

# **Privacy Policy**

## **for the use of Account Information Services for indirect customers of Salt Edge and Payment Initiation Services**

provided by fino run GmbH

### **§ 1 Preamble**

- 1.1. fino run GmbH (registered address: Universitätsplatz 12, 34127 Kassel, Germany; registry court: Kassel; registry number: HRB 17459) (“fino”, “we” or “our”) is an account information and payment initiation service provider licensed by the Federal Financial Supervisory Authority in Germany and registered in the Payment Institutions Register under ID 150228. fino is responsible for the provision of account information services (“AIS”) and/or payment initiation services (“PIS”) to you. fino acts as a data controller with respect to your personal data processed in connection with the provision of AIS and/or PIS.
- 1.2. fino outsources certain parts of the provision of AIS and PIS to Salt Edge Limited (registered address: 71-75 Shelton Street, London WC2H 9JQ, England; registration number: 11178811) (“Salt Edge”). Salt Edge has been appointed by fino as its data processor in accordance with the applicable data protection and privacy laws. Salt Edge will be processing your personal data in connection with the provision of fino’s AIS and PIS subject to the terms of this Privacy Policy for the use of Account Information and Payment Initiation Services (“Privacy Policy”).
- 1.3. This Privacy Policy describes and summarizes the policies and procedures employed by fino with respect to the collection, use, storing, processing, disclosure, sharing, transfer and protection of personal data supplied, made available or acquired through your use of the AIS and/or PIS provided by fino.
- 1.4. With respect to the processing activities carried out separately by Salt Edge in connection with the provision of supplemental services related to AIS (such as provision of, as applicable, an end-user dashboard or widget displaying an overview of the retrieved payment account data; data enrichment; consent management functionalities and other value-added services), the respective privacy policy of Salt Edge, presented to you during the end-user flow, will apply.

### **§ 2 Collection and use of personal data**

- 2.1. When you use the AIS and/or PIS (together, “fino Services”) we will collect information, including personal data, for the purpose of providing, maintaining, protecting and improving the fino Services, as well as complying with applicable laws or regulations. fino collects personal data primarily in four (4) ways:
  - (a) Information you supply to us directly when using the fino Services:

- In accordance with regulatory requirements applicable to fino with respect to anti-money laundering, financing of terrorism and related customer identity, status and operations checks, you may be required from time to time to provide your personal data in order to establish matters such as identity, affiliation, public exposure, ownership of your payment account(s), purpose of transactions and origin of funds on your payment account(s). Such personal data may include, without limitation, name, date of birth, residence address, citizenship, gender, copies of identity documents and other proof of identity or residence.
- When using fino Services, you will have to authenticate yourself with your personalized security credentials towards your payment service provider that provides and maintains your payment account (“Account Provider”). Depending on the authentication flow supported by your Account Provider, in some rare cases we may have access to your personalized security credentials, which we will use in an encrypted way solely in order to establish a secure connection to your payment account and transmit initiated payment orders to the respective Account Provider (for PIS) or retrieve the associated payment account data (for AIS).
- When using PIS, you may manually input certain data in the payment order form, including, but not limited to, payment order details (amount, date, description, currency, category of payment transaction).
- When you contact us with respect to any issues relating to the fino Services, you may voluntarily provide personal data such as: name, email address, phone number and financial data. When you voluntarily submit personal data with your enquiry or request, we will process any such personal data in accordance with this Privacy Policy.

(b) Information collected from your Account Provider:

Following the initiation of a payment order on your behalf through the PIS, your Account Provider will return information on the status of the initiated payment order, as well as associated transaction data that may include personal data (e.g., payment account holder name and IBAN).

In order to provide AIS to you, we will access your payment account held by the respective Account Provider in read-only mode based on your consent in order to retrieve, use, store and process the associated payment account data.

(c) Information received from Partner:

In order to initiate a payment order we will receive from the respective Partner the payment order details, generated from your interaction with the Partner’s website, application or platform for the purpose of making payments directly from your payment

account, and which may include personal data, such as, without limitation, payee's account number, sort code, BIC, IBAN or unique identifier, as applicable.

When you start using the AIS or PIS, we may receive your email address, full name and type of your payment account from the respective Partner that redirects you to the fino Services.

