Bellavista Invest One AG

Privacy and Cookies Policy

of the Crowdlending Platform

www.crowdhive.com

Aegeristrasse 64, 6300 Zug, Switzerland
SRO Membership: VQF (active)

Version 1.2 | Effective date: 06.07.2026

Table of Contents

Part I – General

1. Introduction and Scope

Bellavista Invest One AG (hereinafter the "**Company**") operates an online crowdlending platform accessible at www.crowdhive.com (the "**Platform**"). The Company is committed to protecting the privacy and personal data of all individuals who visit, register on, or otherwise interact with the Platform.

This Privacy and Cookies Policy (the "Policy") describes how the Company collects, processes, stores, shares, and protects personal data in connection with the operation of the Platform. It also explains the rights available to data subjects and the use of cookies and similar tracking technologies.

1.1 Who Is Covered

This Policy applies to all natural persons whose personal data is processed by the Company in connection with the Platform, including:

- Visitors who browse the Platform without creating an account;
- Natural persons who register on the Platform as Investors or Borrowers (collectively, "Users");
- Representatives, beneficial owners, and authorised signatories of legal entities registered on the Platform;
- Any other natural persons whose personal data is processed by the Company in connection with the Platform's operations (e.g. contact persons of Borrowers, guarantors).

1.2 What Is Covered

This Policy covers all personal data processed by the Company through:

- The Platform, including its mobile-responsive web version;
- E-mail, telephone, and other direct communications between the Company and the data subject;
- Third-party tools and services integrated into the Platform (e.g. identity verification providers, payment service providers, analytics tools);
- Public and commercial registers consulted by the Company for due diligence and credit assessment purposes.

1.3 What Is Not Covered

This Policy does not apply to the data processing practices of third-party websites, applications, or services that may be linked to or accessible from the Platform. The Company is not responsible for the privacy practices of such third parties. Users are

encouraged to review the privacy policies of any third-party service before providing personal data.

1.4 Acceptance

This Policy is an information notice within the meaning of Art. 19 FADP and Arts. 13 and 14 GDPR; it does not, of itself, constitute a contractual agreement. By accessing or using the Platform, the data subject acknowledges that they have been informed of the data processing practices described herein. Where specific processing activities require consent, the Company will obtain such consent separately and in a manner that complies with applicable law.

The Company may require the collection of certain personal data to comply with legal obligations (including anti-money laundering and know-your-customer requirements). If a User chooses not to provide such data, the Company may be unable to offer the full range of services available on the Platform.

2. Data Controller

The entity responsible for the processing of personal data described in this Policy is:

Data Controller	Bellavista Invest One AG
Registered Office	Aegeristrasse 64, 6300 Zug, Switzerland
Company Registration No.	CHE-373.552.596
Data Protection Contact	Alena Yudina, Chief Executive Officer (operational contact for data protection matters)
Contact E-mail	compliance@crowdhive.com
Postal Address	Bellavista Invest One AG, Attn: Data Protection, Aegeristrasse 64, 6300 Zug, Switzerland

The Data Protection Contact is the designated point of contact for all enquiries relating to the processing of personal data by the Company. Data subjects may direct any questions, requests, or complaints regarding the processing of their personal data to the contact details specified above.

To the extent that the Company's processing of personal data falls within the territorial scope of the GDPR pursuant to Article 3(2) GDPR, data subjects in the EU/EEA and the competent supervisory authorities may also address the Company's representative in the European Union, as indicated above, on all issues relating to the processing of their personal data (Article 27 GDPR).

Where the Company engages third-party service providers (data processors) to process personal data on its behalf, the Company remains the data controller and is responsible for ensuring that such processors comply with the applicable data protection requirements. A current list of the Company's data processors may be obtained by contacting the Data Protection Contact at the e-mail address specified above.

3. Applicable Legal Framework

The Company processes personal data in compliance with the following legislation:

3.1 Swiss Data Protection Law

As a company incorporated in Switzerland, the Company is subject to the **Swiss Federal Act on Data Protection** (FADP, SR 235.1, as revised and effective from 1 September 2023) and the **Ordinance on Data Protection** (DPO, SR 235.11). These instruments govern the processing of personal data by private persons and federal bodies in Switzerland.

Under the FADP, the Company is required in particular to:

- Process personal data lawfully and in good faith;
- Collect personal data only for a specific and recognisable purpose and process it only in a manner compatible with that purpose;
- Ensure that personal data is accurate and take reasonable steps to correct inaccurate data;
- Implement appropriate technical and organisational measures to protect personal data against unauthorised processing;
- Provide data subjects with adequate information about the collection and processing of their data.

3.2 EU General Data Protection Regulation

To the extent that the Company processes personal data of individuals located in the European Union or the European Economic Area ("**EU/EEA**"), or offers goods or services to, or monitors the behaviour of, such individuals, the **General Data Protection Regulation** (Regulation (EU) 2016/679, "GDPR") applies in addition to the FADP.

The GDPR imposes additional obligations on the Company, including but not limited to:

- The requirement to identify and document a specific legal basis for each processing activity (Article 6 GDPR);
- Enhanced transparency and information obligations (Articles 13 and 14 GDPR);
- The obligation to conduct data protection impact assessments for high-risk processing activities (Article 35 GDPR);
- Restrictions on the transfer of personal data to countries outside the EU/EEA that do not provide an adequate level of data protection (Chapter V GDPR);
- Extended rights for data subjects, including the right to data portability (Article 20 GDPR) and the right to object to processing based on legitimate interests (Article 21 GDPR).

3.3 Interaction Between FADP and GDPR

Where both the FADP and the GDPR apply to a processing activity, the Company will comply with the requirements of both instruments. In the event of a conflict, the Company will apply the standard that affords greater protection to the data subject.

The revised FADP (effective 1 September 2023) has been substantially aligned with the GDPR in many respects. The European Commission has recognised Switzerland as providing an adequate level of data protection for the purposes of Article 45 GDPR. Accordingly, transfers of personal data from the EU/EEA to Switzerland do not require additional safeguards under the GDPR.

3.4 Other Applicable Legislation

In addition to the FADP and the GDPR, the Company's data processing activities may be subject to sector-specific legislation, including:

- The **Swiss Anti-Money Laundering Act** (AMLA, RS 955.0) and related ordinances, which impose obligations regarding the collection, verification, and retention of customer identification data;
- The **Swiss Code of Obligations** (CO, RS 220), which contains provisions on commercial record-keeping and retention periods;
- The **Swiss Telecommunications Act** (TCA, RS 784.10) and the **Ordinance on Telecommunications Services** (OTS, RS 784.101.1), which regulate certain aspects of electronic communications and cookies;
- The regulations of the **VQF (Verein zur Qualitätssicherung von Finanzdienstleistungen)**, the self-regulatory organisation with which the Company is affiliated, which may impose additional requirements relating to the processing and retention of client data.

