Glow – Privacy Policy

Effective date: 2025-11-11

This Privacy Policy explains how Glow (“we”, “us”, “our”) processes personal data when you use our websites, mobile apps, and related services (the “Services”). It is designed to meet or exceed the requirements of the EU/EEA General Data Protection Regulation (GDPR), the German TTDSG, and relevant EU digital platform rules (including the DSA), and provides transparent information on our processing activities, safeguards, and your rights.

1. Controller, Contact Details, and DPO

Controller: Flexbox Kft., 7630 Pécs, Feketerigó utca 17., Hungary (operating the Glow Services).

Email: privacy@glow.support | Mailing address: 7601 Pécs, Jókai u. 10., Hungary

If we appoint a Data Protection Officer (DPO) or EU/UK representative, we will publish their contact details on our website and in the app settings.

2. Scope, Audience, and Eligibility

Scope.

This Policy applies to all processing of personal data collected through the Services, including account creation, profile use, messaging, purchases, support interactions, cookies/SDKs, and safety/moderation features.

Audience and age.

The Services are intended for adults aged 18+. We do not knowingly process data of individuals under 18. If we become aware of such processing, we will delete the data and may remove the account.

Territorial scope.

This Policy primarily addresses the GDPR/EEA requirements and notes applicable German specifics (TTDSG/DSA). Regional supplements may apply for the UK/Switzerland/US (Annex E).

3. Definitions (Plain Language)

Personal data

Any information relating to an identified or identifiable natural person, including identifiers, device and online data, location, or inferences linked to a person.

Special category data

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic/biometric data uniquely identifying a person, health data, or data concerning a person's sex life or sexual orientation (GDPR Art. 9).

Processing

Any operation performed on personal data (collection, storage, use, disclosure, etc.).

Controller / Processor

We are the controller for the processing described here. Processors are service providers acting on our documented instructions.

4. Personal Data We Collect

We collect the following categories depending on your use of the Services. Items marked "optional" are provided at your discretion. Items marked "special" may require explicit consent under Art. 9 GDPR.

4.1 Account & Identifiers

- Registration details: name or username, email address, phone number, date of birth (18+), password or login tokens.
- Third-party sign-in IDs (Apple/Google/Facebook) and the account email and profile image you allow us to access.

4.2 Profile & Community Content (optional; may include "special")

- Profile text (bio), interests, lifestyle tags, relationship goals, hobbies, languages, education/work fields.
- Photos and videos you upload; visibility/blur settings; preference filters.
- Sexual orientation and sex-life preferences (kinks/fetishes, relationship styles) – "special" data, processed only with explicit consent and fully optional.
- Other optional attributes (e.g., religion, political views, ethnicity, health-related info) – "special" data with explicit consent only.

4.3 Communications & Social Interactions

- Direct messages, likes, matches, reports/blocks; timestamps and metadata (e.g., delivery/read status).
- Voice notes, video chat previews/frames (where available).

4.4 Verification & Safety Signals

- Phone/SMS verification, two-factor authentication (2FA).
- Selfie/ID verification data (images/video and, where applicable, derived biometric templates used solely for identity/age verification). Deleted after verification unless needed for security/fraud prevention or required by law.

- Abuse/spam indicators, blocklists, device integrity checks, suspicious-activity scores.

4.5 Location & Device Data

- Approximate or precise location (with your permission) for nearby discovery and safety features.
- Device model, OS version, app version, device IDs, IP address, timezone, language, battery/network status (to improve reliability).

4.6 Usage, Telemetry, and Diagnostics

- Event logs (logins, settings changes, feature usage), crash reports, performance metrics, A/B test variants.

4.7 Purchases & Payments

- Subscription tier, purchase history, renewal status, receipts, tax/VAT info. Payment card data is processed by payment processors; we receive tokens/metadata only.

4.8 Support & Feedback

- Support tickets, emails, attachments, satisfaction ratings, and call/chat recordings (where used) for quality assurance.

4.9 Cookies/SDKs and Similar Technologies

- Cookies, mobile SDKs, pixels, and local storage used for essential operation, analytics, security, and—where consented—marketing. (See Cookie Policy.)

4.10 Third-Party and Public Sources

- Anti-fraud and safety partners may provide risk indicators (e.g., compromised credentials, bot/automation signals).
- If you connect third-party features (e.g., social logins), we receive data those providers share per your settings.
- Public or semi-public data (e.g., reported misuse on platforms) for safety purposes in compliance with law.