Under certain circumstances, some of the information (such as your full name, email address, date of birth, residence address, type of payment account – own, shared or legal, etc.) required by fino before you commence using AIS and/or PIS in order to comply with applicable anti-money laundering and terrorist financing regulations and perform related customer identity, status and operations checks as prescribed by law, may be provided to us by the relevant Partner.

For the purposes of this Privacy Policy, "Partner" means the third party that operates a website, application or platform via which it provides certain services or distributes and offers for sale certain products or goods, in connection with which you are using the fino Services.

- (d) Information collected through your use of the fino Services (by means of session information, cookies and web beacons): please refer to § 8 Log files and Cookies for further details.
- 2.2. The personal data collected in accordance with paragraph 2.1 above will be used for the provision of the fino Services to you and thus, under Article 6.1(b) GDPR the legal basis for processing your personal data is the performance of a contract to which you are a party, particularly the fulfillment of the service contract existing between you and us according to the General Terms and Conditions for the Utilization of fino Services.
- 2.3. All personal data will be collected according to the principle of data minimization and limited to what is reasonably necessary for the provision of fino Services. You are neither legally nor contractually obligated to provide or make available your personal data to us. If you decide not to supply your personal data, we will not be able to provide you the respective fino Services (AIS or PIS), partially or entirely.
- 2.4. We may use the collected personal data for the following purposes:
- (a) to provide, maintain, administer, support, protect and improve the fino Services;
  - (b) to comply with legal obligations to which fino is subject and meet the regulatory compliance requirements set forth in the applicable laws;
  - (c) to provide the status of the initiated payment order and, if such information is returned by your Account Provider, the payment account holder name and IBAN to your Partner (in case of PIS);
  - (d) to provide customer support;
  - (e) to handle and process enquiries submitted by you;

- (f) to send system alert messages and mandatory notifications relating to your use of the fino Services;
- (g) to enforce compliance with the General Terms and Conditions for the Utilization of fino Services and, as applicable, the Terms and Conditions for Account Information Services for indirect customers of Salt Edge or the Terms and Conditions for Payment Initiation Services;
- (h) to investigate any illegal activity or wrongdoing in connection with the fino Services;
- (i) to protect the rights, property and safety of users, fino and related third parties;
- (j) to troubleshoot, investigate and fix service-related errors. In such cases, your personal data may be visible to and/or accessed by our authorized technicians, IT staff and/or system administrators; and
- (k) to respond to your requests for exercising your rights under the applicable data protection and privacy laws.

2.5. In connection with the provision of the fino Services, the following personal data may be collected:

(a) For AIS:

- payment account details (such as account name, IBAN, balance, currency);
- transactions details (such as transaction amount, currency, date, description); and
- account holder information (such as name, address, email, phone number).

(b) For PIS:

- details of each initiated payment order (such as date, amount, currency, status, description, payee details)

(c) For AIS and PIS:

- Personalized security credentials (you may be required to supply your payment account credentials depending on the end-user journey implemented by your respective Account Provider);
- Personal data provided to fino as part of the Know-Your-Customer verification pursuant to paragraph 2.1(a) (such as full name, date of birth, residence address, citizenship, gender, copies of identity documents and other proof of identity or residence);
- Session information stored in the technical log files during your interaction with the fino Services, such as your IP address and device information (e.g., browser type and version, operating system and version, user agent, device model and geolocation data) to the extent that such information qualifies as personal data under the applicable data protection and privacy laws.

### § 3 Duration of storage

- 3.1. We will store your personal data for no longer than strictly necessary for the purposes for which such personal data has been collected and processed. The retention period depends on the requirements of the applicable laws or regulations fino must comply with, the purposes of the collection and processing of personal data, the type of the provided fino Services (one-off or long-term) and the legitimate interests of fino to establish, exercise or defend our legal rights.
- 3.2. We will delete your personal data from our production servers when:
- (a) the provision of fino Services is terminated under, as applicable, the Terms and Conditions for Account Information Services for indirect customers of Salt Edge or the Terms and Conditions for Payment Initiation Services. For clarity, (i) one-off AIS provided to you on a one-time basis are terminated at the latest at the end of the day following the day on which you have given the consent under the Revised Payment Services Directive (“PSD2”) associated to that instance of AIS provision and (ii) PIS are terminated once the initiation of the respective payment order is completed (i.e., it has been transmitted to your Account Provider);
  - (b) in case of long-term AIS, your contract with fino is terminated in accordance with the Terms and Conditions for Account Information Services for indirect customers of Salt Edge; or
  - (c) you exercise the right to be forgotten or, where consent under the General Data Protection Regulation (“GDPR”) is the legal basis for the processing of your personal data, you withdraw such consent.
- 3.3. As a result of the deletion pursuant to paragraph 3.2 above, your personal data will be deleted and excised permanently from our production servers and further use of the fino Services by you will be impossible. Notwithstanding anything to the contrary in this Privacy Policy, we will retain your personal data or portions thereof:
- (a) in backup files on our backup servers for a period of up to one (1) month from the date of deletion from the production servers in order to ensure compliance with internal business continuity and disaster recovery procedures; and
  - (b) in technical log files and audit 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.
- 3.4. Backups and log files containing personal data are stored separately from the production servers. All personal data retained in backup files and log files will be treated in accordance with the terms of this Privacy Policy for as long as it is retained before

