

Privacy Policy

Oxen Finance Platform & Services

Escrowfy GmbH

Bahnhofstrasse 7, 6300 Zug, Switzerland

VQF SRO Membership Nr. 101009

Document Reference: OXN-POL-PRIV-001

Version 2.0 – Effective Date: 1 March 2026

Classification: PUBLIC

Important Notice

Oxen Finance (“Oxen”) is a registered trademark of **Escrowfy GmbH** (“we”, “us”, “our”, or the “Company”), a company incorporated and registered in Switzerland under company number CHE-281.608.494 with its registered office at Bahnhofstrasse 7, 6300 Zug, Switzerland. Escrowfy GmbH is a member of the VQF Self-Regulatory Organisation (SRO) under membership number 101009, operating as a financial intermediary within the meaning of the Swiss Anti-Money Laundering Act (AMLA/GwG).

Oxen Finance is not a separate legal entity. All services, contracts, and legal obligations arising from the use of the Oxen Finance platform are undertaken exclusively by Escrowfy GmbH. Any reference in this Privacy Policy to “Oxen”, “Oxen Finance”, or “the Platform” shall be construed as a reference to Escrowfy GmbH.

Regulatory status: Escrowfy GmbH is not a bank, an electronic money institution, or a deposit-taking entity. We operate as a regulated financial intermediary providing payment facilitation, cryptocurrency exchange, and related financial technology services within the scope of our regulatory authorisations.

1. Scope and Application

This Privacy Policy (“Policy”) applies to all personal data processed by Escrowfy GmbH in connection with the Oxen Finance platform, including but not limited to the website at oxen.finance, mobile applications, APIs, and any services provided thereunder (collectively, the “Services”). This Policy applies to all categories of data subjects, including individual clients, authorised representatives and beneficial owners of corporate clients, prospective clients, website visitors, and any other individuals whose personal data we process in the course of providing our Services. We process personal data in accordance with applicable data protection laws, including but not limited to:

- The Swiss Federal Act on Data Protection (nFADP/DSG) and its implementing ordinance (DPO/DSV);
- The General Data Protection Regulation (EU) 2016/679 ("GDPR"), where applicable to data subjects in the European Economic Area;
- The United Kingdom General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018, where applicable to data subjects in the United Kingdom;
- The ADGM Data Protection Regulations 2021 ("ADGM DPR"), where applicable to data subjects whose data is processed in connection with activities within the Abu Dhabi Global Market;
- The UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data ("UAE PDPL");
- The Personal Information Protection and Electronic Documents Act ("PIPEDA"), Canada;
- The California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA");
- The Lei Geral de Proteção de Dados ("LGPD"), Brazil; and
- Any other applicable data protection legislation in the jurisdictions in which we operate or in which our data subjects are located.

Where there is a conflict between this Policy and mandatory provisions of applicable law, the applicable law shall prevail.

2. Data Controller

The data controller responsible for the processing of your personal data is: Escrowfy GmbH Bahnhofstrasse 76300 Zug, Switzerland

Email: privacy@oxen.finance

Data Protection Contact: dpo@oxen.finance

For the purposes of the GDPR and UK GDPR, where we process personal data of individuals located in the EEA or the United Kingdom, Escrowfy GmbH acts as the data controller. We are not required to appoint a representative in the EEA or UK under Article 27 GDPR at this time; however, we keep this under review and will appoint one if required.

If you have questions or concerns regarding the processing of your personal data, or if you wish to exercise any of your rights as described in this Policy, you may contact our Data Protection Contact at dpo@oxen.finance.

3. Categories of Personal Data We Collect

3.1 Data Provided Directly by You

(a) Account Registration and Identity Verification

When you create an account, apply for our Services, or undergo our Know Your Customer (KYC) and Know Your Business (KYB) verification processes, we may collect:

- Full legal name, date of birth, nationality, and place of birth;
- Residential address and proof of address documentation (e.g., utility bill, bank statement dated within 3 months);
- Government-issued identification documents (passport, national identity card, driver's licence);
- Biometric data for identity verification purposes (facial image, liveness detection video), collected only with your explicit consent;
- Contact information: email address, telephone number;
- Tax identification number(s) and tax residency information;
- Source of funds and source of wealth documentation.