The Company monitors legislative developments and will update this Policy as necessary to ensure ongoing compliance.

3.5 Data Storage Location

Personal data processed by the Company is stored on servers located in Switzerland. Switzerland has been recognised by the European Commission as providing an adequate level of data protection pursuant to Article 45 GDPR. The Company applies the standards set by the FADP and, where applicable, the GDPR to all personal data it processes, regardless of the data subject's country of residence.

Where the Company engages third-party service providers whose servers are located outside of Switzerland, the Company ensures that appropriate safeguards are in place in accordance with Part III of this Policy.

Part II – Data Processing

4. Categories of Personal Data

The scope and nature of the personal data processed by the Company depends on the capacity in which a data subject interacts with the Platform. The Company distinguishes between the following categories of data subjects and collects the data described below for each category.

4.1 Visitors (Non-Registered Users)

When a natural person visits the Platform without registering or logging in, the Company may automatically collect certain technical data, including:

- IP address;
- Browser type and version;
- Operating system;
- Device type and screen resolution;
- Date, time, and duration of the visit;
- Pages viewed and navigation path;
- Referring URL (the website from which the visitor was redirected to the Platform);
- Country of origin and time zone;
- Cookie identifiers and similar tracking data (as further described in Part V).

This data is collected automatically by the Platform's web server and by third-party analytics tools. It cannot, in most cases, be attributed to an identified individual without additional information.

4.2 Investors

When a natural or legal person registers on the Platform as an Investor, the Company collects and processes the following categories of personal data:

a) Registration data:

- First name and surname;
- Date of birth;
- Nationality;
- Residential address or domicile;
- E-mail address;
- Telephone number.

b) Identity verification (KYC) data:

- Copies of a valid identity document (passport or national identity card), including the Machine Readable Zone (MRZ);
- Photograph of the Investor's face (selfie), captured as part of the identity verification process;

- Biometric data derived from the facial recognition and liveness detection procedures performed by the Company's third-party identity verification provider;
- Proof of address (e.g. utility bill, bank statement);
- Video recording, where video identification is used.

c) Financial and transactional data:

- Bank account details (IBAN, account holder name, name of financial institution);
- Records of deposits, withdrawals, and transfers;
- Investment history and portfolio data (projects invested in, amounts, returns);
- Transaction documents.

d) Due diligence and compliance data:

- Proof of wealth (POW) documentation;
- Proof of funds (POF) documentation;
- Declaration of beneficial ownership (Form A and/or Form K);
- Results of sanctions, PEP, and adverse media screening;
- AML risk classification assigned by the Company.

e) Communication data:

- Records of correspondence between the Investor and the Company (e-mail, in-platform messages, support tickets);
- Newsletter subscription preferences.

Where the Investor is a legal entity, the Company additionally collects the data described above in respect of the entity's authorised representatives, persons with signing authority, and beneficial owners, as well as a commercial register extract and other corporate documentation.

4.3 Borrowers

When a legal person (entity) registers on the Platform as a Borrower, the Company collects all categories of personal data listed in Section 4.2 above, together with the following additional data:

a) Corporate and project data:

- Company name, legal form, and registered office;
- Commercial register extract and company registration number;
- Details of the management team and beneficial owners (including background information);
- Articles of incorporation or equivalent constitutive documents;
- Description and documentation of the project for which financing is sought.

b) Financial assessment data:

- Annual financial statements (balance sheet, income statement, cash flow statement);
- Business plan and financial projections;
- Collateral and guarantee documentation;
- Information on existing liabilities and credit history.

c) External due diligence data:

- Data obtained from debt enforcement registers (Betreibungsregister);
- Credit rating information obtained from credit reference agencies and commercial databases (e.g. CRIF, Creditsafe, Dun & Bradstreet, or equivalent providers);
- Information obtained from other public or commercial registers relevant to the assessment of the Borrower's creditworthiness.

The Company reserves the right to collect additional categories of data where required by law, by the SRO, or where the Company deems it necessary for the proper assessment of risk.

5. Legal Basis for Processing

The Company processes personal data on the basis of one or more of the following legal grounds. The applicable legal basis depends on the nature and purpose of the specific processing activity.

For the purposes of the FADP, the processing of personal data by a private controller does not require a specific legal basis, provided that the data protection principles (Arts. 6 and 8 FADP) are complied with; a justification (consent, an overriding private or public interest, or a statutory basis; Art. 31 FADP) is required only where the processing results in a breach of the data subject's personality rights. The legal bases identified below are accordingly documented in particular for the purposes of the GDPR, where it applies.

5.1 Performance of a Contract (Art. 6(1)(b) GDPR; cf. Art. 31(2)(a) FADP)

The Company processes personal data where necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the data subject's request prior to entering into a contract. This applies in particular to:

- The creation and administration of User Accounts;
- The processing of investments, contributions, and repayments;
- The management of loan claims and collateral;
- Communication with Users in connection with their use of the Platform;
- The execution of claim purchase and assignment agreements.

5.2 Compliance with Legal Obligations (Art. 6(1)(c) GDPR; Art. 31(1) FADP)

The Company is subject to a range of legal obligations that require the processing of personal data. These include in particular:

- Identity verification and know-your-customer (KYC) obligations under the AMLA and the applicable VQF regulations;
- Ongoing AML monitoring, including sanctions screening, PEP screening, and adverse media checks;
- Reporting obligations to the Money Laundering Reporting Office Switzerland (MROS);
- Record-keeping and data retention obligations under the AMLA (minimum ten (10) years), the Swiss Code of Obligations, and the VQF regulations;
- Tax-related reporting obligations, where applicable.

5.3 Legitimate Interests (Art. 6(1)(f) GDPR; Art. 31(1) and (2) FADP)

The Company may process personal data where necessary for the purposes of its legitimate interests, provided that such interests are not overridden by the data subject's rights and freedoms. The legitimate interests pursued by the Company include:

- Ensuring the security and integrity of the Platform and protecting against fraud, unauthorised access, and abuse;
- Conducting credit assessments and risk evaluations of Borrowers and their projects;
- Analysing Platform usage patterns to improve services, user experience, and operational efficiency;
- Exercising or defending legal claims;
- Internal administration and corporate governance.

5.4 Consent (Art. 6(1)(a) GDPR; Arts. 6(6), 6(7) and 31(1) FADP)

Where none of the above legal bases applies, the Company processes personal data only with the data subject's freely given, specific, informed, and unambiguous consent. Consent is relied upon in particular for:

- The sending of newsletters and marketing communications;
- The use of non-essential cookies and analytics tools (as further described in Part V);
- The processing of biometric data for identity verification purposes, on the basis of the data subject's explicit consent (Art. 9(2)(a) GDPR; Art. 6(7) FADP).

Where processing is based on consent, the data subject has the right to withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing carried out prior to the withdrawal. The data subject may withdraw consent by contacting the Company at compliance@crowdhive.com or, in the case of newsletters, by using the unsubscribe link provided in each communication.

