

Data Processing Agreement

FlexyConsent · Westcoast Technology Limited · Company number 12008657 · Last updated: October 17, 2026

The current version is published at <https://flexyconsent.com/data-processing-agreement/>

This Data Processing Agreement ("DPA") forms part of the FlexyConsent [Terms of Use](#). It applies whenever FlexyConsent processes personal data of a Publisher's website visitors on the Publisher's behalf. By using FlexyConsent, the Publisher accepts this DPA. A signed copy is available on request from support@flexyconsent.com.

1. Parties and roles

- **Processor:** Westcoast Technology Limited, a company registered in England and Wales, company number 12008657, registered office 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom, trading as FlexyConsent ("FlexyConsent", "we").
- **Controller:** the person or organisation that holds a FlexyConsent publisher account and installs FlexyConsent on its websites, apps or stores (the "Publisher", "you").

The Publisher decides why visitor data is collected: to show a consent notice, record visitors' choices and prove them. FlexyConsent processes that data only to provide the service. For the Publisher's own account and billing data, FlexyConsent is an independent controller under its [Privacy Policy](#), and this DPA does not apply to that data.

2. Definitions

- **Data Protection Law:** the EU General Data Protection Regulation 2016/679 ("EU GDPR"), the UK GDPR and Data Protection Act 2018, and any other privacy law that applies to the processing, including US state privacy laws, Canada's PIPEDA and Quebec's Law 25, Brazil's LGPD and Türkiye's KVKK.
- **Personal Data:** personal data, as defined by Data Protection Law, that FlexyConsent processes for the Publisher under this DPA.
- **Visitor:** a person who visits a Publisher website, app or store where FlexyConsent is installed.
- **Service:** the FlexyConsent consent management platform, including the consent banner, consent logs, cookie scanner, form and checkout consent records, reports and panel.
- **Sub-processor:** a third party that FlexyConsent engages to process Personal Data.
- **Security Incident:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

Other terms (controller, processor, processing, data subject, supervisory authority) have the meanings given in Data Protection Law. US laws' terms "business", "service provider" and "processor" correspond to Controller and Processor here.

3. Details of the processing

FlexyConsent processes only pseudonymous data about Visitors' consent choices. It stores no names, email addresses or IP addresses in consent records.

Item	Details
Subject matter	Showing the consent notice on the Publisher's sites, applying and recording Visitors' choices, and reporting on them
Nature and purpose	Collection, storage, retrieval, aggregation, export and erasure of consent records; signalling choices to the Publisher's tags (IAB TCF, GPP, Google Consent Mode); blocking non-consented trackers in the browser
Data subjects	Visitors to the Publisher's websites, apps and stores; for form and checkout consents, the people who submit those forms or checkouts
Consent records	A random visitor identifier created in the browser; the consent decision and categories chosen; date and time; the source of the decision (banner, preferences, embed, page API, automatic); whether a Global Privacy Control signal was applied; the site domain
Statistics	Daily counts per visitor identifier: page views, banner shown, decision type, country and region, A/B test variant
Form and checkout consents	The wording shown, the purposes accepted or refused, a random event and subject identifier, date and time. No form field contents, no IP address
Data on the Visitor's device	Consent cookies and browser storage (for example <code>_fc_consent_data</code> , <code>euconsent-v2</code> , <code>IABTCF_*</code> , <code>_gpp</code> , <code>usprivacy</code>) that hold the Visitor's choices. These stay on the device and are listed in the consent notice
Transient data	The Visitor's IP address and browser user agent are received with each request. The IP address is used only to find the country and region that decide which privacy law applies. It is not stored in consent records. Web server access logs that contain it are deleted after at most 15 days
Special categories	None. The Publisher must not configure the Service to collect special category data
Frequency	Continuous, on every page view of a site where FlexyConsent is installed
Duration	The term of the Publisher's account, plus the deletion periods in section 9

The cookie scanner visits the Publisher's public pages to list the cookies and trackers they set. It acts as a visitor that accepts all cookies and does not collect Visitors' personal data.

4. Processor obligations

FlexyConsent will:

1. Process Personal Data only on the Publisher's documented instructions. These instructions are this DPA, the Terms of Use and the settings the Publisher chooses in the panel or through the API. If an instruction appears to break Data Protection Law, FlexyConsent will tell the Publisher.
2. Not sell or share Personal Data, and not use it for its own purposes, advertising, profiling or analytics. It will not combine it with data from other customers or sources, except to provide the Service.
3. Ensure that everyone authorised to process Personal Data is bound by confidentiality.
4. Help the Publisher answer Visitors' requests to exercise their rights. The panel and API let the Publisher look up, export and erase a Visitor's consent records by visitor identifier, and erase a

whole project's records.

5. Help the Publisher, as far as is reasonable, with security, breach notifications, data protection impact assessments and consultations with supervisory authorities.
6. Make available the information needed to show compliance with this DPA, as described in section 10.

The Publisher is responsible for its configuration choices, for having a lawful basis and a privacy notice, and for the accuracy of the cookie declarations it edits.

