VONBAN SWISS AG

PRIVACY NOTICE AND DATA PROTECTION

Date of Issuance: December 2024

VONBAN

Contents

1. INTRODUCTION

Vonban Swiss AG (hereinafter "Vonban", "us", "our", or "we") declare that we are responsible for the processing of any personal data that we collect via our online website www.vonban.ch and online portal www.portal.vonban.ch .

This Privacy Notice & Data Protection explains how we process personal data, in particular in relation to our business activities and through our website and online portal. It is applicable to all individuals in contact with Vonban. It should be read by:

- Potential, current and prospective customers ("users");
- Their shareholders, directors, officers, and employees;
- Other related persons such as representatives, signatories, beneficial owners, beneficiaries, security providers, payment recipients;
- Customers of our users and their staff;
- Vendors, suppliers, counterparts who cooperate with customers of our users and their staff;
- Visitors on our website and users of our online portal.

Additional information about how we process personal data can be found in other documentation, such as General Terms and Conditions, and in separate consent forms.

The Privacy Notice & Data Protection is freely accessible on our online website. By accessing the online website or online portal, you are agreeing to this Privacy Notice & Data Protection and you consent to the use of your data by us as set out below.

We reserve the right to change or amend this Privacy Notice & Data Protection at any time. New or amended versions of the Privacy Notice & Data Protection are considered received when they are made available on our online website.

In case of doubt, the English language version of this Privacy Notice & Data Protection and other supplementary provisions of Vonban shall prevail over translations into other languages. In case you are not able to read and/or understand this Privacy Notice & Data Protection or in case you do not agree to be bound by it, you need to leave the Website.

We comply with the legal provisions of the Swiss Data Protection Legislation, in particular the Swiss Federal Act on Data Protection (FADP), the Ordinance to the Federal Act on Data Protection (DPO), but in some circumstances, we may also be subject to the European General Data Protection Regulation (GDPR). This notice therefore includes references to the GDPR as well.

The Controllers of Data:

Vonban Swiss AG, Nüschelerstrasse 31, 8001 Zurich, Switzerland

Email: info@vonban.ch

Data Protection Officer:

If you have any questions in relation with our processing of your personal data, please do not hesitate to contact us at:

Email: dpo@vonban.ch

2. NATURE OF DATA COLLECTED

Personal data is any information about personal and factual circumstances of a specific or determinable natural person (individual information that is or can be assigned to you as a natural person), and visitors to our online website or online portal, or social media sources linked to www.vonban.ch.

Typically, we collect and process personal data during the course of our commercial relationship. Personal data is processed during any phase of the commercial relationship, and the data vary depending on the group of people.

Personal data is only collected and stored if you provide us with this information yourself (when registering at the contact page of www.vonban.ch or at the registration page of our online portal www.portal.vonban.ch, or in other correspondence/communication, or if you authorize us to obtain this information from publicly accessible sources and registers).

We also process personal data that are generated or transmitted based on the use of products or services, or that we have rightfully received from public institutions (e.g., UN and EU and OFAC Sanctions lists) or from other sister companies of Vonban. We may also process personal data from publicly available sources (trade registers, press, and online sources).

You may also provide us with personal data about yourself or relating to other third parties involved in the commercial relationship such as data from authorized representatives, proxies, legal successors, and economic beneficiaries for the commercial relationship. This data may be about co-workers, directors, officers, representatives, signatories, payment recipients, customers, clients, and other related parties, including beneficial owners, and other individuals. This data may be shared using submitted contracts, forms, correspondence, and other documentation, especially when you register to become a user of our services, or during our commercial relationship when you send specific payment instructions and their justification required for AML verification purposes, or when you justify the purpose of a payment receipt.

Whenever you provide information to us, we assume that the data is correct and that you are permitted to share it with us. However, we may not be in direct contact with these individuals and cannot tell them directly about our data processing. It is your responsibility to inform these individuals about our data processing, for example, by pointing them to this Privacy Notice & Data Protection.

The term personal data is understood to refer to the following categories of data:

- **Master Data**
  - Personal data (name, surname, middle name, date of birth, nationality)
  - Contact details and address (physical address, telephone number, email address)
  - Identification information (passport, identity card details)

- Authentication data (specimen of signature)Data from public sources (social security number, tax number/s)

- **Detailed Basic Data:**
  - Information about products and services used (payment transactions data, beneficiaries, currencies, interactions with our online platform)
  - Information about financial characteristics and financial situation (sources of income, sources of wealth/assets, economic background, professional background)
  - Technical data and information about electronic communication with us (record of access and interactions on our online platform)
  - Biometric data as part of our identification process (used to onboard you, carry out identity and age verification including video identification, comply with tax controls, reporting obligations, prevent fraud, assess and manage risks, and learn more about your business as per our Anti-money Laundering requirements)
  - Image and sound files (video or phone recordings).