Biometric identity verification is carried out only with the data subject's explicit consent, given that biometric data constitutes sensitive personal data within the meaning of Art. 5 let. c FADP and a special category of personal data within the meaning of Art. 9(1) GDPR. A data subject who does not wish to consent to biometric processing may complete identification through an alternative procedure that does not involve biometric data (e.g. identification on the basis of a qualified electronic signature or a certified copy of an identity document, in

accordance with the applicable VQF regulations). Choosing the alternative procedure does not prevent onboarding, although it may take longer to complete.

6. Purposes of Processing

The Company processes personal data for the following purposes:

6.1 Provision of Platform Services

The Company processes personal data in order to operate the Platform and provide the services described in the General Terms and Conditions. This includes the registration and administration of User Accounts, the publication of projects, the processing of investments, the execution of loan agreements and assignment agreements, the collection and distribution of repayments, and the facilitation of transactions on the Secondary Market.

6.2 Identity Verification and AML/KYC Compliance

The Company processes personal data to fulfil its obligations under the AMLA and the VQF regulations. This includes the initial identification and verification of Users, the determination of beneficial owners, ongoing transaction monitoring, sanctions and PEP screening, risk classification, and the filing of reports with MROS where required.

6.3 Credit Assessment and Risk Management

In connection with the evaluation of Borrowers and their projects, the Company processes personal and corporate data to assess creditworthiness, evaluate collateral, and determine the risk profile of each project. This may involve the collection and analysis of data from external credit reference agencies and public registers.

6.4 Marketing and Communications

Where the data subject has given consent, the Company uses name and e-mail address to send newsletters and other marketing communications relating to the Platform’s services, new projects, and relevant updates. The data subject may unsubscribe from such communications at any time.

6.5 Analytics and Platform Improvement

The Company processes aggregated and, where necessary, individual usage data to analyse how the Platform is used, to identify technical issues, and to improve the functionality, performance, and security of the Platform. This processing is carried out using cookies and analytics tools as described in Part V.

6.6 Legal and Regulatory Compliance

The Company processes personal data to comply with its obligations under Swiss and, where applicable, EU law, including record-keeping requirements, tax reporting obligations, regulatory inspections, and cooperation with judicial and law enforcement authorities.

6.7 Protection of Rights and Interests

The Company may process personal data where necessary to exercise or defend its legal rights, to enforce contractual obligations, or to protect the Company's legitimate business interests, including in the context of debt collection, litigation, or regulatory proceedings.

7. Data Collection Methods

The Company collects personal data through the following channels:

7.1 Data Provided Directly by the Data Subject

The primary source of personal data is the data subject. Personal data is provided directly when the User:

- Completes the registration form on the Platform;
- Submits identity documents and other verification materials during the KYC process;
- Provides financial documentation (bank details, proof of wealth, proof of funds);
- Submits a project application (Borrowers);
- Communicates with the Company by e-mail, telephone, or in-platform messaging;
- Subscribes to the Company's newsletter;
- Submits a support request or complaint.

7.2 Data Collected Automatically

Certain technical data is collected automatically when a data subject accesses the Platform. This includes the data described in Section 4.1 (IP address, browser type, pages visited, etc.), as well as cookie data and analytics data as further described in Part V.

The Company's web servers generate log files that record each request made to the Platform. These log files are used for security monitoring, error diagnosis, and statistical analysis of Platform usage.

7.3 Data Collected via Third-Party Identity Verification

The Company uses the services of a third-party identity verification provider (currently Sum and Substance Ltd ("Sumsub"), London, United Kingdom) to perform identity checks on Users. During this process, the verification provider collects and processes identity document data, facial images, and biometric data (facial recognition and liveness detection) on behalf of the Company. The results of the verification are transmitted to the Company and stored in the User's file.

The verification provider processes personal data as a data processor acting on the Company's instructions. The applicable data processing agreement between the Company and the provider ensures compliance with the FADP and, where applicable, the GDPR.

7.4 Data Obtained from External Sources

In the course of its due diligence and risk assessment procedures, the Company may collect personal data from external sources, including but not limited to:

- Public registers (commercial register, debt enforcement register);
- Credit reference agencies and commercial credit databases;
- Sanctions lists (SECO, OFAC, UN, EU);
- PEP databases and adverse media databases;
- Other publicly available sources of information relevant to the Company's AML and risk assessment obligations.

The Company processes data obtained from external sources in accordance with the same standards of data protection applicable to data collected directly from the data subject.

Where the Company obtains personal data relating to natural persons other than the User (e.g. representatives, authorised signatories, beneficial owners, guarantors, or contact persons of Borrowers), the User providing such data confirms that they are authorised to do so and undertakes to inform the persons concerned of this Policy. The Company additionally informs such persons of the processing at the latest upon first communication with them or within one (1) month of obtaining the data, in accordance with Art. 14 GDPR and Art. 19 FADP, unless a statutory exception applies.

Part III – Data Sharing and Transfers

8. Recipients of Personal Data

The Company may share personal data with the categories of recipients described below, strictly within the scope of the purposes set out in Section 6 of this Policy. In each case, the Company ensures that only the minimum amount of data necessary for the specific purpose is disclosed.

8.1 Third-Party Identity Verification Provider

The Company engages a specialised third-party provider to perform identity verification (KYC) of Users. For Investors, the full verification process (including document authentication, facial recognition, and liveness detection) is performed by the third-party provider on behalf of the Company. The provider acts as a data processor under a data processing agreement that ensures compliance with the FADP and, where applicable, the GDPR.

The identity verification of Borrowers is performed directly by the Company through online identification procedures in accordance with FINMA Circular 2016/7. However, the Company may use the same or another third-party provider to support specific elements of the Borrower verification process (e.g. document authentication, sanctions screening).

8.2 Payment Service Providers

The Company works with multiple payment service providers located in Switzerland and in the EU/EEA to process deposits, withdrawals, and other financial transactions on the Platform. These providers receive the data necessary to execute and settle payment instructions, including the User's name, bank account details, and transaction amounts.

Each payment service provider operates under its own terms of service and privacy policy. The Company selects providers that maintain appropriate levels of data protection and, where required, enters into data processing agreements with them. To the extent that a payment service provider processes personal data in order to comply with its own statutory obligations (in particular under payment services and anti-money laundering legislation), it does so as an independent data controller and not as a data processor of the Company.

8.3 Credit Reference Agencies and Commercial Databases

In connection with the assessment of Borrowers, the Company may exchange data with credit reference agencies and commercial credit information providers (e.g. CRIF, Creditsafe, Dun & Bradstreet, or equivalent services). The data exchanged may include the Borrower's name, registered office, company registration number, and financial information relevant to the credit assessment.