5. Security

FlexyConsent applies technical and organisational measures appropriate to the risk, including:

- Encryption in transit: all traffic between browsers, our edge servers and the application uses HTTPS (TLS).
- Data minimisation: consent records are keyed by a random identifier; no IP address, name or email address is stored with them.
- Network restrictions: the database accepts connections only from our own servers and a short list of administration addresses.
- Access control: production access is limited to named FlexyConsent staff, who use personal SSH keys; panel accounts are protected by passwords or Google sign-in, and panel sessions expire.
- Separation: each Publisher can see only its own projects and records.
- Resilience: two application copies behind four load balancers, and regular database backups.
- Logging: request logs omit credentials and API keys, and are kept for at most 15 days.

FlexyConsent may update these measures if the overall level of protection does not decrease.

6. Sub-processors

FlexyConsent uses one sub-processor. No other third party receives Visitors' Personal Data.

Sub-processor	Service	Location	Data
OVH SAS (OVHcloud), Roubaix, France	Server hosting (infrastructure only)	Application and database: Gravelines, France. Edge servers: France and Canada	All Personal Data is stored on, or passes through, these servers. OVHcloud does not access its content

The Publisher gives general authorisation for FlexyConsent to engage sub-processors. FlexyConsent will announce any new sub-processor at least 30 days in advance by email or on the website. The Publisher may object on reasonable data protection grounds within that period; if no solution is found, the Publisher may end the Service and receive a pro-rata refund of prepaid fees. FlexyConsent imposes data protection obligations on each sub-processor equivalent to this DPA and stays responsible for its performance.

7. International transfers

FlexyConsent is established in the United Kingdom and stores Personal Data in France. Some requests are served by an edge server in Canada. Backup copies are moved each night to

FlexyConsent's own storage in its office in the EU/EEA; no third party holds them.

- **EU and EEA to the UK and Canada:** covered by the European Commission's adequacy decisions for the United Kingdom and for Canada (commercial organisations).
- **UK to France and Canada:** covered by the UK adequacy regulations for the EEA and for Canada.
- **Other countries:** where Data Protection Law requires a transfer mechanism and no adequacy decision applies, the EU Standard Contractual Clauses (Commission Decision 2021/914, Module 2 or 3), with the UK International Data Transfer Addendum where relevant, are incorporated by reference.
- If an adequacy decision is withdrawn, the Standard Contractual Clauses apply automatically to the affected transfers.

8. Security Incidents

FlexyConsent will notify the Publisher without undue delay, and within 48 hours, after becoming aware of a Security Incident that affects the Publisher's Personal Data. The notice goes to the account email address. It will describe, as far as known: what happened, the categories and approximate number of Visitors and records affected, the likely consequences, and the measures taken or proposed. FlexyConsent will update the Publisher as more facts emerge. A notice is not an admission of fault.

9. Retention and deletion

- **Consent records:** deleted automatically 2 years after they were last updated. The Publisher can export them at any time before then.
- **Daily statistics per visitor identifier:** deleted automatically after 60 days. Totals without a visitor identifier are kept for reporting.
- **Visitor identifiers:** deleted automatically 380 days (about 13 months) after the Visitor's last visit.
- **Form and checkout consent records:** deleted automatically 2 years after they were recorded. A checkout record is kept as long as any later decision of the same shopper is, so a withdrawal never loses the decision it withdraws.
- **On request:** the Publisher can erase one Visitor's records, or all records of a project, at any time in the panel or through the API. Erasure is immediate in the live database.
- **On project or account deletion:** all Personal Data of that project is deleted within 30 days.
- **Backups:** the database is backed up every night. Backups are kept daily for 14 days, weekly for 8 weeks and monthly for 12 months, then deleted. Erased data is not restored to the live service, except to recover from a disaster, and then the erasure is applied again.
- **Visitors' devices:** consent cookies and browser storage expire as stated in the consent notice; the Visitor can delete them at any time.

FlexyConsent will keep Personal Data longer only where law requires it, and then only for that purpose.

10. Audits

On written request, at most once a year, FlexyConsent will answer a reasonable security and privacy questionnaire and provide the information needed to show compliance with this DPA. If that is not enough, or a supervisory authority requires it, the Publisher or an independent auditor bound by confidentiality may audit FlexyConsent with 30 days' notice, during business hours, at the Publisher's cost, without access to other customers' data.

11. Liability

Each party's liability under this DPA is subject to the limits in the Terms of Use. Those limits do not restrict a party's liability to data subjects, or to supervisory authorities, where Data Protection Law does not allow it.

12. Term, precedence and law

- This DPA lasts as long as FlexyConsent processes Personal Data for the Publisher.
- If this DPA conflicts with the Terms of Use, this DPA prevails for the processing of Personal Data. The Standard Contractual Clauses, where they apply, prevail over both.
- FlexyConsent may update this DPA to reflect changes in law or the Service. Material changes will be announced 30 days in advance and will not reduce the protection of Personal Data.
- This DPA is governed by the laws of England and Wales, and its courts have exclusive jurisdiction, except where the Standard Contractual Clauses require another law or court.

Contact

Data protection questions, requests and incident reports: support@flexyconsent.com.

Westcoast Technology Limited · 71-75 Shelton Street, Covent Garden, London WC2H 9JQ, United Kingdom · Company number 12008657