PRIVACY POLICY

Ascendefy OÜ
Document Reference: **ASC-LEGAL-GDPR-2026**
Date of Last Revision: **26 January 2026**
Jurisdiction: **Republic of Estonia**
Data Controller: **Ascendefy OÜ**

---

1. INTERPRETATION AND DEFINITIONS

1.1 Preamble

This Privacy Policy (the **"Policy"**) sets forth the terms under which **Ascendefy OÜ**, a private limited company incorporated under the laws of the Republic of Estonia (the **"Controller," "we," "us," or "our"**), processes Personal Data. This Policy is drafted in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (the **"GDPR"**), the Estonian Personal Data Protection Act (*Isikuandmete kaitse seadus*), and, where applicable *mutatis mutandis*, the California Consumer Privacy Act of 2018 (the **"CCPA"**).

1.2 Definitions

Capitalized terms used herein shall have the meanings ascribed to them in Article 4 of the GDPR, unless otherwise defined below:

- **"Personal Data"** means any information relating to an identified or identifiable natural person (the **"Data Subject"**).
- **"Processing"** means any operation or set of operations which is performed on Personal Data or on sets of Personal Data.
- **"Merchant of Record"** refers to **Whop Inc.**, the entity contractually responsible for financial transaction processing and compliance with the Payment Card Industry Data Security Standards (**PCI-DSS**).

1.3 Amendments

The Controller reserves the right to amend, modify, or supplement this Policy at any time. Material changes shall be communicated via electronic mail or by conspicuous notice on the Service. Continued use of the Service following such notification constitutes acceptance of the revised Policy.

---

2. CONTROLLER DESIGNATION AND LIMITATION OF SCOPE

2.1 Controller Status

Pursuant to Article 4(7) of the GDPR, **Ascendefy OÜ** is designated as the Data Controller for Personal Data collected directly through its proprietary platforms, marketing channels, and community interfaces.

2.2 Severability of Financial Processing

Notwithstanding the foregoing, the Controller explicitly disclaims Controller status with respect to financial instruments, including but not limited to Primary Account Numbers (PAN) and Card Verification Codes (CVC). Such data is collected, processed, and retained exclusively by **Whop Inc.** in its capacity as an independent Data Controller for regulatory banking compliance purposes. Ascendefy OÜ does not possess access rights or decryption keys for such financial data.

3. DATA COLLECTION AND MINIMIZATION PRINCIPLES

In accordance with the principle of data minimization set forth in Article 5(1)(c) of the GDPR, the Controller processes only such Personal Data as is adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

3.1 Categories of Personal Data

The categories of Personal Data processed may include:

- **Identity Data:** First name, surname, unique platform identifiers (including Discord Snowflake IDs), and internal verification tokens.
- **Contact Data:** Email address and billing domicile.
- **Transactional Metadata:** Invoice identifiers, product stock keeping units (SKUs), VAT jurisdiction data, and timestamp records.
- **Technical Telemetry:** IP address, browser user-agent string, operating system specifications, and device hash identifiers.
- **Behavioral Analytics:** Interaction metrics, including scroll depth, clickstream data, and session duration logs.

4. LAWFUL BASIS FOR PROCESSING

The Controller relies on the following lawful bases for Processing pursuant to Article 6 of the GDPR:

4.1 Contractual Necessity (Article 6(1)(b))

Processing of Identity and Contact Data is necessary for the performance of contractual obligations between the Controller and the Data Subject, including the provision of digital services and restricted community access.

4.2 Compliance with Legal Obligations (Article 6(1)(c))

Processing of Transactional Metadata is required under the Estonian Accounting Act (*Raamatupidamise seadus*) and applicable EU VAT Directives, which mandate retention of accounting records for a period of seven (7) years.

4.3 Legitimate Interests (Article 6(1)(f))

Processing of Technical Telemetry and device hashing is conducted for the legitimate interests of ensuring network security, fraud prevention, and intellectual property enforcement. A balancing test has been performed confirming that such interests do not override the rights and freedoms of Data Subjects.