If a Borrower defaults on a loan and reasonable reminder procedures have been exhausted, the Company may report the default to the relevant credit reference agency. The agency may record this information and make it available to other subscribers of its services.

8.4 Debt Collection Service Providers

In the event of a payment default by a Borrower, the Company may engage third-party debt collection agencies or legal counsel to pursue recovery on behalf of Investors. Such parties receive the data necessary to conduct collection or enforcement proceedings, including the Borrower's identity, contact details, outstanding amounts, and relevant contractual documentation.

8.5 Regulatory and Law Enforcement Authorities

The Company may be required by law to disclose personal data to Swiss or foreign regulatory, judicial, or law enforcement authorities. In particular:

- Where the Company identifies a suspicion of money laundering or terrorism financing, it is obligated to file a report with the **Money Laundering Reporting Office Switzerland (MROS)**. The report may contain personal data relating to the User, the Beneficial Owner, and the relevant transactions;
- The Company may be required to provide information to the Swiss tax authorities or to foreign tax authorities under applicable tax treaties or automatic exchange of information agreements;
- The Company is subject to inspections by the VQF and its appointed auditors, who may access User data in the course of regulatory audits;
- The Company may be compelled to disclose data in response to court orders, subpoenas, or binding requests from competent authorities.

Where legally permissible, the Company will inform the affected data subject of a disclosure to authorities. However, in certain circumstances (e.g. where a report to MROS has been filed), the Company is prohibited by law from informing the data subject.

8.6 Professional Advisors

The Company may share personal data with its external auditors, legal counsel, tax advisors, and other professional consultants, to the extent necessary for the provision of their services. Such parties are bound by professional secrecy obligations and/or contractual confidentiality undertakings.

8.7 IT and Hosting Service Providers

The Company engages third-party providers for hosting, server administration, data storage, and technical support. These providers may have access to personal data stored on the Company's systems in the course of performing their services. Such providers act as data processors and are bound by data processing agreements that ensure compliance with the applicable data protection legislation.

8.8 No Sale of Personal Data

The Company does not sell, rent, or otherwise commercially transfer personal data to third parties for their own marketing or other independent purposes.

9. International Data Transfers

The Company stores personal data primarily on servers located in Switzerland. However, certain processing activities may involve the transfer of personal data to recipients located outside of Switzerland, including in the EU/EEA and, in limited cases, in third countries.

9.1 Transfers to the EU/EEA

The Company engages payment service providers and other data processors located in EU/EEA member states. Switzerland has been recognised by the European Commission as providing an adequate level of data protection (adequacy decision pursuant to Article 45 GDPR). Correspondingly, the EU/EEA has been recognised by Switzerland as providing an adequate level of protection. Accordingly, transfers of personal data between Switzerland and the EU/EEA do not require additional safeguards.

9.2 Transfers to Third Countries

In the event that personal data is transferred to a country outside of Switzerland and the EU/EEA that has not been recognised as providing an adequate level of data protection, the Company ensures that appropriate safeguards are in place prior to the transfer. Such safeguards may include:

- Standard Contractual Clauses (SCCs) approved by the European Commission or recognised by the Swiss Federal Data Protection and Information Commissioner (FDPIC);
- Certification of the recipient under the Swiss–U.S. Data Privacy Framework or, where the GDPR applies, the EU–U.S. Data Privacy Framework, each of which has been recognised (by the Swiss Federal Council and the European Commission, respectively) as ensuring an adequate level of protection for personal data transferred to certified organisations in the United States;
- Binding Corporate Rules (BCRs) of the recipient, where applicable;

- The data subject's explicit consent to the specific transfer, after having been informed of the risks;
- Any other mechanism recognised as providing adequate safeguards under the FADP or the GDPR.

At the date of this Policy, personal data may be transferred to the following countries outside Switzerland and the EU/EEA: the United States of America (analytics services provided by Google LLC, which is certified under the Swiss–U.S. and EU–U.S. Data Privacy Frameworks; Standard Contractual Clauses apply in the alternative) and the United Kingdom (identity verification services provided by Sumsub; the United Kingdom has been recognised as providing an adequate level of data protection by both the Swiss Federal Council and the European Commission). An updated list of countries to which personal data may be transferred, together with the applicable safeguard mechanism, may be obtained at any time by contacting the Data Protection Contact at compliance@crowdhive.com.

9.3 Risk Assessment

Before transferring personal data to a third country, the Company conducts a transfer impact assessment to evaluate whether the level of data protection in the receiving country is adequate, taking into account the legal framework of the receiving country, the nature and sensitivity of the data, and the safeguards in place. Where the assessment reveals material risks, the Company implements supplementary measures or refrains from the transfer.

10. Disclosure of Project Information on the Platform

The Platform publishes certain information relating to projects submitted by Borrowers. The scope of information disclosed depends on the viewer's registration status:

10.1 Information Visible to Non-Registered Visitors

Non-registered visitors to the Platform may view the following information:

- Project titles;
- General project category or sector;
- Aggregate fundraising status (e.g. percentage funded);
- Key financial terms (interest rate, duration).

No personal data of the Borrower or its representatives is disclosed to non-registered visitors.

10.2 Information Visible to Registered and Verified Users

Registered and verified Investors have access to a more detailed project description, which may include:

- A description of the project and its business objectives, as provided and approved by the Borrower;
- Financial summary information relevant to the investment decision;
- Information on available collateral and guarantees;

- The risk rating assigned by the Company.

The identity of the Borrower is not disclosed to Investors. Users remain anonymous vis-à-vis one another on the Platform. The Company does not reveal the identity or personal data of any Investor to any Borrower, or vice versa.

10.3 Borrower Consent

Before publishing any project-related information on the Platform, the Company agrees with the Borrower on the specific scope of disclosure. No information is published without the Borrower's prior approval. The Borrower is responsible for the accuracy of the information it provides for publication.

The Borrower acknowledges that once information has been published on the Platform during the Offer Period, it is accessible to all registered and verified Users and cannot be retroactively restricted.

Part IV – Data Security and Retention

11. Technical and Organisational Measures

The Company implements appropriate technical and organisational measures to protect personal data against unauthorised access, accidental or unlawful destruction, loss, alteration, and unauthorised disclosure. These measures are designed in accordance with the principles of privacy by design and privacy by default, and are regularly reviewed and updated to reflect evolving threats and best practices.

11.1 Encryption

The Company applies the following encryption standards:

- **Data in transit:** all communications between the User's browser and the Platform are encrypted using Transport Layer Security (TLS 1.2 or higher). API communications and data exchanges with third-party service providers are likewise encrypted;
- **Data at rest:** personal data stored on the Company's servers is encrypted using industry-standard encryption algorithms (AES-256 or equivalent). Database backups are encrypted to the same standard;
- **Sensitive credentials:** passwords are stored exclusively in hashed form using adaptive cryptographic hashing algorithms (e.g. bcrypt, Argon2). Plain-text passwords are never stored or logged.

