

PERSONAL DATA PROCESSING POLICY

Networking.One Platform

Service Provider: Advanced Engineering 3D Printers LLC

Registered: Georgia

Effective Date: November 3, 2025

1. Introduction

This Personal Data Processing Policy describes how Networking.One handles user data in accordance with:

- **GDPR** (General Data Protection Regulation).
- **UK Data Protection Act 2018**.
- **PECR** (Privacy and Electronic Communications Regulations).

This policy is an internal operational document publicly available for transparency. It complements our [Privacy Policy](#), [Cookie Policy](#), and [End User License Agreement](#).

2. Core principles

What makes us different:

-  **No third-party analytics** — We do NOT use Google Analytics, Facebook Pixel, Mixpanel, Amplitude, or any external tracking tools.
-  **No data sharing** — We never sell, share, or transfer user data to third parties for marketing or advertising.
-  **No profiling** — We do not use data for behavioral profiling, personalized ads, or algorithmic targeting.
-  **Explicit consent only** — All data processing is based on clear user consent.
-  **Essential cookies only** — We use only technical/functional cookies required for the platform to work.
-  **Internal analytics only** — Usage data is collected exclusively through our own systems for technical improvements (bug fixes, performance optimization).

3. Roles and responsibilities

3.1. Data Protection Officer (DPO)

- Ensures compliance with GDPR, UK DPA 2018, PECR.
- Handles user data requests (access, rectification, deletion, portability).
- Coordinates with supervisory authorities if required.
- **Contact:** privacy@networking.one.

3.2. Security administrator / Tech lead

- Implements and maintains technical security measures.
- Manages encryption, access controls, backups.
- Monitors system integrity and responds to security incidents.
- Conducts quarterly security reviews.

3.3. Platform administrators

- Manage user accounts with role-based access.
- Process data deletion requests.
- Provide technical support.

3.4. Marketing / Support team

- Handles marketing communications with explicit user consent.
- Processes unsubscribe requests immediately (within 24 hours).
- Maintains suppression lists to prevent unwanted emails.

For seed-stage: These roles may be combined and assigned to founders, CTO, or senior team members.

4. Technical security measures

We implement industry-standard security to protect user data:

4.1. Encryption

- **In transit:** TLS 1.3 or higher.
- **At rest:** AES-256 encryption for all stored data.
- All database connections are encrypted.

4.2. Access Control

- **Role-Based Access Control (RBAC):** Users/admins have minimum necessary permissions.
- **Two-Factor Authentication (2FA):** Required for all administrative access.
- **Audit logs:** All access to personal data is logged and retained for 12 months.

4.3. Backups

- **Daily automated backups** with geographic redundancy.

- **Retention:** Backups kept for 90 days/
- **Testing:** Backup restoration tested quarterly.

4.4. Monitoring

- **24/7 automated monitoring** of system integrity.
- **Intrusion Detection System (IDS)** to detect suspicious activity.
- **Security patches** applied within 7 days of release for critical vulnerabilities.

4.5. Infrastructure

- Secure hosting with reputable providers compliant with ISO 27001 / SOC 2.
- Network segmentation to isolate sensitive data.
- Regular security audits (quarterly internal, annual independent).

5. User rights (GDPR Articles 15-22)

Users have the following rights regarding their personal data:

5.1. Right to access (Art. 15)

Request a copy of all personal data we hold.

Response time: Within 30 days.

5.2. Right to rectification (Art. 16)

Correct inaccurate or incomplete data.

Response time: Within 7-30 days.

5.3. Right to erasure / "Right to be Forgotten" (Art. 17)

Request deletion of all personal data (subject to legal retention requirements).

Response time: Within 30 days.

5.4. Right to restrict Processing (Art. 18)

Limit how we process data while verifying accuracy or resolving disputes.

Response time: Within 30 days.

5.5. Right to data portability (Art. 20)

Receive data in a machine-readable format (CSV or JSON).