being automatically deleted after the retention period has elapsed. Backup files are stored using strong asymmetric encryption and our authorized personnel don't access such files in the ordinary course of business operations, nor will we actively process any personal data retained in backup files anymore.

#### **§ 4 Personal data security**

- 4.1. All data traffic between your browser or end device and the servers used in connection with the provision of fino Services is encrypted. For this purpose, a modern transmission method, at least TLS protocol 1.2 (Transport Layer Security protocol), is used. This ensures that all data is transmitted in encrypted form and is protected from manipulation and unauthorized access by third parties during transmission.
- 4.2. We are committed to maintaining the confidentiality, integrity, availability and security of the personal data of our users. In this respect, our technical and organizational measures conform to the requirements set forth in PSD2 and GDPR. We employ advanced security techniques to safeguard personal data against unauthorized access, use and/or disclosure. To maintain the security of online sessions and protect our systems from unauthorized access, we use a combination of firewall barriers, encryption techniques and authentication procedures, among others. Access to our systems requires multiple levels of authentication, including biometric recognition procedures. Security personnel monitor the systems 24/7. Our databases are both physically and logically protected from general employee access. We also enforce physical controls on our premises. The technical and organizational measures that we employ are routinely verified pursuant to internal policies and procedures and by external parties.
- 4.3. The application servers used in connection with the provision of fino Services are hosted in ISO 27001 certified data centers in Germany.

#### **§ 5 Use of non-personal data**

- 5.1. We may generate anonymous data derived from or based on personal data collected from you or acquired from your use of the fino 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 fino Services ("Anonymized Aggregated Data"). We may use such Anonymized Data and Anonymized Aggregated Data for various business purposes, including, but not limited to:
  - (a) providing, maintaining, supporting, monitoring and improving the fino Services;
  - (b) conducting analytical research, compiling statistical reports and performance tracking;
  - (c) developing and/or improving other related services and products; and
  - (d) sharing such Anonymized Data and Anonymized Aggregated Data with our affiliates, agents and/or subcontractors.

## § 6 Disclosures and transfers

6.1. By using the fino Services, you consent to the transmission or disclosure of your personal data to our service providers as set out below, which we carefully select and use within the framework of our contractual relationships. The transfer or disclosure of your personal data takes place in order to be able to perform the fino Services and only contains the data reasonably necessary for this.

6.2. Disclosure and/or transfer to subcontractors:

fino has put in place adequate contractual (including data protection, confidentiality and security provisions) and other technical and organizational measures with subcontractors that fino may engage from time to time in connection with the provision, operation, security and/or maintenance of the fino Services or part thereof. fino will ensure that each subcontractor complies with the provisions in this Privacy Policy. At the date of this Privacy Policy fino engages Salt Edge as subcontractor.

6.3. Disclosure and/or transfer to data processors:

fino may disclose and/or transfer personal data to data processors engaged by fino to carry out the processing of personal data on fino's behalf in connection with the provision of fino Services. fino will ensure that any engaged data processor provides sufficient guarantees that appropriate technical and organizational measures are implemented and that processing of personal data by the data processor will meet the requirements set forth in this Privacy Policy and the applicable data protection and privacy laws. If processing of personal data by the data processor will involve transfer to a third country, such transfer will be subject to articles 45 and 46 of the GDPR and will take place either (i) on the basis of an adequacy decision by the European Commission, or (ii) by entering into the standard contractual clauses adopted by the European Commission in effect as at the transfer date and, where required by applicable regulations, subject to fino conducting an appropriate assessment of the adequacy of the level of protection of personal data in the relevant third country and concluding on the sufficiency of such protection. At the date of this Privacy Policy fino engages Salt Edge as its data processor.

