Data Processing Agreement

LiteConsent

Last updated: February 22, 2026

1. Parties

This Data Processing Agreement ("DPA") is entered into between:

- **Data Controller** ("Customer", "you") — the entity that has agreed to the LiteConsent Terms of Service
- **Data Processor** ("LiteConsent", "we") — LiteConsent, operating at liteconsent.com

This DPA supplements and forms part of the LiteConsent Terms of Service (liteconsent.com/terms). By using the service, you accept this DPA.

2. Scope of processing

LiteConsent processes personal data on your behalf solely to provide the cookie consent management service. The processing includes:

Subject matter	Providing cookie consent management, recording consent decisions, and serving consent banners
Duration	For the duration of the Terms of Service agreement
Nature and purpose	Recording and storing consent decisions from website visitors to demonstrate GDPR compliance
Data subjects	Visitors to the Customer's website(s)
Categories of data	Anonymized visitor identifiers, consent decisions (categories accepted/rejected), timestamps, banner version, country/region

3. Obligations of the Processor

LiteConsent shall:

1. Process personal data only on documented instructions from the Controller, including transfers to third countries (unless required by EU or Member State law)
2. Ensure that persons authorized to process the personal data have committed themselves to confidentiality

3. Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk (see Section 6)
4. Not engage another processor without prior written authorization of the Controller (see Section 7 for current sub-processors)
5. Assist the Controller in responding to requests from data subjects exercising their rights under GDPR
6. Assist the Controller in ensuring compliance with Articles 32–36 GDPR (security, breach notification, DPIA, prior consultation)
7. At the choice of the Controller, delete or return all personal data after the end of the service, and delete existing copies unless EU or Member State law requires storage
8. Make available to the Controller all information necessary to demonstrate compliance with Article 28 obligations

4. Obligations of the Controller

The Customer shall:

1. Ensure that the use of LiteConsent complies with applicable data protection laws
2. Provide clear and lawful instructions to LiteConsent regarding the processing of personal data
3. Maintain appropriate privacy policies on their website(s)
4. Ensure they have a lawful basis for the data processing carried out through LiteConsent

5. Data location and transfers

All consent records and primary databases are stored in **Germany (EU)**, hosted by Hetzner Online GmbH.

Where sub-processors are located outside the EU/EEA, we ensure appropriate safeguards are in place through Standard Contractual Clauses (SCCs) adopted by the European Commission. See our Sub-processors page (liteconsent.com/sub-processors) for the current list.

6. Security measures

LiteConsent implements the following technical and organizational measures (Article 32 GDPR):

Encryption

- All data encrypted in transit (TLS 1.2+)
- Passwords hashed with Argon2id (m=64MB, t=3, p=4)
- TOTP secrets encrypted with AES-256-GCM at rest

- Session tokens hashed with SHA-256

Access control

- Role-based access control (Owner, Admin, Editor)
- Two-factor authentication (TOTP) available for all accounts
- Secure session management with HttpOnly, Secure, SameSite cookies

Data minimization

- Visitor identifiers are randomly generated (8 cryptographically random bytes, not derived from any personal data; IP addresses are never stored)
- Consent records contain only the minimum data necessary for compliance proof
- Automatic data purging after retention period expires

Infrastructure security

- DDoS protection via Cloudflare
- Rate limiting on all API endpoints
- CSRF protection on all state-changing operations
- Security headers (HSTS, X-Frame-Options, CSP)

7. Sub-processors

The Controller authorizes the use of the sub-processors listed at liteconsent.com/sub-processors.

LiteConsent will notify the Controller at least **30 days** before adding or replacing a sub-processor, giving the Controller the opportunity to object. If the Controller objects and a reasonable alternative cannot be found, either party may terminate the agreement.

8. Data breach notification

LiteConsent shall notify the Controller without undue delay (and in any event within **72 hours**) after becoming aware of a personal data breach. The notification shall include:

- The nature of the breach, including approximate number of data subjects and records affected
- The likely consequences of the breach
- The measures taken or proposed to address the breach
- Contact details for the LiteConsent point of contact

9. Data retention and deletion

Consent records are retained according to the Customer's plan:

- **Basic:** 1 year
- **Pro:** 2 years
- **Business:** 3 years

Records are automatically purged after the retention period. Upon account termination, all data is permanently deleted within 30 days. The Customer may export their data (CSV) at any time before deletion.

10. Audits

LiteConsent shall make available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR and allow for and contribute to audits conducted by the Controller or an auditor mandated by the Controller.

Audits shall be conducted with reasonable notice (at least 30 days), during normal business hours, and shall not unreasonably interfere with LiteConsent's operations.

11. Contact

For any questions about this DPA, contact support@liteconsent.com.

12. Governing law

This DPA is governed by the laws of England & Wales, without prejudice to the mandatory provisions of the GDPR or other applicable EU data protection law.
