[aRTS] — Privacy Policy

GDPR-compliant privacy policy pursuant to Art. 13/14 GDPR, TTDSG, TMG

1. Controller (GDPR Art. 13(1)(a))

[aRTS] — operated by [TO BE FILLED: Legal Name], [TO BE FILLED: Address], Germany.
Email: arts4berlin@outlook.com
See our Impressum (impressum.html) for full legal contact details.

2. Data We Collect

We collect data only when you take an explicit action (sign in, submit a form, make a purchase). No advertising cookies, third-party tracking scripts, or analytics are used. Data is stored both on your device (browser localStorage) and on our server (encrypted SQLite database on a Hetzner VPS in Helsinki, Finland — EU jurisdiction).

3. Processing Activities & Legal Basis

Authentication (OAuth / Email+Password)

Data: Anonymised user identifier ("sub" claim), email address, display name. Passwords hashed with bcrypt.
Legal basis: Contract performance — Art. 6(1)(b)
Retention: Until account deletion

Session tokens

Data: Cryptographic session token in browser localStorage. Server stores SHA-256 hash.
Legal basis: Contract performance — Art. 6(1)(b)
Retention: 7 days (sliding window) or until logout

IP logging

Data: Encrypted IP address, login provider, tier, timestamp, encrypted user-agent.
Legal basis: Legitimate interest — security — Art. 6(1)(f)
Retention: 90 days maximum

User profile & preferences

Data: Alias, tier, join date, XP points, settings. PII encrypted with AES-GCM at rest.
Legal basis: Contract performance — Art. 6(1)(b)
Retention: Until account deletion

Favourites

Data: Piece IDs stored server-side. Client-side additionally encrypted with AES-GCM.
Legal basis: Contract performance — Art. 6(1)(b)
Retention: Until account deletion

Feedback

Data: Star rating, text (encrypted), page context.
Legal basis: Consent — Art. 6(1)(a)
Retention: Until account deletion or consent withdrawal

Newsletter

Data: Email (encrypted), name, subscription source.
Legal basis: Consent — Art. 6(1)(a)
Retention: Until unsubscribe

Payments & transactions (Stripe)

Data: Card data handled exclusively by Stripe. We store: transaction ID, amount, commission.
Legal basis: Contract — Art. 6(1)(b); Legal obligation — Art. 6(1)(c)
Retention: 10 years (AO §147, UStG §14b), pseudonymised

Algorithm & recommendations

Data: Behavioural signals (views, favourites, purchases), recommendation cache, click tracking.
Legal basis: Legitimate interest — Art. 6(1)(f)
Retention: Impressions: 180 days; cache: regenerated; deleted on account deletion

Content moderation (AI)

Data: Listing metadata, moderation verdicts, AI confidence scores.
Legal basis: Legitimate interest — platform safety — Art. 6(1)(f)
Retention: Anonymised on account deletion; audit trail retained

Form submissions (Formspree)

Data: Inquiry content, reports, art submissions.
Legal basis: Consent — Art. 6(1)(a)
Retention: Per Formspree privacy policy

4. Device Storage (TTDSG §25)

We use browser localStorage (and sessionStorage in Stealth Mode) instead of cookies. Under TTDSG §25, accessing device storage requires consent unless strictly necessary.

Strictly necessary (no consent required): session token, theme preference, CAPTCHA state, stealth mode flag.
Consent-based: feedback data, apparel voucher, view preferences, streak/XP data, bot settings, GDPR consent record.

5. Recipients & Third Parties

• Stripe (Stripe, Inc.) — payment processing

• Cloudflare (Cloudflare, Inc.) — CDN, DDoS protection, DNS

• Hetzner (Hetzner Online GmbH) — VPS hosting (Helsinki, Finland — EU)

• Formspree (Formspree, Inc.) — form submissions

• Google (Google LLC) — OAuth authentication

• Apple (Apple Inc.) — Sign In with Apple

• Resend (Resend, Inc.) — transactional emails

6. International Data Transfers

Some providers (Stripe, Cloudflare, Google, Apple, Formspree, Resend) may process data in the US. Transfers are safeguarded by the EU-U.S. Data Privacy Framework and/or Standard Contractual Clauses (Art. 46(2)(c)). Our primary database is hosted within the EU (Hetzner, Helsinki, Finland).

7. Encryption & Security

All PII is encrypted at rest using AES-GCM. IP addresses and user-agents encrypted before storage. Client-side favourites additionally encrypted with keys derived from OAuth identifier. TLS 1.2+ enforced. Server protected by UFW, fail2ban, Cloudflare-only IP whitelisting.

8. Your Rights (GDPR Art. 15-22)

Right of access (Art. 15) — Request a copy of all personal data we hold.

Right to rectification (Art. 16) — Correct inaccurate personal data.

Right to erasure (Art. 17) — Delete your account via the iD dashboard. Immediate deletion of all personal data. Transaction records pseudonymised and retained 10 years (tax law). Tombstone hash retained 3 years (fraud prevention).

Right to restriction (Art. 18) — Restrict processing in certain circumstances.

Right to data portability (Art. 20) — Receive data in structured, machine-readable format.

Right to object (Art. 21) — Object to processing based on legitimate interest.

Automated decisions (Art. 22) — AI-assisted content moderation — right to human review.

Withdrawal of consent (Art. 7(3)) — Withdraw consent at any time without affecting prior processing.

Deletion timeline: requests fulfilled within 30 days (Art. 12(3)). Self-service deletion is immediate.

9. Supervisory Authority

Berliner Beauftragte fuer Datenschutz und Informationsfreiheit
Friedrichstr. 219, 10969 Berlin — www.datenschutz-berlin.de

10. Data Retention Summary

Session tokens: 7 days (sliding) or until logout. IP logs: 90 days. User profile/favourites/settings/feedback/redemptions: until account deletion. Impressions: 180 days. Newsletter: until unsubscribe. Transaction records: 10 years (pseudonymised). Tombstone hash: 3 years. Moderation logs: indefinite (anonymised on deletion).

11. Contact

Privacy concerns and data requests: TaLK page (inquire.html) or arts4berlin@outlook.com.