Vonban may process sensitive personal data, including biometric information, for specific purposes such as identity verification, AML/KYC compliance, and fraud prevention. Such processing will only occur with your explicit consent, as required under relevant rules and regulations. You have the right to withdraw your consent at any time by contacting our Data Protection Officer at dpo@vonban.ch. Withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

Vonban's services and platforms are restricted for individuals under the age of 18. We do not knowingly collect personal data from children without verifiable parental or legal guardian consent. If we become aware that data of a child under 18 has been collected, we will promptly delete such data. Parents or guardians may contact dpo@vonban.ch to request the removal of any information related to their child.

3. PURPOSE OF DATA COLLECTED

We process data in accordance with the provisions of the FADP, DPO, and GDPR for the purposes and based on the following legal grounds:

- To implement pre-contractual measures, or perform a contract, and for the arrangement of our intermediary services, and for order processing
- To fulfill legal obligations including AML compliance
- To act in public interest (e.g., regulatory compliance)
- To comply with tax laws and treaties and reporting obligations
- To manage risk, product development, audits, and security
- To protect legitimate interests (e.g., fraud prevention, defense against threats)
- Based on your consent, which you provided for us to perform and arrange a transaction or based on an order instruction, the disclosure of data to service providers of Vonban or contractual partners of Vonban.

4. AML/KYC INTEGRATION

Personal data collected for Anti-Money Laundering (AML) and Know Your Customer (KYC) purposes will be processed as required by the Swiss Anti-Money Laundering Act (AMLA) and related regulations, including ongoing monitoring and reporting obligations. Users are required to submit accurate KYC documentation and promptly update any changes to their information, as outlined in our General Terms and Conditions (GTC).

5. SOLICITATION DISCLAIMER

All interactions with VONBAN Swiss AG are user-initiated. Vonban does not market or solicit its services in jurisdictions where such activities are restricted. Users confirm accessing Vonban's services voluntarily and acknowledge their responsibility for ensuring compliance with applicable laws.

6. ACCESS TO DATA COLLECTED & DATA RETENTION PERIOD

Access to your data may be obtained by authorized bodies inside and outside of Vonban. Within Vonban, your data can only be processed by employees or departments if this is required to fulfill our contractual, legal, and regulatory obligations, or to protect our legitimate interests.

Commercial confidentiality and data protection rules allow personal data to be accessed for these purposes by Vonban's sister companies, service providers, or other agents.

Processors can include companies categorized as Money Laundering Reporting Officers, Auditors, Bank service providers, Correspondent Banks, IT Services, contractually bound professional consultants, and Accountants.

In addition, recipients of your data in this context could include other financial intermediaries and financial services institutions or comparable bodies to whom we transmit personal data in order to implement the commercial relationship, such as Banks and other payment providers.

When there is an applicable legal or regulatory obligation, public authorities and institutions (for example, supervisory authorities, tax authorities, financial intelligence units) may also obtain your personal data.

In instances where data are transferred outside of Switzerland and the European Economic Area (EEA) ("third countries"), and the GDPR regulations do not deem the country in question to provide an adequate level of security, such data transfer will be carried out using suitable measures, such as recognized data protection clauses. These measures ensure compliance with data privacy provisions. Further information on such measures can be requested from the Data Protection Officer.

If the situation does not permit the use of suitable data privacy provisions for a third country, data will only be transferred as required for the implementation of pre-contractual measures or for the performance of a contract (to comply with statutory obligations outside of the EEA

based on the chosen service or product requested by you), or the processing of a transaction on your instructions. Data will also be transferred to third countries if you have explicitly consented, if it is necessary for public interest (e.g., preventing money laundering), or if it is required by law (e.g., legal reporting obligations).

We process and store personal data throughout the duration of the commercial relationship, unless specific data are subject to deletion obligations, which may result in shorter retention periods. It is important to note that our commercial relationships can last for years.

Vonban is committed to ensuring the confidentiality and security of your personal data. Access to your personal data will only be granted to those who need it to fulfil our contractual, legal, and regulatory obligations, or to protect our legitimate interests.