(b) Corporate Client Data

For corporate or business accounts, we additionally collect:

- Legal entity name, registration number, registered office address, and articles of association or equivalent formation documents;
- Identity documentation for all directors, authorised signatories, shareholders holding 25% or more of voting rights or capital, and ultimate beneficial owners (UBOs);
- Proof of business activity, nature of business, and purpose of the account relationship;
- Corporate structure chart and group ownership information;
- Financial statements and proof of source of corporate funds where required.

© Financial and Transactional Data

- Bank account details (IBAN, BIC/SWIFT, account holder name);
- Cryptocurrency wallet addresses;
- Payment card details (where applicable, processed in PCI DSS-compliant environments);
- Transaction history: amounts, dates, currencies, counterparty details, and transaction references.

3.2 Data Collected Automatically

When you interact with our Platform, we automatically collect:

- IP address (IPv4 and IPv6), approximate geolocation derived from IP;
- Device identifiers, device type, operating system, and browser type and version;
- Pages visited, navigation paths, referral URLs, session duration, and clickstream data;
- Cookie identifiers and similar tracking technologies (see Section 10);
- Log files, error reports, and performance data.

3.3 Data Received from Third Parties

We may receive personal data from the following categories of third-party sources:

- Identity verification and electronic Know Your Customer (eKYC) service providers;
- Credit reference agencies and fraud prevention databases;
- Sanctions and Politically Exposed Persons (PEP) screening databases;
- Publicly available sources, including commercial registers and public records;
- Financial institutions and payment service providers involved in your transactions;
- Regulatory authorities and law enforcement agencies, where permitted by law.

3.4 Special Categories of Data

We do not generally process special categories of personal data (also known as sensitive data) as defined under Article 9 GDPR or equivalent provisions. Where biometric data is processed for identity verification, this is done only with your explicit consent and in compliance with applicable law. We do not process data revealing racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, or data concerning health or sexual orientation.

4. Purposes and Legal Bases for Processing

We process your personal data only where we have a lawful basis to do so. The table below sets out the purposes for which we process personal data, the categories of data involved, and the corresponding legal bases under applicable data protection laws.

Purpose	Categories of Data	Categories of Data
Account opening, onboarding, and identity verification (KYC/KYB)	Identity, contact, financial, biometric (with consent)	Performance of contract (Art. 6(1)(b) GDPR); Legal obligation (Art. 6(1)(c) GDPR); Explicit consent for biometrics (Art. 9(2)(a) GDPR); nFADP Art. 31(1)
AML/CTF compliance, sanctions screening, PEP checks, ongoing monitoring, and suspicious activity reporting	Identity, financial, transactional, third-party screening data	Legal obligation (Art. 6(1)(c) GDPR); Swiss AMLA Arts. 3–8; ADGM AML Rules

Processing transactions, payment facilitation, and settlement	Financial, transactional, identity	Performance of contract (Art. 6(1)(b) GDPR); nFADP Art. 31(1)
Customer support, dispute resolution, and complaint handling	Identity, contact, transactional, communications	Performance of contract; Legitimate interest (Art. 6(1)(f) GDPR)
Fraud detection, prevention, and security	Identity, technical, transactional, device data	Legitimate interest (Art. 6(1)(f) GDPR); nFADP Art. 31(1)
Product improvement, analytics, and service optimisation	Identity, contact, financial, biometric (with consent)	Legitimate interest (Art. 6(1)(f) GDPR); nFADP Art. 31(1)
Direct marketing and promotional communications	Contact, preferences	Consent (Art. 6(1)(a) GDPR); withdrawable at any time
Compliance with legal, regulatory, and tax obligations (incl. CRS/FATCA reporting)	Identity, financial, tax identification	Legal obligation (Art. 6(1)(c) GDPR); Swiss tax laws; UAE tax regulations
Exercise and defence of legal claims	All relevant categories	Legitimate interest (Art. 6(1)(f) GDPR); nFADP Art. 31(1)

Legitimate Interest Balancing: Where we rely on legitimate interest as a legal basis, we have conducted a balancing test to ensure that our interests do not override your fundamental rights and freedoms. You may request information about our balancing assessments by contacting dpo@oxen.finance.

5. Data Sharing and Disclosure

We do not sell, rent, or trade your personal data. We may share your personal data only in the limited circumstances described below and only to the extent necessary for the stated purpose.

5.1 Service Providers and Processors

We engage carefully selected third-party service providers who process personal data on our behalf under written data processing agreements. These include:

- Cloud infrastructure and hosting providers;
- Identity verification and eKYC service providers (e.g., Sumsub);
- Payment processors, card issuers, and banking partners;
- Sanctions screening and risk intelligence providers;
- Customer communication platforms;
- IT security, monitoring, and audit service providers.

