitimate interests to protect, realise and grow the value of our business and assets.

If You would like more information about who we share Your data with and why, please contact us (see Section 15 'How to contact us' below).

7. TRANSFERRING YOUR PERSONAL DATA OUT OF THE EEA COUNTRIES

7.1. We store Your Personal Data processed for the purpose of providing the Services on our own and third-party servers located in the European Economic Area ("EEA"). We take all adequate measures to ensure that Your Personal Data is at all times treated securely and in accordance with this Privacy Policy.

7.2. Depending on the way Your App Provider operates their App, in order for You to be able to receive their services, Your App Provider may retrieve Your Payment Account Data to countries outside the UK and the EEA. We expect that, as Controller, Your App Provider duly informed You of the locations where they keep and process Your Personal Data as part of providing their App to You. Please refer to Your App Provider for more detailed information in this respect.

7.3. Occasionally, to ensure troubleshooting, debugging, support, error-fixing of the Services or addressing Your requests, inquiries and complaints, Your Personal Data may be remotely accessed, viewed and used by the authorised personnel of our subcontractor, Salt Edge Inc., who may be located in third countries in relation to the EEA. In particular, it is expected that such remote access and viewing may be conducted by personnel located in the Republic of Moldova. In case we have to resort to transfers of Your Personal Data to third countries in relation to the EEA, we will do so in compliance with the requirements of the Data Protection Laws designed to ensure the privacy of Your Personal Data.

Under the Data Protection Laws, we can only transfer Your Personal Data to other countries, where there is an adequacy decision in respect of such country or where we ensure that there are appropriate safeguards in place, together with enforceable rights and effective legal remedies for You as a data subject. Should we resort to such a transfer, we will do so on the basis of an adequacy decision or (where it is not available) on the basis of legally approved standard data protection clauses recognised or issued further to Article 46(2) of the EU GDPR or UK GDPR.

7.4. As there is no adequacy decision in respect of the Republic of Moldova, we have taken appropriate safeguards under the Data Protection Laws to ensure that Salt Edge Inc. treats any of Your Personal Data they may remotely access from outside the EEA securely and in accordance with this Privacy Policy at all times.

7.5. If You would like further information about whether Your Personal Data may be subject to transfers outside the EEA and the safeguards we put in place in connection with such transfers, please contact us (see Section 15 'How to contact us' below).

8. SPECIAL CATEGORIES OF PERSONAL DATA

The Data Protection Laws establish special rules for the processing of Special Categories of Personal Data, which include: Personal Data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data and biometric data processed for the purpose of uniquely identifying an individual; data concerning an individual's health, sex life or sexual orientation. We do not require to process Special Categories of Personal Data in order to provide the Services to You and we do not deliberately solicit, access, collect or process any such data. Special Categories of Personal Data may be occasionally and incidentally contained in the Payment Account Data that we retrieve from Your Payment Account(s). Insofar as this may happen, please be assured that we do not analyse, filter, map, or perform any other processing to identify or single out Special Categories of Personal Data. You are requested at all times to refrain from voluntarily providing to us any Special Categories of Personal Data by any means of communication, unless we expressly request You to provide such data.

9. YOUR RIGHTS UNDER DATA PROTECTION LAWS

9.1. Under the Data Protection Laws, You have the following rights, which You can exercise free of charge:

- a. the right to be informed: You have the right to receive fair processing information about Your Personal Data processed by us, including, without limitation, the recipients or categories of recipients to whom the Personal Data has been or will be disclosed, in particular transfers to recipients in third countries or international organizations, and the appropriate safeguards relating to such transfers;
- b. the right of access: You have the right to obtain: (i) confirmation that Your Personal Data is being processed, and (ii) access to such Personal Data;
- c. the right to rectification: You are entitled to have Personal Data rectified if it is inaccurate or incomplete;
- d. the right to erasure (also known as "the right to be forgotten"): You have the right to request the deletion of Your Personal Data when there is no compelling reason for its continued

processing or, where Your consent is the legal basis for processing, You withdraw Your consent to such processing;

- e. the right to restrict processing: You can demand from us to restrict the processing of your Personal Data in certain situations: such as when You contest the accuracy of the data or where You object against the processing and await for us to verify whether we have overriding legitimate interests to continue to process Your data. In such cases, our processing of Your Personal Data will be restricted to storage, processing for the establishment, exercise or defence of legal claims, for reasons of important public interest and for the protection of the rights of another person;
- f. the right to data portability: You may request to receive free of charge a copy of Personal Data stored in our systems in a structured, commonly used and machine-readable format, or have us transmit the data directly to another organization, if this is technically feasible;
- g. the right to object: You have the right to object to (i) processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); (ii) direct marketing (including profiling);
- h. rights in relation to automated individual decision-making: You have the right to demand that You are not subject to decisions that legally or otherwise significantly affect You, and which are based solely on automated processing of Your Personal Data (without human involvement). Such automated processing may consist of profiling, which aims to evaluate, analyse or predict certain personal aspects in Your respect;
- i. the right to lodge a complaint with a supervisory authority: You have the right to lodge a complaint about Salt Edge's data protection or privacy practices, or the exercise of any of Your rights with respect to Your Personal Data, with Your local supervisory authority;
- j. the right to withdraw consent: provided that Your consent is the legal basis for processing, You may withdraw Your consent to our processing of Your Personal Data at any time. You may also withdraw your GDPR Consent at any time by contacting us or by using the consent management tools available in the Dashboard.