6.4. Disclosure to your Account Provider:

In order to provide the fino Services fino will disclose to your respective Account Provider certain personal data (particularly, your personalized security credentials (where applicable), your payment order details (for PIS) and in certain cases, depending on the Account Provider, your payment account number).

6.5. Disclosure by sharing with third parties:

(a) with your Partner:

In case of PIS, we will share the status of the initiated payment order and, if such information is returned by your Account Provider, the payment account holder name and

IBAN with your Partner. Such Partner, as the receiving party, will act as an independent data controller with respect to the personal data so shared. Therefore, the Partner is solely and severally responsible for complying with its obligations as data controller as set forth in the applicable data protection and privacy laws after receiving such data from fino.

(b) with Salt Edge:

In case of AIS (both long-term and one-off), we will disclose by transmission the retrieved payment account data associated with your payment account(s) with Salt Edge in order for them to provide you the supplemental AIS-related services as set out in paragraph 1.4 above. Salt Edge, as the receiving party, will act as an independent data controller with respect to the personal data so transmitted. Therefore, Salt Edge is solely and severally responsible for complying with its obligations as data controller as set forth in the applicable data protection and privacy laws after receiving such data from fino.

#### 6.6. Disclosure for legal reasons:

fino may disclose personal data without your consent when we believe in good faith that the disclosure of such information is reasonably necessary or appropriate:

- (a) to comply with the applicable data protection and privacy laws, any subpoena, enforceable request from the competent authorities, or other legal process;
- (b) to enforce our rights against you or in connection with a breach by you of the General Terms and Conditions for the Utilization of fino Services, including investigation of potential violations;
- (c) to help detect, curb or investigate fraud or other prohibited or illegal activities that affect or hurt the interests of fino or third parties;
- (d) to help fino comply with a legal obligation to which we are subject, or accounting or security requirements, in which case fino may disclose such information to its auditors, professional consultants, accountants and/or legal advisors.

In all the foregoing cases, fino will disclose personal data only as required or permitted by the applicable data protection and privacy laws.

### **§ 7 Rights of the data subjects**

7.1. We guarantee your right to informational self-determination and the protection of your personal rights when using the fino Services. Taking into account the nature of the processing and the type of personal data processed, you have the right to exercise the following rights as set forth in the GDPR:

- (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;

- (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 (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 the consent is the legal basis for processing under GDPR, you withdraw consent to such processing;
  - (e) the right to restrict processing: you have the right to block processing of your personal data on the grounds specified in the GDPR;
  - (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), and (iii) processing for purposes of scientific/historical research and statistics;
  - (h) rights in relation to automated decision-making and profiling: you have the right to object to processing of personal data for the purposes of automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual);
  - (i) the right to lodge a complaint with a supervisory authority: you have the right to lodge a complaint about our data protection or privacy practices, or the exercise of any of your rights with respect to your personal data, with your local supervisory authority; and
  - (j) the right to withdraw consent: provided that the consent is the legal basis for processing under GDPR, you may withdraw consent to the processing of your personal data at any time.
- 7.2. You may exercise any of the foregoing rights at any time by contacting us at [privacy@saltedge.com](mailto:privacy@saltedge.com). We will endeavor to respond to any requests submitted by you in the manner and as set forth in the GDPR. Where your requests for exercising your rights under GDPR are manifestly unfounded or excessive, in particular because of their repetitive character, or further copies of the 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.