11.2 Access Control

Access to personal data within the Company is restricted on a strict need-to-know basis. The Company implements the following access control measures:

- Role-based access control (RBAC): each employee or contractor is assigned a role that determines the minimum set of data and systems they may access;

- Individual user accounts with strong authentication requirements for all internal systems;
- Multi-factor authentication (MFA) for administrative access to systems containing personal data;
- Periodic review of access rights to ensure that permissions remain appropriate and are revoked promptly upon changes in role or termination of engagement;
- Logging and monitoring of access to systems containing personal data.

11.3 Pseudonymisation and Data Minimisation

Where technically feasible and consistent with the processing purpose, the Company applies pseudonymisation techniques to reduce the identifiability of personal data. In particular:

- Internal analytics and reporting are performed on pseudonymised or aggregated data sets wherever possible;
- The Company collects and processes only the minimum amount of personal data necessary for each specific purpose;
- Data fields that are not required for a given processing activity are not made accessible to the personnel performing that activity.

11.4 Infrastructure and Hosting

The Company's infrastructure is hosted with a professional hosting provider whose data centres meet the following minimum requirements:

- Physical security measures, including restricted access, surveillance, and environmental controls;
- Redundant systems and regular backup procedures to ensure data availability and recovery in the event of a system failure;
- Compliance with internationally recognised information security standards (ISO/IEC 27001, SOC 2, or equivalent certifications);
- Data centres located in Switzerland, unless otherwise indicated in Section 9 of this Policy.

The Company regularly evaluates its hosting arrangements and may change its hosting provider, provided that any new provider meets or exceeds the standards described above.

11.5 Organisational Measures

In addition to the technical measures described above, the Company maintains the following organisational safeguards:

- A designated Data Protection Contact responsible for overseeing compliance with this Policy and applicable data protection legislation;
- Written internal policies and procedures governing the handling of personal data;
- Confidentiality undertakings for all employees and contractors who have access to personal data;

- Regular training of personnel on data protection principles, information security practices, and the identification of phishing and social engineering attacks;
- Documented incident response procedures for the handling of data protection breaches.

12. Data Retention Periods

The Company retains personal data only for as long as is necessary to fulfil the purpose for which it was collected, or as required by applicable law. Upon expiry of the applicable retention period, personal data is securely deleted or, where deletion is not technically feasible, irreversibly anonymised.

The following retention periods apply to the principal categories of personal data processed by the Company:

Category of Data	**Retention Period**	**Legal Basis / Rationale**
Identity verification (KYC) data	10 years after termination of the business relationship	Art. 7 AMLA; VQF regulations; Art. 958f CO
Biometric verification data (facial recognition templates, liveness detection data)	Deleted upon completion of the identity verification; the verification result and identity document copies are retained as KYC data (10 years)	Explicit consent (Art. 9(2)(a) GDPR; Art. 6(7) FADP); proportionality (Art. 6(2) FADP); Art. 7 AMLA (verification result only)
AML screening results (sanctions, PEP, adverse media)	10 years after termination of the business relationship	Art. 7 AMLA; VQF regulations
Transactional data (investments, repayments, transfers)	10 years after the last transaction	Art. 7 AMLA; Art. 958f CO (commercial record-keeping)
Contractual documentation (loan agreements, assignment agreements)	10 years after expiry or termination of the contract	Art. 958f CO; Art. 127/128 CO (statute of limitations)
Borrower credit assessment data	10 years after termination of the business relationship	Art. 7 AMLA; VQF regulations; duty of care
Communication records (e-mail, support tickets, in-platform messages)	5 years after the last communication or termination of the business relationship, whichever is later	Legitimate interest (evidence preservation); Art. 958f CO
Newsletter and marketing preferences	Duration of the subscription; upon unsubscription, contact details are removed from the mailing list within 30 days and a minimal suppression record (hashed e-mail address) is retained to ensure the opt-out is respected	Consent (Art. 6(1)(a) GDPR); legitimate interest (evidence of opt-out)
Server and access logs	90 days	Legitimate interest (security monitoring, error diagnosis)
Cookie and analytics data	As specified in the cookie table (Part V)	Consent for non-essential cookies; legitimate interest for strictly necessary cookies (see Part V)

User Account data (registration data)	Duration of the business relationship; thereafter retained together with KYC data for 10 years	Contractual necessity; Art. 7 AMLA

Where personal data is subject to more than one retention period (e.g. data that is relevant to both a contractual relationship and an AML obligation), the longer period applies.

During the retention period, personal data is kept confidential and access is restricted to personnel who require it for the applicable purpose. Data held solely for legal retention purposes is archived and is not used for any operational purpose.

Upon request from a data subject, the Company will confirm whether their personal data is still being retained and, if so, under which legal basis. If the data is held solely due to a statutory retention obligation, the Company will inform the data subject accordingly and will delete the data upon expiry of that obligation.

13. Data Breach Notification

The Company maintains a documented data breach response procedure to ensure the timely detection, assessment, and notification of personal data breaches in accordance with the FADP and, where applicable, the GDPR.

13.1 Definition

A personal data breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed by the Company or its data processors.

13.2 Internal Procedures

Upon becoming aware of a suspected or confirmed data breach, the following steps are taken:

- **Detection and escalation:** any employee or contractor who identifies or suspects a data breach must immediately report it to the Data Protection Contact;
- **Assessment:** the Data Protection Contact, in coordination with the relevant technical personnel, assesses the nature, scope, and severity of the breach, including the categories and approximate number of data subjects affected, the categories of personal data involved, and the likely consequences;
- **Containment:** the Company takes immediate steps to contain the breach and mitigate its effects, including isolating affected systems, revoking compromised credentials, and restoring data from backups where necessary;
- **Documentation:** all data breaches are documented in an internal breach register, regardless of whether notification to the authorities or data subjects is required. The register records the facts of the breach, its effects, and the remedial actions taken.

13.3 Notification to the Authorities

Under Art. 24 FADP, the Company shall notify the **Federal Data Protection and Information Commissioner (FDPIC) as soon as possible** of any data breach that is likely to result in a high risk to the personality or the fundamental rights of the affected data subjects.

Where the GDPR applies, the Company shall in addition notify the competent EU/EEA supervisory authority of any data breach **without undue delay and, where feasible, not later than seventy-two (72) hours** after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons (Art. 33 GDPR). Where notification is not made within seventy-two (72) hours, it shall be accompanied by the reasons for the delay.

The notification shall include:

- A description of the nature of the breach, including the categories and approximate number of data subjects and data records affected;
- The name and contact details of the Data Protection Contact;
- A description of the likely consequences of the breach;
- A description of the measures taken or proposed to address the breach and mitigate its effects.

If it is not possible to provide all required information at the time of the initial notification, the Company shall provide the information in phases without further undue delay.