All processors are contractually bound to process data only in accordance with our documented instructions, to implement appropriate technical and organisational security measures, and to delete or return personal data upon termination of the engagement.

5.2 Regulatory Authorities and Law Enforcement

We may disclose personal data to regulatory authorities, law enforcement agencies, tax authorities, or courts where required to do so by applicable law or regulation, or in response to a valid legal process. This includes, without limitation:

- The Swiss Money Laundering Reporting Office (MROS) under AMLA reporting obligations;
- The Swiss Financial Market Supervisory Authority (FINMA) or the VQF SRO;
- Tax authorities under CRS, FATCA, or equivalent automatic exchange of information frameworks;
- The Financial Conduct Authority (FCA), the Information Commissioner's Office (ICO), or other UK authorities;
- ADGM Financial Services Regulatory Authority (FSRA) or the UAE Central Bank;
- Law enforcement agencies in response to lawful requests (subpoenas, court orders, warrants);
- Any other competent authority where we are legally obligated to do so.

5.3 Group Entities

We may share personal data with affiliated entities within our corporate group (including, where applicable, entities operating under the Oxen or Escrowfy brand in other jurisdictions), solely for the purposes described in this Policy and subject to equivalent data protection safeguards.

5.4 Business Transfers

In the event of a merger, acquisition, corporate restructuring, or sale of all or a substantial part of our assets, your personal data may be disclosed to the prospective acquirer or successor entity, subject to appropriate confidentiality obligations and the protections described in this Policy. We will notify you of any such transfer where required by applicable law.

5.5 Professional Advisors

We may share personal data with our legal counsel, auditors, accountants, and other professional advisors to the extent necessary for the provision of their professional services to us, subject to professional privilege and confidentiality obligations.

6. International Data Transfers

As we operate internationally, your personal data may be transferred to, stored in, and processed in countries other than the country in which you are located. These countries may have data protection laws that differ from those in your jurisdiction. We ensure that all cross-border transfers of personal data are carried out in compliance with applicable data protection law and are subject to appropriate safeguards, including:

6.1 Transfers from Switzerland

Where personal data is transferred from Switzerland to a country that does not provide an adequate level of data protection as recognised by the Swiss Federal Council (Annex 1 to the Data Protection Ordinance, DPO/DSV), we implement the following safeguards:

- EU/Swiss-approved Standard Contractual Clauses (SCCs) with the Swiss-specific amendments as required by the FDPIC;
- Binding Corporate Rules (BCRs), where applicable;
- Explicit consent, in limited circumstances where no other safeguard is feasible and you have been informed of the risks.

6.2 Transfers from the EEA

Where personal data is transferred outside the EEA, we rely on:

- An adequacy decision by the European Commission (Art. 45 GDPR);
- Standard Contractual Clauses adopted by the European Commission (Art. 46(2) © GDPR);
- Binding Corporate Rules (Art. 47 GDPR), where applicable.

Switzerland benefits from an adequacy decision of the European Commission and is therefore treated as providing an adequate level of data protection for transfers from the EEA.

6.3 Transfers from the United Kingdom

For transfers of personal data outside the UK, we rely on UK adequacy regulations, the International Data Transfer Agreement (IDTA), or the UK Addendum to the EU SCCs, as approved by the UK Information Commissioner's Office (ICO).

6.4 Transfers from the UAE / ADGM

Where personal data subject to the ADGM Data Protection Regulations is transferred outside the ADGM, we ensure compliance with the transfer provisions of the ADGM DPR, including reliance on adequacy determinations, standard data protection clauses, or other approved transfer mechanisms as prescribed by the ADGM.

You may request a copy of the appropriate safeguards we have in place by contacting dpo@oxen.finance.

