



IVORY S.R.L.

- Via Iacopo da Benevento 27 - Benevento (BN) 82100 - Italy
- info@ivory.live • P.IVA: 58.880.201/0001-00
- www.ivory.live

PRIVACY POLICY

updated on 29/05/2026

1. Who We Are and How to Contact Us

Ivory is an academic social network designed to connect students, researchers, university professionals, and professionals from all sectors, while respecting your security and privacy. Personal data collected will be processed in accordance with the principles of fairness, lawfulness, transparency, necessity, data minimization, accuracy, integrity, and confidentiality required by applicable legislation and through the adoption of the security measures necessary to protect such data pursuant to EU Regulation No. 679/2016.

Data Controller:

Ivory S.r.l.

Address: Via Iacopo da Benevento 21, Benevento (BN), Italy

Privacy contact email: privacy@ivory.live

Website: ivory.live

If you have any questions regarding this Privacy Policy or the processing of your personal data, you may contact us at privacy@ivory.live

2. What Personal Data We Process

To enable you to use the Ivory platform and ensure an authentic and secure academic environment, we process various categories of personal data.

2.1 Data Provided Directly by You

First and last name;

Email address;

Date of birth (to verify legal age and service suitability);

Username (handle) and password (stored in encrypted form);

Any profile information you choose to provide (for example: biography, profile photo, affiliated institution/organization, field of study, city/country, personal website).

2.2 Identity Verification and Academic Qualifications

To ensure that Ivory remains a genuine academic community, the following data are required:

- a copy of your identity card or passport;



- a selfie and/or a short video of your face for biometric comparison with the identity document;
- your academic qualifications and/or credentials (e.g., degree, PhD, affiliations with research institutions).

Such data are processed exclusively for identification purposes, prevention of abuse, and confirmation of affiliation with the academic world or other professional sectors. For this purpose, we inform you that we may verify the information received through external confirmation requests (e.g., to universities regarding the degree indicated in your CV, to professional associations listed in your profile, etc.).

2.3 Data Relating to Content and Interactions

Content you publish: posts, comments, reactions, files, and publications shared on the platform, including participation in thematic communities (Towers). Messages exchanged with other users through the platform's messaging systems.

2.4 Behavioral Data

To understand how you use the platform and improve your experience, we may collect information regarding:

- posts and content viewed;
- time spent in different sections of the platform;
- searches performed;
- interactions with content (likes, comments, shares, participation in Towers and groups);
- frequency and times of access.

Where required, and subject to your consent, these data may also be used for profiling and targeted marketing purposes.

2.5 Technical and Geolocation Data

While using Ivory, we also collect:

- device information (device type, operating system, browser type and version);
- IP address, from which your approximate geographic area (country or region) may be inferred;
- online identifiers (cookies and similar technologies) used for authentication, security, analytics and, where consent is provided, personalized advertising;

- geolocation data, if you enable this functionality, to connect you with nearby users and provide localized services and content.

3. Purposes and Legal Bases for Processing

We process your personal data only where there is a valid legal basis under the GDPR.

3.1 Account Creation and Platform Use

We use your data to:

- create and manage your account on the Ivory platform;
- allow you to use the main social network functionalities (publishing content, interacting with other users, participating in Towers and thematic communities, sending and receiving messages);
- manage subscriptions or premium services and related transactions.

The legal basis is the performance of the contract ("Terms and Conditions") enabling access to the platform.

3.2 Identity Verification and Prevention of Unlawful Activities

To maintain a safe environment aligned with the platform's academic mission, we process identity data, selfies/facial videos, and academic qualifications in order to:

- verify account authenticity;
- prevent fraud, misuse, impersonation, or the creation of fake accounts;
- comply with any legal obligations concerning user identification.

The legal basis is the performance of the contract ("Terms and Conditions") to ensure compliance with the platform rules and our legitimate interest in preventing abuse of the platform. For biometric data such as selfies and facial videos, the legal basis is your consent.

3.3 Profiling and Marketing

With your consent:

- we analyze your browsing and interaction behavior (behavioral data) and information regarding your academic qualifications and educational background;
- * we create profiles relating to your professional and personal interests within academic contexts;

- we display personalized content (e.g., suggested Towers, researchers, publications, and educational opportunities) and targeted advertising consistent with your profile.