5. Where We Get Personal Data From

- Directly from you (account creation, profile edits, content you upload, messages).
- Automatically from your devices when using the Services (subject to your settings and consent for non-essential tracking).
- From processors and partners assisting with payments, analytics, verification, security, and support.
- From other users (e.g., reports/blocks) and publicly available sources where lawful.

6. Purposes and Legal Bases

We process personal data for the purposes below. Multiple legal bases may apply depending on context.

Contract performance (Art. 6(1)(b))

- Create and manage your account; enable login and profile display; provide messaging and matching features; process purchases and subscriptions.

Legitimate interests (Art. 6(1)(f))

- Ensure relevance and safety; detect abuse/spam/fraud; enforce terms; measure and improve performance; develop features; customer support.

We apply a balancing test (Legitimate Interest Assessments) to ensure our interests do not override your rights (see Annex C). You may object at any time (Section 15).

Consent (Art. 6(1)(a) and Art. 9(2)(a) for special data)

- Special category profile fields (orientation, kinks) are fully optional and processed only with explicit consent; can be withdrawn in settings.
- Non-essential cookies/SDKs and marketing communications in the EEA/UK require consent.

Legal obligations (Art. 6(1)(c))

- Tax/accounting retention; responding to lawful requests; safety duties under applicable platform rules.

Vital interests / Public interest

- In emergencies threatening life or safety, we may process/disclose data to protect individuals (Art. 6(1)(d)).

Purpose	Data categories (examples)	Legal basis
Account & login	Identifiers, device data	Contract; legitimate interests (security)
Profile & discovery	Profile fields; location (opt-in)	Contract; legitimate interests; consent (special data)
Messaging	UGC, metadata	Contract; legitimate interests (safety)

Verification & safety	ID/selfie; risk indicators	Legitimate interests; legal obligations; consent (where required)
Payments	Purchase meta; receipts	Contract; legal obligations; legitimate interests (anti-fraud)
Analytics & improvement	Usage, telemetry, A/B tests	Legitimate interests; consent (cookies/SDKs)
Marketing	Contact details; cookie IDs	Consent; legitimate interests (where permitted)

7. Automated Decision-Making and Profiling

We use automated systems to recommend profiles, prioritize discovery ranks, and detect policy violations or abnormal patterns. Inputs may include your profile, preferences, engagement signals, device/network signals, and reports. We do not make decisions producing legal or similarly significant effects solely by automated means.

Human review and appeal.

If your content is removed or your account is restricted based on automated signals, you can request human review through in-app tools or support. We will explain the main reasons and provide an appeal path, consistent with the DSA.

8. Community Safety, Moderation, and Illegal Content

We combine automated tools and human moderators to enforce our Terms and Community Guidelines. Illegal content (e.g., non-consensual imagery, hate speech) may be removed and reported to authorities where required. Repeat or severe violations may lead to suspension or ban. We keep audit logs of moderation actions for an appropriate period and provide notices and appeal mechanisms.

9. Marketing, Measurement, and Personalization

- Marketing communications (email/SMS/push) require consent in the EEA/UK; you can withdraw anytime via links or settings.
- Ads and personalization in the EEA/UK rely on consent for non-essential cookies/SDKs; otherwise, you may receive contextual or non-personalized ads.
- We honor platform privacy signals where required (e.g., consent banners, OS tracking toggles).

10. Cookies, SDKs, and Similar Technologies

Details are provided in our Cookie Policy (Annex A in a separate document). You can change your choices through the consent banner/preferences center and device/browser settings.

11. How We Share Personal Data (Categories of Recipients)

- Processors under contract: hosting/CDN, databases, analytics, A/B testing, crash reporting, moderation, verification, communications, customer support, and payments.
- Independent controllers (where applicable): app stores, payment providers, single sign-on providers, and ad partners you directly interact with.
- Law enforcement and authorities: where required by law or necessary to protect rights and safety.
- Corporate transactions: in the event of a merger, acquisition, or restructuring, with appropriate safeguards and notices.

12. International Data Transfers

Where data is transferred outside the EEA/UK/CH, we use safeguards such as EU Standard Contractual Clauses (SCCs), the UK IDTA/Addendum, and technical and organizational measures. We conduct transfer risk assessments where appropriate. You may request a copy of relevant safeguards (with redactions for confidentiality).

13. Data Retention and Deletion

We retain personal data only as long as necessary for the purposes listed above, and to meet legal/accounting requirements. Typical periods:

Data Category	Typical Retention
Account & profile	Life of account + up to 3 months grace; up to 2 years for banned accounts to prevent recidivism.
Verification (ID/selfie/biometric templates)	For verification only; deleted afterwards unless needed for security/fraud or legal obligations.
Messages and UGC	As long as necessary for the Service and safety; may be deleted by you subject to legal holds.
Logs/telemetry	Up to 12 months for security/operations.
Payments/receipts	Up to 10 years (tax/accounting).
Support/complaints	Typically 5–6 years for compliance and legal claims.

