

Data Policy and Usage

Data Policy

This policy describes the information we process to support SALVE FINANCIAL HUB and other services, products, and features (abbreviated by SPF) offered by it. In addition, SALVE FINANCIAL HUB complies pursuant to Law 171/2018 of the Republic of San Marino and **EU Regulation 2016/679 (General Data Protection Regulation)** about the protection of personal data, to those who interact with our SPF in different ways.

The data controller for personal data is Salve Financial Hub, headquartered at Via Consiglio dei Sessanta n. 99 – 47899 Serravalle (R.S.M.), and can be contacted through info@salve.sm.

A. What kinds of information do we collect?

A.1. Information and content you provide. We collect the content, communications, and other information the Customer (or through the Customer's profile) provided while using our SPF, including while signing up for an account, editing a profile, creating content, sending messages, uploading documents, entering beneficiary information, communicate with us via available features such as helpdesk or do monetary transactions. This can include information in or about the content the Customer provides. Our systems may automatically, manually, or process the Customer's activities to analyze context and what's in them for the purposes described below.

A.1.1. Compliance and Risk check. We collect from the Customer information such as declared while onboarding or edited and added once the Customer becomes our official user, information of the introduced Beneficiaries by the Customer, information and documents added in relation to the purpose of the Customer's monetary transactions (Invoices, Inspection Letters, Shipping information, or whatsoever)

A.1.2. Customer profile information. We collect from the Customer (which, for the purposes of this section refer to the Customers and its business) identifying information such as name, business name, nature, registry details, addresses, phone number, e-mail address or similar. Depending upon the Services requested by the Customer, we may collect additional KYC Information (Know Your Customer) such as National ID, State ID, or Passport/Visa; citizenship status; Tax ID, third party bank account and transaction information; criminal offenses; credit history; credit score; credit report; dependent or beneficiary name(s); biometric information; and other personal identification numbers, scanned versions of the Customer's business' legal documents or whatever.

A.1.3. Customer's usage. We collect information about how the Customer uses our SPF; and the time, frequency, and duration of activities. For example, we collect logs when a Customer is using and has last used our SPF, viewed contents transactions submitted by the Customer.

A.1.4. Information about transactions made on our SPF. If a Customer uses our SPF for financial transactions, we collect information about the transaction. This includes payment information, such as Customer and Beneficiary's

account and authentication information; and billing, shipping, and contact details.

A.1.5. Device Information To reduce security and breaching risks, we may collect information from and about computers, tablets & phones, and other web--

connected devices our Customer uses to integrate with our SPF, and we combine this information across different devices the Customer uses which includes:

A.1.5.1. Device attributes: information such as the operating system, hardware and software versions, signal strength, available storage space, browser type, app and file names and types, and plug-ins.

A.1.5.2. Device operations: information about operations and behaviors performed on the device, such as whether a window is foreground or background, or mouse movements (which can help distinguish humans from bots).

A.1.5.3. Identifiers: unique identifiers, device IDs, and other identifiers from accounts the Customer uses.

A.1.5.4. Data from device settings: Information that the Customer allows us to receive through device settings, such as access to GPS location, camera, or photos.

A.1.5.5. Network and connections: Information such as the name of the mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and, in some cases, information about other devices that are nearby or on the Customer's network.

A.1.5.6. Cookie data: data from cookies stored on the Customer's, including cookie IDs and settings.

A.2. Purposes and Legal Bases of Processing the Customer Data

The processing of personal data by Salve Financial Hub is carried out for the following purposes and based on the corresponding legal grounds:

A.2.1. Account Management and Service Provision (Art. 5(1)(b) Law 171/2018 and GDPR (Art. 6(1)(b) GDPR – Performance of a Contract):

A.2.1.1. Creating and managing Customer accounts.

A.2.1.2. Access to payment and electronic money services through the SPF.

A.2.1.3. Management of financial transactions.

A.2.2. Legal Compliance (Art. 5(1)(c) Law 171/2018 and (Art. 6(1)(c) GDPR – Legal Obligation):

A.2.2.1. Retention of data for tax and accounting purposes.

A.2.2.2. Compliance with anti-money laundering (AML) regulations and the Central Bank of San Marino's requirements.

A.2.2.3. Responding to requests from competent authorities.

A.2.3. Fraud Prevention and Security (Art. 5(1)(f) Law 171/2018 and (Art. 6(1)(f) GDPR – Legitimate Interest):

A.2.3.1. Monitoring activities to prevent fraud, unauthorized access, or harmful behavior.

A.2.3.2. Analyzing devices and behaviors to differentiate real users from automated activities (bots).

A.2.4. Marketing and Communications (Art. 5(1)(a) Law 171/2018 and (Art. 6(1)(a) GDPR – Consent):

A.2.4.1. Sending newsletters and personalized promotions, subject to explicit consent.

A.2.5. Service Improvement (Art. 5(1)(f) Law 171/2018 and (Art. 6(1)(f) GDPR – Legitimate Interest):

A.2.5.1. Analyzing platform usage to enhance user experience.

A.2.5.2. Conducting market research and developing new features.

A.2.6. Complaint and User Request Management (Art. 5(1)(b) Law 171/2018 and (Art. 6(1)(b) GDPR – Performance of a Contract):

Managing support requests and disputes submitted by users.

A.2.7. Communication: In order to correspond with you, we only use those contact information that the Customer has provided us.

A.3. Data Retention Periods

Personal data will be retained only for as long as strictly necessary to fulfill the purposes for which it was collected unless specific legal obligations require otherwise. For example:

A.3.1. Data from closed accounts: Retained for 10 years in compliance with anti-money laundering regulations and for audit purposes.

A.3.2. Data for marketing purposes: Retained until consent is withdrawn by the Customer.