13.4 Notification to Data Subjects

Where a data breach is likely to result in a high risk to the rights and freedoms of affected data subjects, the Company shall inform those data subjects without undue delay, unless:

- The Company has implemented appropriate technical and organisational protection measures (e.g. encryption) that render the personal data unintelligible to any unauthorised person;
- The Company has taken subsequent measures that ensure the high risk is no longer likely to materialise;
- The notification would involve disproportionate effort, in which case the Company will instead issue a public communication or similar measure.

The notification to data subjects shall be made in clear and plain language and shall describe the nature of the breach, the likely consequences, and the measures taken or recommended by the Company to address the breach and protect the affected individuals.

Under the FADP, the Company shall in addition inform the affected data subjects where this is necessary for their protection or where the FDPIC so requests (Art. 24(4) FADP).

13.5 Continuous Improvement

Following the resolution of any data breach, the Data Protection Contact conducts a post-incident review to identify the root cause, evaluate the effectiveness of the response, and implement measures to prevent recurrence. The findings of the review are documented

and, where appropriate, incorporated into the Company's security policies and training materials.

Part V – Cookies and Analytics

14. Cookies

14.1 What Are Cookies

Cookies are small text files that are placed on the User's device (computer, tablet, or smartphone) by the Platform's web server when the User visits the Platform. Cookies enable the Platform to recognise the User's device on subsequent visits, store preferences, and collect information about Platform usage.

Cookies do not contain personal data that directly identifies the User (such as name, address, or bank details). However, cookie data may be combined with other information held by the Company to identify the User in certain circumstances.

14.2 Types of Cookies

The Company uses the following categories of cookies:

a) Strictly Necessary Cookies

These cookies are essential for the basic operation of the Platform. They enable core functionalities such as user authentication, session management, and security features. Without these cookies, the Platform cannot function properly. Strictly necessary cookies do not require the User's consent.

b) Functional Cookies

Functional cookies enable the Platform to remember choices made by the User (such as language preferences or display settings) and provide enhanced, personalised features. These cookies improve the User's experience but are not essential for the Platform's basic operation.

c) Performance and Analytics Cookies

Performance cookies collect anonymised or pseudonymised information about how Users interact with the Platform, including pages visited, time spent on pages, and error messages encountered. This data is used to analyse overall usage patterns, identify technical issues, and improve the Platform's performance. These cookies do not identify individual Users.

d) Marketing and Targeting Cookies

Marketing cookies are used to track Users across websites in order to display advertisements or content that is relevant to the User's interests. These cookies may be set by the Company or by third-party advertising partners. The Company does not currently use marketing or targeting cookies. Should the Company introduce such cookies in the future, this Policy will be updated accordingly and the User's consent will be obtained.

14.3 Cookie Inventory

The following table provides an overview of the cookies currently used on the Platform:

Cookie Name	Category	Provider	Duration	Purpose
session_id	Strictly Necessary	Bellavista Invest One AG	Session	Maintains the User's authenticated session while browsing the Platform
csrf_token	Strictly Necessary	Bellavista Invest One AG	Session	Protects against cross-site request forgery attacks
cookie_consent	Strictly Necessary	Bellavista Invest One AG	12 months	Stores the User's cookie consent preferences
lang	Functional	Bellavista Invest One AG	12 months	Stores the User's language preference
_ga	Performance	Google	2 years	Google Analytics: distinguishes unique users by assigning a randomly generated identifier
_ga_[ID]	Performance	Google	2 years	Google Analytics 4: maintains session state

14.4 Cookie Consent and Management

When the User first visits the Platform, a cookie consent notice is displayed, providing the User with the opportunity to accept all, reject all, or individually configure non-essential cookies (functional and performance cookies), with the available options presented with equal prominence. Non-essential cookies are not set before the User has given consent. Strictly necessary cookies cannot be disabled as they are required for the Platform to function.

The User may at any time change their cookie preferences through the cookie settings accessible on the Platform, or by adjusting the settings in their web browser. Most browsers allow Users to:

- View the cookies stored on their device;
- Delete individual cookies or all cookies;
- Block cookies from specific or all websites;
- Configure the browser to notify the User before a cookie is placed.

Disabling or deleting cookies may affect the functionality of the Platform. In particular, disabling strictly necessary cookies may prevent the User from logging in or using core features.

The User may also prevent the collection of data by analytics cookies by installing browser add-ons such as the Google Analytics Opt-Out Browser Add-on (available at https://tools.google.com/dlpage/gaoptout).

15. Analytics Tools

15.1 Google Analytics

The Company uses Google Analytics 4, a web analytics service provided by Google LLC ("Google"), to analyse usage of the Platform. Google Analytics uses cookies (as described in the cookie table above) to collect information about how Users interact with the Platform. This information is used to compile statistical reports on Platform activity for the Company.

The Company has implemented the following measures to protect User privacy in connection with Google Analytics:

- **IP anonymisation:** Google Analytics 4 does not log or store IP addresses; IP data is used momentarily to derive approximate location and is then discarded;
- **Data Processing Amendment:** the Company has entered into a data processing agreement with Google that governs the processing of personal data by Google on behalf of the Company;
- **Data retention settings:** the Company has configured Google Analytics to retain user-level and event-level data for the minimum period available (2 months for user-level data);
- **No data sharing:** the Company has disabled all optional data sharing features with Google (benchmarking, technical support, account specialists, advertising products).

Google may transfer and store analytics data on servers located outside of Switzerland and the EU/EEA, including in the United States. Google LLC is certified under the Swiss–U.S. Data Privacy Framework and the EU–U.S. Data Privacy Framework, which have been recognised by the Swiss Federal Council and the European Commission, respectively, as ensuring an adequate level of data protection; in the alternative, the Company relies on Standard Contractual Clauses. Analytics cookies are set only after the User has given prior consent via the cookie consent notice (Section 14.4).

Further information about Google's data practices is available at https://policies.google.com/privacy and https://policies.google.com/technologies/partner-sites.

15.2 Other Analytics Tools

The Company does not currently use analytics tools other than Google Analytics. Should the Company introduce additional analytics or tracking tools in the future, this Policy will be updated to describe the tools used, the data collected, and the applicable legal basis and safeguards.

16. Social Media

16.1 Social Media Links

The Platform contains links to the Company's profiles on third-party social media platforms, including LinkedIn, Facebook (Meta), X (formerly Twitter), Instagram, and Telegram. These links are displayed as icons in the footer of the Platform.

The social media links on the Platform are standard hyperlinks and do not involve the use of embedded plugins, widgets, or tracking pixels. When a User clicks on a social media link, they are redirected to the external social media platform in a new browser window. No personal data is transmitted to the social media platform as a result of the link being displayed on the Platform. Data is transmitted to the social media platform only if and when the User actively clicks the link and interacts with the platform.

16.2 Interaction with Social Media Platforms

Once the User navigates to a third-party social media platform, the processing of personal data is governed by the privacy policy of that platform. The Company has no control over and accepts no responsibility for the data processing practices of third-party social media platforms.