You may withdraw your consent at any time through your profile settings without affecting the lawfulness of processing carried out before withdrawal. The legal basis for such processing is your consent.

3.4 Statistical Analysis and Service Improvement

We process data, including aggregated and anonymized data, in order to:

- analyze platform usage;
- measure feature performance;
- improve stability, security, and service usability.

Where analysis involves cookies or similar technologies for non-essential purposes, the legal basis is your consent. For purely technical and security-related activities, the legal basis is our legitimate interest in ensuring proper service operation.

3.5 Geolocation

If you consent to the use of location data, we process such information to:

- connect you with other users and communities in your geographic area;
- suggest localized services, events, and content.

The legal basis is your consent, which may be freely withdrawn at any time through your device or profile settings.

3.6 Network Security, Fraud Prevention and Protection of Rights

We process your data to:

- monitor and prevent unauthorized access, suspicious activities, spam, and abuse;
- respond to requests from competent judicial or administrative authorities;
- establish, exercise, or defend legal claims in judicial or extrajudicial proceedings.

The legal basis is our legitimate interest in ensuring platform security and protecting our rights, as well as compliance with legal obligations where applicable.

4. Security, Architecture and Protection Measures

The protection of your personal data is integrated by design (privacy by design) and by default (privacy by default).

4.1 System Architecture and Resilience

We use professional cloud infrastructure, hosting systems, and high-performance Content Delivery Networks (CDNs) with high security standards. We implement continuous and parallel backup systems and internal caching mechanisms to reduce latency and ensure service availability even in the event of technical failures. Formalized disaster recovery and data restoration procedures are in place to protect your history, documents, and content in case of incidents or malfunctions.

4.2 Technical Security Measures

- Encryption of data in transit through updated TLS protocols;
- Encryption of data at rest using robust cryptographic algorithms;
- Passwords stored using strong hashing functions (e.g., bcrypt) and never in plain text;
- Messaging protected by end-to-end encryption, ensuring that only the sender and recipient can read message contents;
- Access controls based on the “need-to-know” principle, limiting staff access to strictly necessary data.

4.3 Organizational Measures

The organizational measures adopted include:

- periodic staff training on GDPR and personal data protection;
- security audits and periodic reviews of technical and organizational measures;
- documented procedures for managing personal data breaches and, where required, notification to competent authorities and affected individuals.

Despite the measures adopted, no system can be guaranteed to be 100% secure. In the event of a personal data breach likely to result in a high risk to your rights and freedoms, you will be informed without undue delay, within the limits established by law.

5. Sharing of Personal Data

We do not sell your personal data. However, we may share certain categories of data with third parties within the limits and for the purposes described below.

5.1 Data Publicly Visible on the Platform

By default, certain information may be visible to other users or the public, depending on your account settings:

- name, username (handle), profile photo, and biography;
- published content (posts, comments, reactions) on public profiles and public Towers;
- follower/following lists, unless otherwise configured (private profile).

If you set your profile as private, your content will be visible only to followers and/or connections approved by you.

5.2 Other Users and Social Features

Direct messages are shared only with selected recipients and protected by end-to-end encryption. Content published within Towers or communities is visible to members of that space according to the Tower settings.

5.3 Service Providers

We engage external service providers that process personal data on our behalf and under our contractual instructions (data processors), including for example:

- hosting and cloud infrastructure providers;
- Content Delivery Networks (CDNs) and security systems;
- email service providers;
- payment processors for financial transactions.

These parties are bound by specific Data Processing Agreements (DPAs) and are required to:

- process data only for purposes specified by Ivory;
- implement appropriate security measures;
- refrain from disclosing data to third parties except where authorized;
- delete or return data upon completion of the services.

5.4 Commercial Partners and Advertisers

If you consent to profiling and personalized advertising activities, we may:

- use third-party tools (e.g., advertising networks) to display advertisements tailored to your interests;
- share pseudonymized or aggregated data (e.g., audience segments, cookie identifiers, thematic preferences) for campaign measurement and optimization purposes.
-

We do not share the content of your messages, your private documents, or authentication credentials with advertisers.

5.5 Authorities and Legal Obligations

We may disclose your personal data to:

- judicial authorities, law enforcement agencies, or administrative authorities where required by applicable law or lawful orders;
- legal advisors where necessary to protect our rights in judicial or extrajudicial proceedings.