Within Vonban, personal data will only be processed by employees or departments on a need-to-know basis, and access is strictly controlled. All access to personal data is granted in compliance with the highest standards of confidentiality and data protection principles.

In certain cases, personal data may be shared with Vonban's affiliated companies, service providers, or other third parties (e.g., auditors, money laundering reporting officers, banks, IT service providers, financial intermediaries, and legal professionals). These third parties will only process personal data based on specific contractual agreements that mandate compliance with applicable data protection laws and ensure the confidentiality and security of the data.

We take every reasonable precaution to ensure that any third parties who process personal data on our behalf (data processors) adhere to strict security measures. These include implementing secure data handling practices, data encryption, and access control mechanisms. Regular audits and security assessments are conducted to verify their compliance.

If your personal data needs to be transferred to countries outside of Switzerland and the European Economic Area (EEA), Vonban ensures that such transfers are conducted in full compliance with data protection laws. We are committed to safeguarding the privacy and security of your data when transferred to jurisdictions that do not offer the same level of data protection.

If the destination country does not provide an adequate level of data protection, we will ensure that suitable safeguards are in place. This includes using Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) as provided by the European Commission or other legal instruments that ensure that your data is protected to the same standards as it would be within the EEA.

In cases where suitable legal safeguards cannot be applied, data will only be transferred to third countries when required for the performance of a contract, pre-contractual measures, or other lawful obligations (e.g., fulfilling public interest goals like preventing money laundering). Data will also be transferred if you have explicitly consented to the transfer

You have the right to request detailed information about the safeguards we use to protect your data during international transfers. These details can be provided upon request by our Data Protection Officer (DPO).

Vonban will retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, in line with contractual, legal, or regulatory requirements. Data retention periods will be determined based on the nature of the data and the purposes for which it is processed. This ensures that data is not stored longer than required.

When data is no longer necessary for the purposes outlined in this Privacy Notice & Data Protection or when you withdraw consent, we will take prompt action to securely delete or anonymize your personal data. Data will also be periodically reviewed to ensure compliance with this policy.

Certain data may be retained for longer periods where required by law, regulation, or to meet our legal obligations, such as complying with tax reporting requirements, money laundering regulations, or legal proceedings. In these cases, Vonban ensures that data retention is aligned with the statutory limitation periods.

Vonban adheres to the principle of data minimization, ensuring that only the minimum amount of personal data necessary for fulfilling the intended purpose is collected and stored.

Vonban implements appropriate technical and organizational security measures to protect personal data against unauthorized access, disclosure, alteration, or destruction. These measures include:

Personal data is encrypted both in transit and at rest to ensure that unauthorized individuals cannot access it.

Strict access controls are enforced to limit data access to only those who require it to perform their job functions.

Vonban conducts periodic security audits and vulnerability assessments to identify and mitigate potential threats to data security.

In the event of a data breach, Vonban will notify affected individuals within the timeframes specified under the GDPR (within 72 hours, if feasible) and cooperate with relevant authorities to mitigate the impact.

We require our third-party data processors to implement similar security measures, and we ensure that they undergo regular audits to verify their compliance with data protection laws and security best practices. Where applicable, Vonban also ensures that third-party processors are certified under relevant security standards, such as ISO/IEC 27001, to ensure the robustness of their data protection practices.

Vonban may disclose your personal data to public authorities, such as tax authorities, financial intelligence units, or supervisory authorities, when required by law or regulation. We will take all reasonable steps to ensure that such disclosures are made in compliance with applicable legal frameworks and that the sharing of your personal data is justified

You retain the right to access, correct, or delete your personal data in accordance with applicable data protection laws. You may also object to processing in certain circumstances and request restrictions on the processing of your data.

The retention period also depends on the necessity and purpose of the relevant data processing. If the data is no longer required to fulfil legal and regulatory obligations or to protect our legitimate interests (fulfilment of purpose), or if consent is withdrawn, the data will be periodically deleted unless further processing is necessary due to contractual or legal retention periods, documentation obligations, or the need to preserve evidence during a relevant statutory limitation period.

In the event of a personal data breach that poses a risk to your rights and freedoms, Vonban will notify affected individuals and relevant supervisory authorities within a reasonable timeframe of becoming aware of the breach, as required under the relevant rules and regulations. The notification will include:

- The nature of the breach and categories of data affected;
- Potential consequences of the breach;
- Measures taken or proposed to address the breach and mitigate its adverse effects; and
- Contact details for further information.