Response time: Within 30 days.

5.6. Right to object (Art. 21)

Object to processing for direct marketing (unsubscribe).

Response time: Immediate (within 24 hours).

5.7. Right to withdraw consent

Withdraw consent at any time without penalty.

Effect: Immediate cessation of processing based on that consent.

How to exercise rights: Email privacy@networking.one with your request. We verify identity before processing.

6. Consent management

6.1. Explicit Consent Required

We obtain clear, affirmative consent for:

- Creating an account and processing account data.
- Sending marketing communications.
- Processing contact data uploaded by users.
- Using functional cookies.

6.2. How we obtain consent

- **Checkboxes** (no pre-ticked boxes).
- **Clear language** explaining what data is collected and why.
- **Separate consents** for different purposes (account vs. marketing).
- **Consent records** stored with timestamp, IP address, method, and policy version.

6.3. Consent renewal

- **Marketing consent:** Renewed every 24 months.
- **Cookie consent:** Renewed every 12 months.
- Users are notified before renewal and can opt out.

6.4. Withdrawal

Users can withdraw consent at any time via:

- Account settings.
- Unsubscribe links in emails.
- Email to privacy@networking.one.

7. Data Retention

We retain data only as long as necessary:

Data Type	Retention Period	Reason
Active account data	While account is active	Service provision
After account closure	Up to 2 years	Legal/contractual obligations
Financial records (invoices)	7 years	Tax law compliance
Backups	90 days	Disaster recovery
Marketing suppression lists	2 years	Prevent unwanted emails
Security logs	12 months	Security monitoring

Automatic deletion: After retention periods expire, data is permanently deleted and cannot be recovered.

8. Cookies

8.1. What Cookies We Use

Only essential/functional cookies:

- **Authentication:** Keep users logged in.
- **Security:** Protect against malicious activity.
- **Session management:** Maintain platform state.
- **Preferences:** Remember language and settings.

8.2. What We DO NOT Use

- ✗ Analytics cookies (Google Analytics, etc.).
- ✗ Marketing cookies (retargeting, ads).
- ✗ Social media tracking pixels.
- ✗ Third-party cookies.

Full details: [Cookie Policy](#).

9. Marketing communications (PECR Compliance)

9.1. Consent required

We send marketing emails only with explicit user consent (except for "soft opt-in" for existing customers about similar products).

9.2. Unsubscribe

- **One-click unsubscribe** link in every email.
- Processing time: **Immediate** (within 24 hours maximum).
- Confirmation email sent after unsubscribing.

9.3. Suppression lists

- Users who unsubscribe are added to suppression lists.
- Lists checked before every marketing send.
- Retained for 2 years to prevent re-contact.

9.4. Preference centre

Users can manage:

- Email frequency (weekly, monthly, never).
- Content types (product updates, events, newsletters).
- Channels (email only for now; future: SMS, in-app).

Access: Account settings or link in marketing emails.

10. Security incident response

If a security incident or data breach occurs:

10.1. Detection and containment (0-24 hours)

- Immediate investigation by Security Admin/DPO.
- Isolate affected systems.
- Assess scope and severity.

10.2. Notification (Within 72 hours)

- **If high risk to user rights:** Notify affected users without undue delay.
- **If required by GDPR Art. 33:** Notify supervisory authority within 72 hours.
- **Communication:** Email to affected users explaining what happened, what data was affected, and what we're doing.

10.3. Remediation (7 days)

- Fix vulnerabilities.
- Restore services.
- Implement additional safeguards.

10.4. Post-incident review (30 days)

- Document lessons learned.
- Update security procedures.
- Train team on prevention.

Incident records retained for 7 years.

11. Staff training

11.1. Onboarding

All team members with access to user data complete:

- Basic GDPR/data protection training (online course or internal session).
- Security best practices (passwords, phishing, access controls).
- Confidentiality agreement signed.