## § 8 Log files and Cookies

8.1. Each time the fino Services are used, data about this process is automatically recorded in a log file. The collected information relates to, without limitation: (i) which fino Services are being used, (ii) all the areas within the fino Services that you visit, (iii) the time of day when you access and use the fino Services, (iv) actions taken by you when using and interacting with the fino Services, (v) which fino Services or parts thereof generate error messages, and (vi) your browser, operating system, geolocation data (where available) and IP address. All personally identifiable information collected through your use of the fino Services is treated as personal data in accordance with the terms of this Privacy Policy. The information collected in such a way will only be used for the following purposes and will not be passed on to third parties:

- (a) Prevention, detection and investigation of fraud, illegal activities and criminal acts;
- (b) Search for the root cause of possible server problems;
- (c) Ensuring steady performance of the fino Services and improving the user experience;
- (d) Analysis and troubleshooting of technical errors;
- (e) Maintenance of the underlying systems;
- (f) Ensuring network and system security;
- (g) Protection against misuse (e.g., detection and defense against hacker attacks);
- (h) Handling, processing and responding to your requests and inquiries;
- (i) Anonymization and aggregation of the collected data (i.e., in such a manner that the data subject is not or no longer identifiable) for compiling statistical reports and analysis;
- (j) Optimization and improvement of fino Services and underlying systems.

8.2. The legal basis for collecting and processing your personal data as set forth in this § 8 is based on Art. 6(f) GDPR and the legitimate interests (described in paragraph 8.1 above) pursued by fino as the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child. We collect the information described in paragraph 8.1 above automatically as part of our technical log files or other metadata, as well as through the use of cookies (first-party cookies).

8.3. Information collected by cookies:

- (a) A cookie is a data file placed on a device 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 to a

service. Cookies work by assigning a number to users that has no meaning outside of the assigning website or application. We use cookies for various purposes, including, without limitation, analyzing trends, gathering statistical data, improving user experience and the overall quality of the fino Services and tracking your movements when interacting with the fino Services. We encode and encrypt the cookies so that only we can interpret the information stored in them. Cookies can be disabled or controlled by setting a preference within your web browser or on your device. Thus, if you do not want information to be collected through the use of cookies, you can restrict or limit the use of cookies at the individual browser or device level. However, if you choose to disable cookies some features of the fino Services may not function properly or we may not be able to customize the delivery of information to you. For detailed guidance on how to control, manage and delete cookies, you are advised to visit <https://www.aboutcookies.org/>.

- (b) First-party cookies: We use session cookies and persistent cookies when you use the fino Services. These types of cookies are essential to the operation and provision of fino Services. The session cookie is stored in temporary memory and is not retained after the browser is closed. Session cookies do not collect information from your computer. They store information in the form of a session identification that does not personally identify you. The persistent cookies are set with expiration date and are stored on your hard drive until they expire or you delete them. We do not collect any personal data in the session and persistent cookies. We use session and persistent cookies for technical purposes, including but not limited to verifying the origin of requests, distributing requests among multiple servers, authenticating you and determining what functionality of the fino Services you are allowed to access.

## **§ 9 Links to external providers**

The fino Services may include links to, or otherwise direct your attention towards, websites operated and controlled by third parties (including without limitation Partners and Account Providers) and not by fino. Such links are provided solely for your convenience and informational purposes. The inclusion of any link does not imply an association, support, endorsement, consent, examination, or approval by fino of such third party and third-party website (including without limitation any content on such third-party website). We shall not be liable for the information and content contained in any third-party website or for your use of or incapacity to use such website. Access to any third-party website is at your own risk, and you must be aware of the fact that linked websites have terms and privacy policies different from ours and fino does not control them. If you decide to provide any personal data when accessing such links or using the services provided by such third parties, the respective third parties will be responsible for complying with the obligations set forth in the applicable data protection and privacy laws in respect of any

personal data you submit to them and any processing activities carried out by such third parties on your personal data.

## **§ 10 Privacy Policy update**

fino reserves the right to change this Privacy Policy at any time and from time to time in order to reflect changes in the fino Services, the General Terms and Conditions for the Utilization of fino Services or the applicable laws. If we decide to change this Privacy Policy in the future, we will post an appropriate notice at the top of this Privacy Policy page and/or, in case of long-term fino Services, give you reasonable advance notice by email. Any non-material change (such as clarifications) to this Privacy Policy will become effective on the date the change is posted and any material changes will become effective forty-five (45) days from their publishing. Your continued use of the fino Services after the changes to this Privacy Policy become effective signifies your acceptance of any such changes.

## **§ 11 Data Protection Officer**

If you have any questions about the processing of your personal data or about this Privacy Policy in general, please contact the data protection officer, who is also available to you in the event of any data protection complaints:

fino run GmbH

Data Protection Officer

Universitätsplatz 12, 34127 Kassel

E-Mail: [privacy@saltedge.com](mailto:privacy@saltedge.com)

Kassel, 1 June 2021