Users are encouraged to review the privacy policies of the relevant social media platforms:

- LinkedIn: https://www.linkedin.com/legal/privacy-policy
- Facebook / Meta: https://www.facebook.com/privacy/policy/
- X (formerly Twitter): https://x.com/en/privacy
- Instagram: https://privacycenter.instagram.com/policy
- Telegram: https://telegram.org/privacy

16.3 Future Changes

Should the Company decide to embed social media plugins, widgets, or tracking pixels directly into the Platform in the future, this Policy will be updated to describe the data exchanged with the relevant social media platforms, the applicable legal basis, and the opt-out mechanisms available to the User.

Part VI – User Rights

17. Rights of Data Subjects

Under the FADP and, where applicable, the GDPR, data subjects have the following rights in relation to their personal data. The Company is committed to facilitating the exercise of these rights in a transparent and timely manner.

17.1 Right of Access

The data subject has the right to obtain confirmation from the Company as to whether personal data concerning them is being processed and, if so, to receive a copy of the personal data together with information about the purposes of processing, the categories of data concerned, the recipients to whom the data has been or will be disclosed, and the envisaged retention period.

17.2 Right to Rectification

The data subject has the right to request that the Company correct any inaccurate personal data without undue delay. The data subject also has the right to request that incomplete personal data be completed, including by means of a supplementary statement.

17.3 Right to Erasure

The data subject has the right to request that the Company delete their personal data without undue delay where:

- The personal data is no longer necessary for the purposes for which it was collected;
- The data subject withdraws the consent on which the processing is based and no other legal basis applies;
- The data subject objects to the processing and there are no overriding legitimate grounds;
- The personal data has been unlawfully processed.

Limitation: the right to erasure does not apply where the retention of personal data is required for compliance with a legal obligation (in particular AML record-keeping requirements under Article 7 AMLA, which mandate retention for a minimum of ten (10) years after termination of the business relationship) or for the establishment, exercise, or defence of legal claims. In such cases, the Company will restrict the processing of the data to the legally mandated retention purpose and will delete the data upon expiry of the applicable retention period.

17.4 Right to Restriction of Processing

The data subject has the right to request that the Company restrict the processing of their personal data where:

- The accuracy of the personal data is contested by the data subject, for the period necessary to verify accuracy;
- The processing is unlawful and the data subject requests restriction rather than erasure;
- The Company no longer needs the personal data for the purposes of processing, but the data is required by the data subject for the establishment, exercise, or defence of legal claims;
- The data subject has objected to processing pending verification of whether the Company's legitimate grounds override those of the data subject.

Where processing has been restricted, the Company will store the data but will not process it further (other than for storage) without the data subject's consent, unless the processing is necessary for the establishment, exercise, or defence of legal claims or for reasons of important public interest.

17.5 Right to Data Portability

Under the GDPR (Article 20) and the revised FADP (Art. 28 FADP), the data subject has the right to receive the personal data that they have provided to the Company in a structured, commonly used, and machine-readable format (e.g. CSV or JSON). The data subject also

has the right to request that the Company transmit that data directly to another controller, where technically feasible.

This right applies only to personal data processed on the basis of consent or contractual necessity, and only to data that is processed by automated means.

17.6 Right to Object

The data subject has the right to object at any time to the processing of their personal data where such processing is based on the Company's legitimate interests (Section 5.3). Upon receipt of an objection, the Company will cease processing the data unless it demonstrates compelling legitimate grounds for the processing that override the data subject's interests, rights, and freedoms, or where the processing is necessary for the establishment, exercise, or defence of legal claims.

Where personal data is processed for direct marketing purposes (including newsletters), the data subject has an unconditional right to object at any time, and the Company will cease such processing immediately upon receipt of the objection.

17.7 Right to Withdraw Consent

Where processing is based on consent, the data subject has the right to withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing that was carried out on the basis of consent prior to its withdrawal.

Consent may be withdrawn by:

- Sending an e-mail to compliance@crowdhive.com;
- Using the unsubscribe link provided in marketing communications (for newsletter consent);
- Adjusting cookie preferences on the Platform (for cookie consent).

17.8 Right Not to Be Subject to Automated Decision-Making

The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them. The Company does not currently make decisions based solely on automated processing that produce legal effects for Users. For a detailed description of the automated tools used by the Company and the applicable human oversight, see Section 21 of this Policy.

18. How to Exercise Rights

18.1 Submitting a Request

Data subjects may exercise any of the rights described in Section 17 by submitting a request to the Company by e-mail at compliance@crowdhive.com.

The request should include:

- The data subject's full name and the e-mail address associated with their User Account (if applicable);
- A description of the right the data subject wishes to exercise;
- Any relevant details that will assist the Company in locating and processing the request (e.g. the nature of the data concerned).

18.2 Identity Verification

To protect the privacy and security of data subjects, the Company may need to verify the identity of the requesting individual before processing the request. Where the Company has reasonable doubts concerning the identity of the person making the request, it may ask for additional information or documentation necessary to confirm their identity.

18.3 Response Timeline

The Company will acknowledge receipt of the request and provide a substantive response **within thirty (30) days** of receiving the request. Where the GDPR applies, the response period is one (1) month and may be extended by two (2) further months where necessary, taking into account the complexity and the number of requests. In any such case, the Company will inform the data subject of the extension and the reasons for the delay within the initial thirty-day (or, under the GDPR, one-month) period.

18.4 Fees

Requests are processed free of charge. However, where requests are manifestly unfounded or excessive (in particular due to their repetitive character), the Company may either charge a reasonable fee reflecting the administrative costs of providing the information, or refuse to act on the request. The Company will inform the data subject of the reasons for any fee or refusal.

18.5 Outcome

If the Company grants the request, it will carry out the requested action without undue delay and inform the data subject accordingly. If the Company is unable to grant the request (in whole or in part), it will explain the reasons in writing, including any applicable legal exceptions, and inform the data subject of the right to lodge a complaint with the competent supervisory authority.

19. Right to Lodge a Complaint

If a data subject believes that the Company's processing of their personal data infringes applicable data protection legislation, the data subject has the right to lodge a complaint with the competent supervisory authority.

19.1 Switzerland

For data subjects whose data is processed under the FADP, the competent supervisory authority is:

Authority	Federal Data Protection and Information Commissioner (FDPIC)
Address	Feldeggweg 1, CH-3003 Bern, Switzerland
Website	https://www.edoeb.admin.ch

19.2 European Union / EEA

For data subjects located in the EU/EEA whose data is processed under the GDPR, the competent supervisory authority is the data protection authority of the EU/EEA member state in which the data subject resides, works, or in which the alleged infringement has taken place.

A list of EU/EEA data protection authorities and their contact details is available on the website of the European Data Protection Board at https://edpb.europa.eu.