7. Data Retention

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by applicable law or regulation. The specific retention periods depend on the nature of the data and the legal or regulatory obligation:

Category of Data	Retention Period	Categories of Data
KYC/KYB identity documents and verification records	10 years from termination of the business relationship	Swiss AMLA Art. 7; AMLD5 Art. 40; ADGM AML Rules
Transaction records and financial data	10 years from the date of the transaction	Swiss AMLA Art. 7; Swiss Code of Obligations Art. 958f
AML/CTF screening logs and suspicious activity records	10 years from the date of the report or record	Swiss AMLA; FATF Recommendation 11
Contracts and commercial correspondence	10 years from termination	Swiss Code of Obligations Art. 958f
Tax-related documentation (CRS/FATCA)	As required by applicable tax law (typically 7–10 years)	Swiss Tax Administrative Assistance Act; CRS/FATCA reporting frameworks
Marketing consent and preference records	Duration of consent; 3 years from last interaction if no consent	GDPR Art. 7; nFADP Art. 6
Technical logs and security data	12 months from date of collection	Legitimate interest; proportionality
Support tickets and communications	5 years from resolution	Legitimate interest; contractual necessity

At the end of the applicable retention period, personal data is securely deleted or irreversibly anonymised. Where deletion is not technically feasible (e.g., data in backup archives), we ensure that the data is isolated, access-restricted, and excluded from further processing until deletion is possible.

8. Your Data Protection Rights

Subject to applicable law and any regulatory obligations that may limit the exercise of certain rights, you may be entitled to the following data protection rights:

8.1 Rights Under Applicable Law

Right	Description	Applicable Laws
Right of access	Request confirmation of whether we process your personal data and obtain a copy thereof	nFADP Art. 25; GDPR Art. 15; UK GDPR Art. 15; ADGM DPR
Right to rectification	Request correction of inaccurate or incomplete personal data	nFADP Art. 32(1); GDPR Art. 16; UK GDPR Art. 16; ADGM DPR
Right to erasure (right to be forgotten)	Request deletion of your personal data, subject to legal retention obligations	GDPR Art. 17; UK GDPR Art. 17; ADGM DPR; nFADP Art. 32(2)(a)
Right to restriction of processing	Request that we limit the processing of your personal data in certain circumstances	GDPR Art. 18; UK GDPR Art. 18; ADGM DPR

Right to data portability	Receive your personal data in a structured, commonly used, machine-readable format	GDPR Art. 20; UK GDPR Art. 20; nFADP Art. 28
Right to object	Object to processing based on legitimate interests or for direct marketing purposes	GDPR Art. 21; UK GDPR Art. 21; ADGM DPR
Right to withdraw consent	Withdraw your consent at any time where processing is based on consent, without affecting the lawfulness of processing prior to withdrawal	nFADP Art. 6(6); GDPR Art. 7(3); ADGM DPR
Right not to be subject to automated decision-making	Not be subject to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects	GDPR Art. 22; UK GDPR Art. 22; nFADP Art. 21
Right to lodge a complaint	Lodge a complaint with a supervisory authority (see Section 8.3)	All applicable laws

8.2 How to Exercise Your Rights

To exercise any of the rights described above, please submit your request to:

Email: dpo@oxen.finance

Subject line: "Data Subject Request – [Your Right]"

Postal address: Escrowfy GmbH, Bahnhofstrasse 7, 6300 Zug, Switzerland

We may require you to verify your identity before processing your request. We will respond to all valid requests within 30 days, or within the timeframe required by applicable law. Where a request is complex or voluminous, we may extend this period by an additional 60 days, subject to notifying you of the extension and the reasons therefor.

Please note that certain rights may be limited by applicable law, including where we are required to retain data to comply with anti-money laundering, tax, or other regulatory obligations. In such cases, we will explain the basis for the limitation.

8.3 Right to Lodge a Complaint

If you are dissatisfied with how we handle your personal data or your data protection request, you have the right to lodge a complaint with the competent supervisory authority. The relevant authorities include:

- Switzerland: Federal Data Protection and Information Commissioner (FDPIC/PFPDT) – www.edoeb.admin.ch
- European Union: The supervisory authority in your EU Member State of habitual residence, place of work, or place of the alleged infringement
- United Kingdom: Information Commissioner's Office (ICO) – ico.org.uk
- Abu Dhabi / ADGM: ADGM Office of Data Protection – www.adgm.com
- Canada: Office of the Privacy Commissioner of Canada – www.priv.gc.ca

- California (USA): California Privacy Protection Agency — cpa.ca.gov
- Brazil: Autoridade Nacional de Proteção de Dados (ANPD) — www.gov.br/anpd

9. Data Security

We implement appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing, accidental loss, destruction, or damage. These measures include, but are not limited to:

- Encryption of personal data in transit (TLS 1.2+) and at rest (AES-256);
- Multi-factor authentication and role-based access controls following the principle of least privilege;
- Network segmentation, intrusion detection and prevention systems, and web application firewalls;
- Regular vulnerability assessments, penetration testing, and security audits;
- Data minimisation, pseudonymisation where appropriate, and access logging;
- Business continuity and disaster recovery procedures;
- Staff training on data protection, information security, and confidentiality obligations.