Anonymized or aggregated data (no longer identifying you) may be retained for analytics and reporting.

14. Security (Technical and Organizational Measures)

- Encryption in transit (TLS) and at rest where applicable; hardened configurations; segmented environments.
- Access controls with least privilege, role-based access, and multi-factor authentication for administrators.
- Secure development lifecycle, code reviews, dependency scanning, and security testing.
- Monitoring, logging, and anomaly detection; regular backups and disaster recovery planning.
- Vendor due diligence, DPAs with processors, and periodic audits.
- Incident response plan and breach notification procedures pursuant to GDPR/DSGVO.

15. Your Choices and Data Subject Rights

Choices

- Profile controls: edit/delete certain fields; toggle visibility; withdraw special-data consent; adjust discovery settings.
- Notifications: manage email/SMS/push; opt out of marketing at any time.
- Cookies/SDKs: manage via consent banner and device/browser settings.

GDPR Rights

- Access, rectification, erasure, restriction, portability, objection (incl. to profiling based on legitimate interests), and consent withdrawal.
- Right to contest automated decisions and request human review where applicable.

How to exercise: use in-app tools (where available) or contact privacy@glow.support. We will respond within one month or explain any justified extension.

You may lodge a complaint with your local supervisory authority in the EEA/UK.

16. Moderation Notices and Appeals

If we remove content or restrict your account, we will, where required, provide a notice explaining the main reasons and how to appeal. Appeals are reviewed by trained staff. Repeated or egregious violations may result in bans.

17. Children’s Data

We do not knowingly process personal data of individuals under 18. If you believe a minor has provided us data, please contact us so we can delete it and take appropriate measures.

18. Changes to This Policy

We may update this Policy periodically. If material changes are made, we will provide prominent notice and update the effective date. Continued use after the effective date means you acknowledge the updated Policy.

19. Contact and Supervisory Authorities

For questions or requests regarding this Policy or your personal data, contact privacy@glow.support.

You also have the right to lodge a complaint with a supervisory authority. In Germany, contact the competent state data protection authority; in Hungary, the NAIH; in other EEA countries, your local DPA.

Annex A – Detailed Data Categories (Illustrative)

- Identifiers: name/username, email, phone, device IDs, IP, OS/browser info.
- Special category (opt-in): sexual orientation/preferences; religion; political views; ethnicity; health data.
- UGC: photos, videos, profile text, prompts, and metadata (timestamps, geotags when enabled).
- Telemetry: events, crashes, performance metrics, A/B variant IDs.
- Security & fraud: risk flags, blocklists, device integrity scores, bot indicators.
- Financial meta: plan tier, receipts (no full card numbers).
- Support artifacts: messages, attachments, recordings (if any).

Annex B – Processor Categories and Examples

- Hosting/CDN and database providers; cloud platforms; storage/backups.
- Analytics and measurement tools; crash reporting; A/B testing frameworks.
- Identity verification and document processing providers; communications (SMS/email) gateways.
- Customer support and CRM platforms; helpdesk software.
- Payment processors and anti-fraud services.
- Content moderation vendors (where applicable).

Annex C – Legitimate Interest Assessments (Summary)

- Relevance and discovery: balancing user expectations for compatible matches with privacy by minimizing data and offering opt-outs.
- Security and abuse prevention: necessary to protect users and platform integrity; strong safeguards and narrow retention.
- Product improvement and analytics: aggregated measurement with controls; non-essential tracking requires consent in the EEA/UK.
- Customer support quality: limited access, retention windows, and audit logs.

Annex D – DPIA and Risk Management

We evaluate high-risk processing (e.g., identity verification, special category data, automated moderation) through Data Protection Impact Assessments (DPIAs) and apply supplementary safeguards (e.g., encryption, access controls, retention limits, human oversight).

Annex E – Regional Supplements

EEA/Switzerland/UK

- GDPR/UK GDPR rights apply as described; TTDSG consent required for non-essential cookies/SDKs; additional children's codes may apply in the UK.

United States (if applicable)

- We do not sell personal data as defined by certain US laws. State-specific rights (e.g., access, deletion, opt-out of targeted advertising) are available where required. A separate US addendum may apply.

This comprehensive version supersedes prior versions. For older versions or change logs, contact us at privacy@glow.support.