19.3 Prior Consultation

Before lodging a complaint with a supervisory authority, the Company encourages data subjects to contact the Company directly at compliance@crowdhive.com in order to seek an amicable resolution. The Company takes all complaints seriously and will endeavour to address the data subject's concerns promptly and fairly.

Part VII – Miscellaneous Provisions

20. Privacy by Design and by Default

The Company integrates data protection principles into the design and operation of the Platform, its internal processes, and its business practices from the outset. This approach ensures that privacy considerations are embedded into every stage of the data lifecycle, from collection through to deletion.

20.1 Privacy by Design

The Company applies the following design principles:

- **Data minimisation:** the Company collects and processes only the personal data that is strictly necessary for the specific purpose. Data fields, forms, and processes are designed to avoid the collection of superfluous information;
- **Pseudonymisation:** where technically feasible and consistent with the processing purpose, the Company applies pseudonymisation techniques so that personal data cannot be attributed to a specific data subject without the use of additional information held separately;
- **Purpose separation:** personal data collected for one purpose is not used for a different, incompatible purpose. Internal systems are configured to ensure logical separation of data according to processing purpose;

- **Access restriction:** access to personal data is granted on a strict need-to-know basis, and technical controls enforce the principle that personnel may only view the data required for the performance of their specific tasks;
- **Secure deletion:** the Company maintains an active deletion concept ensuring that personal data is systematically identified and securely deleted or anonymised upon expiry of the applicable retention period.

20.2 Privacy by Default

The Company ensures that the default configuration of the Platform and its systems reflects the highest level of privacy protection. In particular:

- Non-essential cookies and tracking technologies are disabled by default and activated only upon the User's affirmative consent;
- Newsletter subscriptions and marketing communications require explicit opt-in and are not pre-selected;
- The visibility of User information on the Platform is restricted to the minimum necessary for the operation of the service;
- New features and functionalities are evaluated for their data protection impact before deployment.

20.3 Data Protection Impact Assessments and Records of Processing

The Company carries out and documents data protection impact assessments (Art. 22 FADP; Art. 35 GDPR) prior to any processing that is likely to result in a high risk to the personality or the fundamental rights of data subjects. Data protection impact assessments are conducted and kept up to date in particular for the biometric identity verification process, the credit assessment of Borrowers, and the automated AML screening and risk-scoring processes. Where an assessment reveals a high residual risk, the Company consults the FDPIC (Art. 23 FADP) or, where the GDPR applies, the competent supervisory authority (Art. 36 GDPR) prior to commencing the processing.

The Company maintains a record of its processing activities in accordance with Art. 12 FADP and Art. 30 GDPR.

21. Automated Decision-Making and Profiling

The Company uses automated tools in certain aspects of its operations, including:

- Automated identity verification and document authentication performed by the Company's third-party KYC provider;
- Automated screening of Users against sanctions lists, PEP databases, and adverse media sources;
- Automated risk scoring as part of the AML monitoring process.

None of these automated processes results in a decision that is based solely on automated processing and that produces legal effects concerning the data subject or similarly significantly affects them. All automated results are reviewed by the Company's

personnel before a decision is taken that affects a User's access to the Platform or their ability to invest or borrow. The Platform automatically restricts registration from jurisdictions that the Company does not serve; this restriction is based solely on the prospective User's jurisdiction of residence, applies uniformly to all prospective Users from the relevant jurisdiction, and does not involve an evaluation of personal aspects within the meaning of profiling. Any adverse decision concerning an individual User that is based on screening or scoring results is taken only after review by the Company's personnel.

Should the Company introduce automated decision-making processes with legal or similarly significant effects in the future, it will update this Policy and ensure that affected data subjects are informed and afforded the right to obtain human intervention, express their point of view, and contest the decision, in accordance with Article 22 GDPR and the applicable provisions of the FADP.

22. Children's Data

The Platform is not directed at individuals under the age of eighteen (18) years. The Company does not knowingly collect or process personal data from children or minors.

If the Company becomes aware that it has inadvertently collected personal data from a person under the age of eighteen, the Company will take immediate steps to delete such data from its systems and, where applicable, close the associated User Account.

If a parent or legal guardian believes that their child has provided personal data to the Company, they are encouraged to contact the Company at compliance@crowdhive.com so that appropriate action can be taken.

23. Amendments to This Policy

The Company reserves the right to amend this Policy at any time. The current version of this Policy is published on the Platform and is identified by its version number and effective date on the cover page. Material amendments – in particular changes concerning the purposes of processing, the categories of personal data or recipients, or international data transfers – will be announced in advance by e-mail to registered Users and/or by means of a prominent notice on the Platform.

Amendments become effective upon publication on the Platform, subject to the advance notice described above. Where an amendment concerns a processing activity based on the data subject's consent, the Company will obtain fresh consent before the amended processing takes effect.

The Company recommends that Users review this Policy periodically to remain informed of any changes. If a User objects to any amendment, the User should cease using the Platform and may request the deletion of their personal data in accordance with Section 17.3, subject to applicable legal retention obligations.

The Data Protection Contact is responsible for the regular review of this Policy and for initiating any necessary updates to reflect changes in legislation, regulatory guidance, the Company's processing activities, or technological developments.

24. Disclaimer

24.1 Third-Party Websites and Services

This Policy applies exclusively to personal data processed by the Company in connection with the Platform. It does not extend to the data processing practices of third-party websites, applications, or services that may be linked to or accessible from the Platform, including social media platforms, payment service providers, and identity verification providers acting in their own capacity.

The Company has no control over and accepts no responsibility for the content, privacy practices, or security measures of third-party websites. Users are advised to review the applicable privacy policy of any third-party service before providing personal data.

24.2 International Data Transfers

While the Company takes all reasonable steps to ensure the protection of personal data transferred internationally (as described in Section 9), the level of statutory data protection in a recipient country may differ from that in Switzerland or the EU/EEA. The Company transfers personal data abroad only in accordance with Section 9 of this Policy and on the basis of the safeguards described therein. Nothing in this Policy excludes or limits the Company's statutory obligations or liability under the FADP or, where applicable, the GDPR.

24.3 Security of Electronic Communications

The User acknowledges that the transmission of information over the open Internet is never completely secure. While the Company implements appropriate technical and organisational measures to protect personal data (as described in Section 11), the Company cannot guarantee the absolute security of data in transit over the open Internet. Users are encouraged to protect their login credentials, use strong and unique passwords, and keep their devices and browsers up to date. This Section does not limit the Company's statutory data security obligations under Art. 8 FADP and Art. 32 GDPR.

24.4 Accuracy of Information

The Company relies on the accuracy and completeness of the personal data provided by Users. The Company accepts no responsibility for decisions made or actions taken on the basis of inaccurate or incomplete data provided by the User. Users are obligated to keep their personal data up to date in accordance with the General Terms and Conditions.