9.1 Data Breach Notification

In the event of a personal data breach that is likely to result in a risk to your rights and freedoms, we will:

- Notify the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of the breach (as required by GDPR Art. 33, ADGM DPR, and recommended under nFADP Art. 24);
- Notify affected data subjects without undue delay where the breach is likely to result in a high risk to their rights and freedoms (GDPR Art. 34; nFADP Art. 24(2));
- Document all breaches in our internal breach register, including the facts, effects, and remedial action taken, regardless of whether notification thresholds are met.

10. Cookies and Tracking Technologies

We use cookies and similar tracking technologies (web beacons, pixel tags, local storage) on our Platform. We classify cookies into the following categories:

Category	Purpose	Consent Required
----------	---------	------------------

Strictly necessary	Essential for the operation of the Platform (e.g., session management, security, authentication)	No (exempt under ePrivacy Directive Art. 5(3); Swiss Telecommunications Act Art. 45c)
Functional	Enable enhanced functionality and personalisation (e.g., language preferences, user settings)	Yes (EEA/UK); Implied (Switzerland)
Analytics	Collect aggregated data about Platform usage and performance	Yes (EEA/UK); Implied (Switzerland)
Marketing / Advertising	Track users across websites to display targeted advertisements	Yes (all jurisdictions)

Where consent is required, we obtain it through a cookie consent management platform before placing non-essential cookies. You may manage or withdraw your cookie preferences at any time via our Cookie Settings Tool accessible on the Platform, or by adjusting your browser settings.

11. Automated Decision-Making and Profiling

We may use automated processes in the following contexts:

- **Transaction monitoring:** Automated systems analyse transactions for indicators of money laundering, terrorist financing, fraud, or sanctions violations. Transactions flagged by automated systems are reviewed by trained compliance personnel before any action is taken that could affect your account or services.
- **Risk scoring:** We may assign risk scores to clients as part of our AML/CTF compliance framework. Risk scoring is used to determine the level of due diligence and ongoing monitoring applied to your account and does not, in isolation, result in decisions that produce legal effects concerning you.
- **Identity verification:** Automated biometric matching may be used as part of the identity verification process, subject to your explicit consent. The results are reviewed and confirmed by our compliance team.

We do not make decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you, without human review, unless such processing is authorised by applicable law (e.g., for AML/CTF compliance) and appropriate safeguards are in place. You have the right to request human intervention, express your point of view, and contest any such decision.

12. Children's Privacy

Our Services are directed exclusively at individuals aged 18 years and over. We do not knowingly collect or process personal data from individuals under the age of 18 (or such other age of legal capacity as may apply in the relevant jurisdiction).

If we become aware that we have inadvertently collected personal data from a minor, we will take prompt steps

to securely delete such data. If you believe that a minor has provided us with personal data, please contact us at dpo@oxen.finance.

13. Jurisdiction-Specific Provisions

The following provisions supplement the general terms of this Policy and apply to data subjects located in specific jurisdictions. In the event of a conflict between the general provisions and these jurisdiction-specific provisions, the jurisdiction-specific provisions shall prevail for data subjects to whom they apply.

13.1 Switzerland

This Policy complies with the Swiss Federal Act on Data Protection (nFADP/DSG), effective 1 September 2023, and its implementing ordinance. Under Swiss law, you have the right to request information about your personal data, to request its correction, deletion, or restriction, and to receive your data in a commonly used electronic format. The supervisory authority is the Federal Data Protection and Information Commissioner (FDPIC).

13.2 European Economic Area (EEA)

Where we process personal data of data subjects located in the EEA, we do so in compliance with the GDPR. The legal bases for processing are set out in Section 4 above. You may exercise all rights under Articles 15–22 GDPR as described in Section 8.

13.3 United Kingdom

For data subjects located in the United Kingdom, we process personal data in accordance with the UK GDPR and the Data Protection Act 2018. Your rights are as described in Section 8. The competent supervisory authority is the Information Commissioner's Office (ICO).

13.4 United Arab Emirates and ADGM

Where we process personal data in connection with our activities within the Abu Dhabi Global Market (ADGM), we do so in compliance with the ADGM Data Protection Regulations 2021. Where we process personal data subject to the UAE Federal Decree-Law No. 45 of 2021, we comply with the provisions thereof, including the requirements relating to purpose limitation, data minimisation, cross-border transfers, and data subject rights. You may exercise your rights as set out in Section 8 or contact the ADGM Office of Data Protection.