Vonban is committed to cooperating with all stakeholders to minimize risks and ensure compliance during such incidents.

Vonban retains personal data only for as long as necessary to fulfil the purposes for which it was collected, including:

- AML/KYC documentation: Minimum of 10 years from the end of the business relationship, as required by Swiss Anti-Money Laundering Act (AMLA);
- Transaction records: 10 years for compliance with tax laws and reporting obligations;
- Marketing data: Until consent is withdrawn or deemed no longer necessary;
- General business communications: Up to 5 years, unless required longer for legal proceedings.

Data no longer needed will be securely deleted or anonymized in compliance with applicable laws.

7. CROSS-BORDER DATA TRANSFERS

Where personal data is transferred to jurisdictions outside Switzerland or the EEA that may not provide an adequate level of data protection as recognized by relevant rules and regulations, Vonban ensures the implementation of appropriate safeguards, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). In cases where such safeguards are unavailable, Vonban will transfer data only:

- With your explicit consent;
- Where necessary for the performance of a contract;
- To comply with legal obligations; or
- For the protection of public interest (e.g., AML compliance).

You may request details about applicable safeguards by contacting the Data Protection Officer.

8. PROFILING AND AUTOMATED DECISION MAKING

We may process personal data using automated methods, particularly for risk management and AML compliance. This may involve analysing your personal data to assess your financial situation, identify potential risks, or evaluate customer characteristics. Automated decision-making may also support audits and regulatory compliance.

If you believe that automated decision-making processes used by Vonban significantly affect you, you have the right to:

- Request a human review of the decision;
- Express your viewpoint; and
- Contest the decision. To exercise this right, please contact our Data Protection Officer at dpo@vonban.ch. Vonban will ensure a prompt review of your request in accordance with applicable regulations.

9. PRIVACY RIGHTS

You have rights under applicable data protection laws, including:

- The right to access, correct, or delete your personal data
- The right to restrict or object to processing
- The right to data portability (receive personal data in a structured, machine-readable format)
- The right to withdraw consent at any time, without affecting prior processing

If you believe your data has been misused, you have the right to lodge a complaint with the competent supervisory authority (in Switzerland, the Federal Data Protection and Information Commissioner - FDPIC).

For any requests regarding your privacy rights, please contact our Data Protection Officer at dpo@vonban.ch.

To process your privacy-related requests (e.g. access, correction, deletion), Vonban may require proof of identity. This ensures that requests are made by the rightful data subject and protects against unauthorized access. Acceptable forms of verification may include a

government-issued ID or equivalent documentation. Vonban will securely handle such information and delete it after verification is complete.

10. CHANGES AND AMENDMNETS

Due to the further development of our online website and online portal, or due to changed legal or official requirements, it may become necessary to change or amend this Privacy Notice & Data Protection. You can access and print out the current data protection statement at any time on the website at www.vonban.ch .

Possible changes and amendments will be published at all timers on our online website.

11. APPLICABLE LAWS AND JURISDICTION

These terms are governed by Swiss law. Disputes shall be resolved in the exclusive jurisdiction of the courts in the Canton of Zurich. Parties may opt for mediation or arbitration under the Swiss Rules of International Arbitration, ensuring a fair and balanced resolution process.

12. DATA PROTECTION AND PRIVACY

Vonban processes personal data in compliance with the General Data Protection Regulation (GDPR) and the Federal Act on Data Protection (FADP). This includes obtaining user consent for processing their personal data, where required, and ensuring that individuals' data protection rights are respected, such as the right to access, correct, and delete their personal data.

Vonban uses cookies and similar technologies to enhance your experience on our website, analyze traffic, and provide tailored content. Cookies may collect information such as browser type, IP address, and pages visited.

By using our website, you consent to the use of cookies in accordance with our Cookie Policy. You may manage your preferences or withdraw consent at any time through your browser settings or the cookie management tool available on our website.

13. EMPLOYEE AND VENDOR DATA

Vonban collects and processes personal data from its employees and vendors strictly for business purposes, including contract performance, payroll administration, regulatory compliance, and workplace management. This data may include:

- Identification details (e.g. name, date of birth, tax ID);
- Employment or contractual information (e.g. role, job description, and performance data);
- Financial details (e.g., salary, bank account for payments).

Vonban ensures confidentiality and processes such data in accordance with applicable data protection laws. Data may be shared with authorized third parties (e.g. payroll providers or tax authorities) under strict contractual obligations.