9.2. If You would like to exercise any of those rights, please:

- write to us – see below Section 15 'How to contact us'; and
- let us know what right You want to exercise and the information to which Your request relates; and
- provide information which You reasonably consider enough to identify yourself.

9.3. We will endeavor to respond to any requests submitted by You in the manner and as set forth in the Data Protection Laws. Where Your requests for exercising Your rights under the Data Protection Laws are manifestly unfounded or excessive, in particular because of their repetitive character, or further copies of Personal Data undergoing processing are requested, we may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested.

10. DATA RETENTION AND DELETION

10.1. Salt Edge will retain Your Personal Data for no longer than strictly necessary for the purposes for which such Personal Data is collected and processed. The retention period depends on the requirements of the applicable laws or regulations we must comply with, the legal bases and the purposes of the collection and processing of Personal Data.

We will delete Your Personal Data from our production systems:

- a. in their entirety, when our agreement with You for the provision of the Services is terminated in accordance with the Dashboard Terms and Conditions or when You validly exercise Your right to be forgotten under the applicable Data Protection Laws. As a result of the deletion, Your Payment Account Data and connections to Payment Account(s) associated with Your use of the Services will be deleted and excised permanently from our production systems. Further use of the Services by You will be impossible.
- b. in the part relating to a specific connection to Your Payment Account(s), when (i) such connection is deleted either by You or by Your App Provider, or (ii) automatically, if no data refreshes were requested by You or Your App Provider for more than 180 days. As a result of the deletion, this specific connection to Your Payment Account(s) and Your Payment Account Data will be deleted and excised permanently from our production systems. Further use of the Services by You via such connection will be impossible.

10.2. We will delete from our production systems the IT Identifiers associated with any particular connection(s) to Your Payment Account(s) within six (6) months after the deletion of the relevant connection(s).

10.3. Regardless of the above, Salt Edge will retain Your Personal Data or portions thereof:

- i. contained in the Payment Account Data and relevant IT Identifiers and your IP address in backup files on our backup servers for a period of up to one (1) month from the date of deletion from the production systems, in accordance with general internal retention procedures.
- ii. contained in the relevant IT Identifiers and Session Information in log files in order to: (i) comply with the requirements of the applicable laws or regulations, (ii) exercise or defend (ongoing) legal claims, and (iii) meet audit or statutory requirements. The retention period for Personal Data retained in log files will be a minimum of five (5) years from the date of deletion from the production servers, or such longer period as required by the applicable laws, unless subject to statutory or regulatory change.

10.4. Backups and log files containing Personal Data are stored on servers separate from our production servers, using strong asymmetric encryption. The files are not actively processed and are not accessible to personnel in the ordinary course of business operations. All Personal Data retained in backup files and log files will be automatically deleted after the retention period has elapsed and until such deletion will be treated in accordance with the terms of this Privacy Policy.

10.5. We will retain Your Identification and contact data in our internal systems for a period of at least six (6) years from the date of submission or receipt, as applicable, of the last of the replies in the communication thread to resolve the respective enquiry, request or complaint.

10.6. We will retain Your Personal Data in our internal systems, to the extent such Personal Data is part of Salt Edge's records generated by applying know-your-customer and anti-money laundering checks, including, without limitation, copies of identity documents, conducted monitoring and analyses, information obtained by electronic identification means, as required for Salt Edge to comply with applicable anti-money laundering, counter-terrorist financing and similar regulatory requirements. The period of such retention shall be a minimum of five (5) years from the date of deletion of Your User Account or last use of the Services based on one-day AIS Consent, unless otherwise provided by applicable laws or unless competent authorities extend such period in accordance with applicable laws.