13.5 Canada

For individuals in Canada, we process personal data in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA). We rely on your implied or express consent for most processing activities. You have the right to access your personal data, to request correction of inaccurate information, and to withdraw consent for certain processing. Complaints may be directed to the Office of the Privacy Commissioner of Canada.

13.6 California, United States

If you are a California resident, the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA/CPRA) provides you with specific rights:

- Right to know: You may request disclosure of the categories and specific pieces of personal information we have collected, the purposes of collection, and the categories of third parties to whom we disclose data.
- Right to delete: You may request deletion of your personal information, subject to legal exceptions.
- Right to correct: You may request correction of inaccurate personal information.
- Right to opt-out: You may opt out of the “sale” or “sharing” of personal information. We do not sell personal data for monetary consideration. If we engage in targeted advertising that may constitute “sharing” under the CCPA/CPRA, you may opt out by contacting privacy@oxen.finance.
- Right to non-discrimination: We will not discriminate against you for exercising any of these rights.

Notice at Collection: We collect personal identifiers, financial data, internet or network activity, geolocation data, and biometric data (with consent). These categories are collected for the purposes described in Section 4. We retain this data as described in Section 7.

13.7 Brazil

For data subjects in Brazil, we process personal data in accordance with the Lei Geral de Proteção de Dados (LGPD). You may exercise all rights under Articles 17–18 LGPD, including confirmation of processing, access, correction, anonymisation, data portability, deletion, information about sharing, and withdrawal of consent. We will provide responses in Portuguese upon request.

13.8 Australia

For data subjects in Australia, we handle personal information in accordance with the Australian Privacy Act 1988 and the Australian Privacy Principles (APPs). You have the right to request access to and correction of your personal information, and to lodge a complaint with the Office of the Australian Information Commissioner (OAIC).

14. Conflicts of Interest and Data Integrity

We maintain a formal Conflicts of Interest Policy to ensure the fair, objective, and transparent handling of your personal data. This policy includes organisational safeguards to prevent the misuse, improper access, or unauthorised sharing of personal or confidential information by our employees, contractors, affiliates, or partners. All personnel with access to personal data are subject to contractual confidentiality obligations and receive regular training on data protection, information security, and conflicts of interest management.

15. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our processing practices, legal or regulatory requirements, or our business operations. We will post any revised version on our website with an updated Effective Date. Where changes are material, we will notify you by email or through a prominent notice on the Platform prior to the changes taking effect. Where required by applicable law, we will obtain your renewed consent before implementing material changes that affect the processing of your personal data. We encourage you to review this Policy periodically.

16. Contact Us

If you have any questions about this Privacy Policy, wish to exercise your data protection rights, or have concerns about how we handle your personal data, please contact us:

Data Controller	Escrowfy GmbH
Registered Address	Bahnhofstrasse 7, 6300 Zug, Switzerland
Data Protection Contact	dpo@oxen.finance
General Privacy Enquiries	privacy@oxen.finance
Postal Requests	Please mark envelope: "Privacy – Confidential"

17. Definitions

"Personal Data" means Any information relating to an identified or identifiable natural person, within the meaning of nFADP Art. 5(a), GDPR Art. 4(1), and equivalent definitions under applicable law.

"Processing" means Any operation or set of operations performed on personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, restriction, erasure, or destruction.

"Data Controller" means The natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data. In the context of this Policy, the data controller is Escrowfy GmbH.

"Data Processor" means A natural or legal person which processes personal data on behalf of the data controller.

"Oxen Finance" / "Oxen" / "the Platform" means The online platform, website (oxen.finance), and associated services operated by Escrowfy GmbH under the Oxen Finance brand.

“Services” means All financial technology services provided by Escrowfy GmbH through the Platform, including payment facilitation, cryptocurrency exchange, card services, and related ancillary services.

“nFADP” / “DSG” means The Swiss Federal Act on Data Protection, as revised and effective from 1 September 2023 (SR 235.1).

“GDPR” means Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data.

“UK GDPR” means The GDPR as retained in UK law by virtue of the European Union (Withdrawal) Act 2018, read together with the Data Protection Act 2018.

“ADGM DPR” means The Abu Dhabi Global Market Data Protection Regulations 2021.

“AML” / “GwG” means The Swiss Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act).