A.4. How is this information shared?

The Customer information is shared with others in the following ways:

A.4.1. Public information can be seen with the Customer's permission by other clients using SALVE FINANCIAL HUB or through APIs related to the related Banks or Authorities the Customer is communicating with us through the SALVE FINANCIAL HUB.

A.4.2. New owner. If the ownership or control of all or part of our SPF or their assets changes, we may transfer the Customer information to the new owner.

A.4.3 Sharing with Third-Party Partners We work with third-party partners who help us provide and improve our SPF but we don't sell any of the Customer information to anyone, and we never will. We also impose strict restrictions on how our partners can use and disclose the data we provide.

A.4.4. Vendors and service providers. We provide information and content to vendors and service providers who support our business, such as by providing technical infrastructure services, analyzing how our SPFs are used, providing customer service, facilitating payments or conducting surveys.

A.4.5. Legal Inquiries. In order to keep our transparency and assist legal and regulatory entities in fraud monitoring and prevention; compliance with applicable laws & regulations; protecting our and other's businesses against illegal activity; and performing audits; we may deliver Customer information upon inquiries and requests received by authorities.

B. How can the Customer exercise its rights and those of its business?

The data subject may exercise the rights provided by law at any time regarding SALVE Financial Hub S.p.A by submitting a written request using one of the following methods:

a- By registered mail addressed to Salve Financial Hub S.p.A., Via Consiglio dei Sessanta n. 99 - 47899 SERRAVALLE (R.S.M.);

b- By sending an email to: **coo@salve.sm**

Using the same methods, the Customer may also revoke at any time any consent previously given through this Data Policy.

B.1 Right of Access

The Customer may obtain confirmation from Salve as to whether the Customer's Personal Data is being processed and, if so, gain access to Personal Data and the information provided under Art. 15 of the Law and GDPR. This includes, but is not limited to, the purposes of processing, the categories of data involved, the recipients to whom the data may be disclosed, the applicable retention period, and the existence of automated decision-making processes.

B.2. Right to Rectification

The Customer may obtain from Salve Financial Hub, without undue delay, the rectification of any inaccurate personal data concerning the Customer. Additionally, taking into account the purposes of the processing, the Customer may provide a supplementary statement to ensure the data is complete if it is incomplete.

B.3. Right to Erasure

The Customer may request the erasure of its Personal Data on SPF if one of the reasons outlined in Art. 17 of the Law and GDPR apply. For example, if the Personal Data is no longer necessary for the purposes for which it was collected or processed, or if the Customer has withdrawn consent and there is no other legal basis for processing. Please note that the withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. SALVE cannot proceed with the erasure of the Customer's Personal Data if processing is necessary, for instance:

- To comply with a legal obligation;
- For reasons of public interest;
- For the establishment, exercise, or defense of legal claims.

B.4. Right to Restriction of Processing

The Customer may request the restriction of processing of its Personal Data under the circumstances outlined in Art. 18 of the Law and GDPR. For example:

- If the Customer contests the accuracy of its Personal Data being processed;
- If the Customer's Personal Data is required for the establishment, exercise, or defence of legal claims, even if Salve Financial Hub no longer needs it for processing purposes.

B.5. Right to Object

The Customer may object at any time to the processing of its Personal Data once the processing is carried out in the public interest or for the legitimate interests pursued by Salve Financial Hub S.P.A. (including profiling activities), as outlined in Art. 21 of the Law and GDPR. If the Customer exercises this right, Salve Financial Hub will refrain from further processing of the Customer's Personal Data unless there are compelling legitimate grounds for the processing that override the Customer's interests, rights, and freedoms, or if the data is required for the establishment, exercise, or defense of legal claims.

B.6. Right to Data Portability

In compliance with Art. 20 of the Law and GDPR, if the processing of the Customer's personal data is based on consent or is necessary for the performance of a contract or pre-contractual measures, and the processing is carried out by automated means, the Customer may:

- B.6.1.**-Request to receive its personal data in a structured, commonly used, and machine-readable format (e.g., computer or tablet);
- B.6.2.**-Transmit the Customer's personal data to another data controller without hindrance from Salve Financial Hub.

The Customer may also request that Salve Financial Hub S.P.A. transmit its personal data directly to another data controller specified by the Customer, provided it is technically feasible for Salve Financial Hub. In this case, it will be the Customer's responsibility to provide Salve Financial Hub with all the exact details of the new data controller and grant us the necessary written authorization.

B.7.Right to Lodge a Complaint with the Data Protection Authority

Without prejudice to the Customer's right to appeal to any other administrative or judicial authority, if the Customer believes that the processing of its personal data by Salve Financial Hub violates the law and/or applicable regulations, the Customer may lodge a complaint with the competent Data Protection Authority.

C. How do we respond to legal requests or prevent harm?

We access, preserve, and share the Customer's information with regulators, law enforcement, or others:

In response to a legal request (like an AML auditing warrant, search warrant, or court order Subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the country where we register Salve Financial Hub, when we have a good-faith belief that the responses required by law in that jurisdiction and is consistent with internationally recognized standards.

When we have a good-faith belief it is necessary to: detect, prevent, and address fraud, unauthorized use of our SPF, violations of our terms or policies, or other harmful or illegal activity; to protect ourselves, you, or others, including as part of investigations or regulatory inquiries; or to prevent death or imminent bodily harm. To comply with our ethics and remain transparent and accountable to the law, we also retain all information from closed or suspended accounts – although not visible to the public – to be available for 10 years (starting from closure or suspension) for any future legal claims, auditing warrants, or court orders.

D. How will we notify the Customer of changes to this policy?

We'll notify the Customer before we make changes to this policy and allow the Customer to review the revised policy before choosing to continue using our SPF.