11.2. Ongoing training

- **Annual refresher:** GDPR and security updates.
- **Ad-hoc training:** When policies change or new features launch.
- **Incident training:** After any security incident.

11.3. Documentation

Training completion recorded with date and topics covered.

12. Third-party processors

We use a limited number of trusted service providers who may access user data to help us operate the Platform:

Provider Type	Purpose	Compliance
Hosting provider	Infrastructure, servers	ISO 27001, SOC 2
Email service	Transactional emails (password resets, etc.)	GDPR compliant
Payment processor	Subscription payments (if applicable)	PCI-DSS compliant
Support tools	Customer service tickets	GDPR compliant

All third-party processors:

Sign Data Processing Agreements (DPAs).

Comply with GDPR Article 28 requirements.

Are located in the EU/UK or have adequate safeguards (Standard Contractual Clauses).

Do NOT use data for their own purposes.

List updated: Quarterly

View current processors: Available on request at privacy@networking.one

13. International data transfers

Primary data location: European Union / United Kingdom

If data is transferred outside EU/UK:

- **Only to countries with adequacy decisions** (e.g., Canada, Japan, Switzerland).
- **OR with Standard Contractual Clauses (SCCs)** approved by the EU Commission.
- **OR under other GDPR-compliant transfer mechanisms.**

We do NOT transfer data to countries with no adequate protections.

14. User data requests (DSARs)

14.1. How to submit

Email privacy@networking.one with:

- Your name and registered email.
- Type of request (access, deletion, rectification, etc.).
- Identity verification (we may request additional info).

14.2. Processing

- **Acknowledgment:** Within 48 hours.
- **Completion:** Within 30 days (may extend to 60 days for complex requests).
- **Delivery:** Secure email with encrypted attachment or through account portal.

14.3. No charge

Data subject requests are processed **free of charge** unless:

- The request is manifestly unfounded or excessive.
- Repeated requests for the same information.

15. Record keeping

We maintain the following records to demonstrate GDPR compliance:

15.1. Records of processing activities (ROPA)

- Categories of data processed.
- Purposes of processing.
- Legal bases (consent, contract, legitimate interest).
- Data retention periods.
- Security measures.

Updated: Quarterly or when processing changes

15.2. Consent records

- Timestamp of consent.
- IP address.
- Method of consent (checkbox, button click).
- Version of policy/consent text shown.

Retained: For duration of processing + 3 years

15.3. User request log

- Date request received.
- Type of request.
- Date completed.
- Outcome.

Retained: 3 years.

15.4. Incident log

- Date/time of incident.
- Nature and scope.
- Actions taken.
- Notifications sent.

Retained: 7 years.

16. Review and updates

16.1. Regular review

This policy is reviewed:

- **Every 6 months** (routine review).
- **When laws change** (GDPR amendments, new regulations).
- **When the platform changes** (new features, data processing).
- **After incidents** (to improve procedures).

16.2. Policy updates

If we make significant changes:

- **30 days advance notice** to users.
- Email notification to all active users.
- Prominent notice on website/platform.
- Version number incremented.

Change log: Available at <https://networking.one/data-processing-policy/changelog>

17. Complaints and escalation

17.1. Internal Complaints

If you're unhappy with how we handle your data:

Email: privacy@networking.one

We investigate and respond within 30 days.

17.2. Supervisory authority

You have the right to lodge a complaint with:

UK users:

Information Commissioner's Office (ICO)

Website: <https://ico.org.uk>

Phone: 0303 123 1113

EU users:

Your national data protection authority

List: https://edpb.europa.eu/about-edpb/board/members_en

18. Contact information

Data Protection Officer:

Email: privacy@networking.one

Response time: Within 48 hours (business days)

Service Provider:

Advanced Engineering 3D Printers LLC

Registered in Georgia

Website: <https://ae3dp.com>

General inquiries: support@networking.one

Legal matters: legal@networking.one

IP Rights Holder:

AE Intellectual Property LTD

Registered in Cyprus

Website: www.aeip.ltd