4.4 Consent (Article 6(1)(a))

Processing of Behavioral Analytics and the deployment of non-essential tracking technologies is conducted solely on the basis of the Data Subject’s explicit and informed consent, which may be withdrawn at any time without adverse consequences.

---

5. INTERNATIONAL DATA TRANSFERS

Where Personal Data is transferred outside the European Economic Area, the Controller ensures compliance with Chapter V of the GDPR and relevant case law, including *CJEU Case C-311/18 (Schrems II)*.

5.1 Transfer Mechanisms

- **EU–US Data Privacy Framework:** Transfers to entities certified under the Framework are conducted pursuant to the European Commission Adequacy Decision of 10 July 2023.
- **Standard Contractual Clauses:** For transfers not covered by an adequacy decision, the Controller relies on the European Commission’s Standard Contractual Clauses (Decision 2021/914/EU, Module Two).

5.2 Supplementary Measures

Supplementary safeguards include encryption in transit (TLS 1.2 or higher) and pseudonymization to mitigate risks arising from foreign surveillance legislation, including FISA Section 702.

---

6. DATA SECURITY AND INTEGRITY

6.1 Technical and Organizational Measures

Pursuant to Article 32 of the GDPR, the Controller implements appropriate technical and organizational measures, including:

- Pseudonymization and encryption of Personal Data;
- Measures ensuring confidentiality, integrity, availability, and resilience of systems;
- Periodic testing and evaluation of security measures.

6.2 Personal Data Breaches

In the event of a Personal Data Breach, the Controller shall notify the Estonian Data Protection Inspectorate (*Andmekaitse Inspektsioon*) without undue delay and, where feasible, within seventy-two (72) hours of becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

---

7. DATA RETENTION

Personal Data shall be retained only for as long as necessary to fulfill the purposes outlined in this Policy, subject to statutory retention obligations.

Data Category	Retention Period	Legal Basis
Transaction Metadata	7 years	Estonian Accounting Act
Account Data	Duration of service + 3 years	Civil statute of limitations
Analytics Data	14 months	Commercial efficacy
Security Logs	6 months	Incident investigation

8. RIGHTS OF THE DATA SUBJECT

Data Subjects are entitled to the rights set forth in Chapter III of the GDPR, including:

- **Right of Access** (Article 15);
- **Right to Rectification** (Article 16);
- **Right to Erasure** (Article 17), subject to statutory exceptions;
- **Right to Restriction of Processing** (Article 18);
- **Right to Object** (Article 21).

Requests to exercise these rights must be submitted via the Whop Resolution Center or the designated privacy contact email.

9. CALIFORNIA CONSUMER PRIVACY ACT (CCPA) ADDENDUM

9.1 Applicability

This section applies solely to individuals residing in the State of California ("Consumers").

9.2 Consumer Rights

Consumers have the right to request disclosure of the categories and sources of personal information collected, the purposes of collection, and categories of third parties with whom information is shared. Consumers may also request deletion of personal information, subject to statutory exemptions.

9.3 No Sale of Personal Information

The Controller does not sell personal information within the meaning of the CCPA. Data sharing is limited to service providers pursuant to written agreements.

10. CHILDREN’S PRIVACY

The Services are not intended for individuals under the age of eighteen (18). The Controller does not knowingly collect Personal Data from minors. Any such data discovered will be deleted without undue delay.

---

11. LIMITATION OF LIABILITY

11.1 Commercial Limitation

To the maximum extent permitted by law, the Controller’s aggregate liability arising out of or relating to this Policy (excluding claims under Article 82 of the GDPR) shall not exceed the fees paid by the Data Subject in the twelve (12) months preceding the relevant claim.

11.2 Non-Excludable Rights

Nothing in this Policy shall exclude or limit liability for death or personal injury caused by negligence, fraud, or any liability that cannot be lawfully excluded.

---

12. CONTACT DETAILS

Data Controller: Ascendefy OÜ
Registered Office: Republic of Estonia
Email: privacy@ascendefy.com
Supervisory Authority: Estonian Data Protection Inspectorate (*Andmekaitse Inspektsioon*)