EQUIPMENT OWNERSHIP & OPERATIONS PROGRAM

LEGAL & GOVERNANCE FRAMEWORK

DOCUMENT 08

Privacy Policy

How the Companies collect, use and protect personal data

e-Investment LLC · OncoBeam AG

Document number	08
Classification	Public — Customer-facing
Version	1.0
Status	Approved
Effective date	July 30, 2026
Owner	Data Protection Lead

Scope. This policy explains how the Seller and the Operator process personal data in connection with the Program, consistent with the EU/UK GDPR, the Swiss Federal Act on Data Protection (FADP) and applicable United States privacy laws. It is supported by the internal Information Security & Cybersecurity Policy (Doc 21). Capitalised terms have the meanings in Document 02.

1. Controllers

The Seller (for the sale and title functions) and the Operator (for custody, operations and settlement) each act as a controller for the personal data they process, and as joint controllers where they determine purposes and means together. The Seller's address is 111 NE 1st Street, 8th Floor, Miami, Florida 33132, USA; the Operator's registered office is Loretohöhe 10, 6300 Zug, Switzerland. Contact details, including for the Data Protection Lead and any EU/Swiss representative, are published on the Platform.

2. Personal data we collect

Category	Examples	Source
Identity & contact	Name, address, date of birth, email, phone	You
Verification (KYC)	Identity-document data, verification results	You; verification providers
Transaction	Orders, Asset IDs, payments, Rent Statements	You; our systems
Operational	Custody, service and utilisation records linked to your Equipment	Operator systems

Category	Examples	Source
Technical	Device, log and cookie data from the Platform	Automatically
Communications	Correspondence and support records	You

3. Purposes and legal bases

Purpose	Legal basis (GDPR/FADP)
Performing the Sale Agreement and the Lease	Performance of a contract
AML/KYC, sanctions screening and reporting	Legal obligation
Operating leased Equipment and paying Fixed Rent	Contract; legitimate interests
Security, fraud prevention and record-keeping	Legal obligation; legitimate interests
Service communications	Contract; legitimate interests
Marketing (where applicable)	Consent, which you may withdraw

4. How we share data

We share personal data with: the other Company in the Program as described above; verification, payment, IT and professional-service providers acting as processors under contract; and authorities where required by Applicable Law. We do not sell personal data. Onward sharing to recipients suggested by third parties is not undertaken without a lawful basis and your knowledge.

5. International transfers

The Program operates across the United States and Switzerland, so personal data may be transferred between these countries and others. Where data is transferred out of the EEA, the United Kingdom or Switzerland, we rely on an adequacy decision or on appropriate safeguards such as the European Commission's Standard Contractual Clauses (with the Swiss addendum), and we make information about the safeguards available on request.

6. Retention

We retain personal data for as long as necessary for the purposes above and to meet legal, tax and regulatory retention requirements (including AML record-keeping), after which it is deleted or anonymised. Retention periods are governed by Document 20 (Records Management & Document Retention Policy).

7. Your rights

Subject to Applicable Law, you may request access to, and correction or deletion of, your personal data; object to or restrict certain processing; request portability; and withdraw consent. Where the FADP or GDPR applies, you may also lodge a complaint with a supervisory authority (in Switzerland, the FDPIC). To exercise your rights, contact the Data Protection Lead using the details on the Platform.

8. Security

We apply technical and organisational measures appropriate to the risk, as set out in Document 21, including access control, encryption in transit, logging and incident response under Document 19. No system is perfectly secure, and we cannot guarantee absolute security.

9. Cookies

The Platform uses strictly necessary cookies and, subject to your choices, analytics or preference cookies. You can manage non-essential cookies through the Platform's cookie controls; we default to the most privacy-preserving setting until you choose otherwise.

10. Children

The Program is not directed at children, and we do not knowingly process the personal data of children.

11. Changes and contact

We may update this policy under Document 29 and will indicate the effective date. For any privacy question or request, contact the Data Protection Lead at the address published on the Platform. Cross-references: Master Definitions (Doc 02); Information Security & Cybersecurity Policy (Doc 21); Incident Response & Regulatory Reporting Procedure (Doc 19); Records Management & Document Retention Policy (Doc 20).