11. PERSONAL DATA SECURITY

11.1. We are committed to maintaining the confidentiality, integrity and security of Your Personal Data. We employ advanced security techniques to safeguard Personal Data against accidental loss, unauthorized access, use and/or disclosure. We rigorously limit access to Personal Data to those who have a genuine need to access it and our databases are both physically and logically protected from general employee access. We carefully select the individuals privileged with access to Personal Data in accordance with our internal security policies and practices, and each such individual is bound by confidentiality obligations. We enforce physical controls on our premises. Security personnel monitor our systems 24/7. Access to our systems requires multiple levels of authentication. To maintain the security of online sessions and protect our systems from unauthorized access, we use, among others, a combination of firewall barriers, encryption techniques and authentication procedures. We test our systems for any failure points that might allow hacking. We are routinely verified for our use of encryption technologies and audited for our privacy practices. We regularly review our privacy and security practices and adapt them as necessary to deal with new regulatory requirements, changes in legislation and/or security standards.

11.2. We ensure that we apply adequate contractual (including data protection, confidentiality, and security provisions) and other technical and organisational measures with subcontractors that we may engage from time to time in connection with the provision, operation, security and/or maintenance of the Services. We will restrict access, disclosure and/or transfer of Personal Data to subcontractors to what is strictly necessary for the performance of their contractual obligations towards us and will ensure that each subcontractor complies with the provisions in this Privacy Policy.

11.3. Although we take appropriate measures to ensure that Your Personal Data is treated and stored securely, unfortunately, the sending of information via the Internet is not totally secure and on occasion such information may be intercepted. Therefore, we cannot guarantee the security of Personal Data that You choose to voluntarily send to us via electronic means. We expressly disclaim all liability for any interception or interruption of any Internet transmissions sent by You or any resulting losses of, or changes, to data, including Personal Data.

12. NOTIFICATION OF PERSONAL DATA BREACH

If a security breach causes an unauthorized intrusion into Salt Edge's systems, software or networks that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Salt Edge ("**Personal Data Breach**"), we will notify the relevant Supervisory Authority(ies) unless the Personal Data Breach is unlikely to result in a risk

to the rights and freedoms of affected users. Salt Edge will report the Personal Data Breach to the relevant Supervisory Authority without undue delay after having become aware of it and in any case within the timeframes as provided for in the applicable Data Protection Laws. When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of affected users, or if required by the relevant Supervisory Authority, we will also communicate the Personal Data Breach to the affected users without undue delay.

13. COOKIES NOTICE

13.1. A cookie is a small data file placed on a browser or device (such as computer or mobile phone) when it is used to access a service. Cookies or similar technologies may be used for many purposes, including without limitation remembering You and Your preferences and tracking Your access and use of information technology services. Cookies work by assigning a number to users that has no meaning outside of the assigning website or application.

13.2. We use session cookies and persistent cookies when You use the Services. These types of cookies are essential to the operation of Dashboard and the provision of Services. Salt Edge uses them for technical purposes such as verifying the origin of requests, distributing requests among multiple servers, authenticating You and determining what functionality of the Services You are allowed to access. The session cookies are stored in temporary memory and are not retained after You close the browser. Session cookies do not collect information from Your computer. They are used to identify the session during which You interact with our systems only for the duration of that session. The persistent cookies are set with an expiration date and are stored on Your hard drive until they expire, or You delete them. The persistent cookies we use expire within an hour from the last time You access our systems in any given session of interaction. We use these cookies to remember for a short while Your preferences in terms of device theme settings (light/dark) and a presumably more convenient language of the interface; as well as to remember Your App Provider who redirected You to our systems, to ensure that You are redirected back to them when You finish Your interaction with us. We do not collect any Personal Data in our cookies. The cookies we use do not identify You as an individual. All the cookies we use are first-party cookies. We do not use third-party cookies to provide the Services, nor do we use analytical or advertising cookies or social media plugins.

13.3. You can disable or control cookies by setting a preference within Your web browser or on Your device. Thus, if You do not wish that cookies are used in Your respect, You can restrict or limit the use of cookies at the individual browser or device level. However, since the cookies we use are necessary for the provision of the Services to You, if You choose to disable cookies some features of the Services may not function properly or we might not be able to provide the Services to You at all. For detailed guidance on how to control, manage and delete cookies, You are advised to visit <https://www.aboutcookies.org/>.

14. PRIVACY POLICY UPDATE

We may change this Privacy Policy from time to time. When we do so, we will post an appropriate update notice at the top of this Privacy Policy page. You are advised to print a copy of this Privacy Policy for reference and revisit it from time to time to ensure that You are aware of any changes.

15. HOW TO CONTACT US

If You have any questions, comments or feedback regarding this Privacy Policy or our collection, use, disclosure or processing of Personal Data, or any other privacy or security concern, please address them to us using the following contact details:

Our contact details	Our Data Protection Officer's contact details
Mailing address: 2nd Floor Amba House, 15 College Road, Harrow, HA1 1BA, England, United Kingdom Email: privacy@saltedge.com	Mailing address: 2nd Floor Amba House, 15 College Road, Harrow, HA1 1BA, England, United Kingdom Email: dpo@saltedge.com