In such cases, disclosure will be limited to relevant and necessary data only. Where legally permitted, we will inform you of such requests.

5.6 Corporate Transactions

In the event of mergers, acquisitions, business transfers, or other corporate transactions involving Ivory, personal data may be transferred to successor entities in compliance with applicable law and ensuring continuity of the protections provided by this Privacy Policy.

6. Transfers of Data to Third Countries

Some of our service providers or partners may be located outside the European Economic Area. In such cases, transfers of personal data take place in accordance with Articles 44 et seq. GDPR through appropriate safeguards, including:

- Standard Contractual Clauses (SCCs) approved by the European Commission;
- additional contractual obligations aimed at strengthening protection (e.g., encryption measures).

You may request further information regarding the safeguards adopted by writing to privacy@ivory.live

7. Data Retention Periods

We retain your personal data only for as long as necessary to achieve the purposes for which they were collected or for longer periods required by law or for the protection of legal rights.

For example:

- identification data (including academic qualifications): for a period of one year, necessary to carry out appropriate verification of the accuracy of declared information;
- account data: for the duration of the contractual relationship and, following account closure, for a limited period (e.g., 30 days) to allow restoration upon user request and management of potential complaints;

- published content (posts, comments): until deleted by you, with a limited and protected technical retention period (soft delete);
- log data and IP addresses: for a limited period (e.g., 30–90 days) for security and fraud prevention purposes;
- data used for profiling and statistical analysis: for a maximum period of two years unless consent is withdrawn;
- transaction-related and accounting documentation: for the periods required under applicable tax and civil law.

Upon expiry of retention periods, data are deleted or anonymized.

8. Your Rights Under the GDPR

As a data subject, you may exercise the following rights at any time:

- **Right of access:** obtain confirmation as to whether personal data concerning you are being processed and receive a copy of such data together with relevant information regarding processing.
- **Right to rectification:** obtain correction of inaccurate data or completion of incomplete data.
- **Right to erasure (right to be forgotten):** obtain deletion of your personal data in the cases provided for by Article 17 GDPR (e.g., withdrawal of consent, data no longer necessary).
- **Right to restriction of processing:** request that the use of your data be restricted in specific circumstances.
- **Right to data portability:** receive personal data concerning you in a structured, commonly used, machine-readable format and transmit them to another controller.
- **Right to object:** object at any time to processing based on legitimate interests, including related profiling, subject to balancing against overriding legitimate grounds or legal obligations.
- **Right to withdraw consent:** withdraw consent at any time for specific purposes (e.g., profiling, geolocation, marketing), without affecting processing already carried out.

Furthermore, if you believe that the processing of your data infringes the GDPR, you have the right to lodge a complaint with the competent Data Protection Authority or with the supervisory authority of the Member State where you habitually reside, work, or where the alleged infringement occurred. You may exercise your rights through:

- the tools available in your profile settings (e.g., data download, consent management, account deletion);
- a written request sent to [\[privacy@ivory.live\]](mailto:privacy@ivory.live)(mailto:privacy@ivory.live).

We will respond within a maximum period of 30 days, subject to extensions permitted by the GDPR.

9. Cookies and Tracking Technologies

Ivory uses cookies and similar technologies to ensure proper platform operation, improve performance and, where consent is provided, personalize content and advertisements. You may manage your preferences through the cookie banner displayed upon first access and subsequently through the privacy settings section.

10. Minors

Ivory is intended exclusively for adult users (18 years or older). We do not knowingly collect personal data relating to minors. If we become aware that a minor has provided personal data without parental responsibility holders' consent, we will promptly delete such information. If you believe that a minor is using Ivory or has provided personal data, please contact us at: privacy@ivory.live

11. Changes to this Privacy Policy

We reserve the right to periodically update this Privacy Policy, including to reflect legal developments or changes in the services offered. In the event of material changes, we will provide appropriate notice through available channels (e.g., in-app notifications, email, website banners) and, where required, request your consent again. The date of the latest update will always be indicated at the beginning of the Privacy Policy.

12. Contact Information

For any request for clarification, exercise of rights, or additional information regarding the processing of personal data, you may contact us by email at: privacy@ivory.live