

Data Processing Agreement

AI Services LLC (OpenWAF) · Version 2026-10-27. Published at <https://openwaf.dev/legal/dpa/>. Accepted electronically at sign-up, without a separate signature (section 1).

This is an English translation provided for convenience. In case of any discrepancy, the Spanish version prevails.

In short

- For the traffic of your websites, your DNS zones and the other data in Annex I, you are the controller and we are your processor (art. 28 GDPR), and your service provider under the CCPA/CPRA.
- We only process that data following your instructions, which are the configuration you set through the dashboard, the API, the CLI or the MCP server.
- Data stay in the European Union: Germany (Hetzner) and, for the Madrid edge node, Spain (Vultr). Our sub-processors are listed in Annex III and on the [Sub-processors](#) page.
- We will tell you about a personal data breach without undue delay and in any event within 72 hours of becoming aware of it.
- Transfers outside the EEA rely on the EU Standard Contractual Clauses (modules 2 and 3), incorporated in section 9, and the UK Addendum.
- Security events expire after 30 days; your data are deleted within 30 days of closing your account, and from backups within 6 months.

1. Parties and incorporation

This Data Processing Agreement ("DPA") is entered into between the customer that uses OpenWAF Cloud (the "Customer"), as controller, and AI Services LLC, trade name OpenWAF, 99 Wall Street #2351, New York, NY 10005, USA ("OpenWAF"), as processor. It forms part of the [Terms of Service](#) and is concluded when the Customer accepts it at sign-up, by ticking its box before the Customer's organisation is created, without the need to sign it separately. OpenWAF records the version accepted (identified by its date, currently 2026-10-27), the accepting user and the date and time of acceptance. If the Customer is an agency acting on behalf of its own clients, the Customer acts as processor for them, and OpenWAF acts as its sub-processor under the same terms.

2. Subject matter, duration, nature and purpose

- **Subject matter:** the processing of personal data needed to provide the authoritative DNS, web application firewall (WAF), edge cache and related services for the Customer's domains and websites, and the AI egress gateway if the Customer enables it.
- **Duration:** while the Customer uses the service, and afterwards until the data are deleted as described in section 10.
- **Nature:** receiving, inspecting, filtering, caching, forwarding and logging HTTP(S) requests to the Customer's proxied hostnames; answering DNS queries; sending access-gate e-mails; collecting real-user performance measurements if enabled; inspecting and forwarding the requests of the Customer's AI agents to the providers the Customer chooses if AI egress is enabled; storing the Customer's configuration.

- **Purpose:** protecting and accelerating the Customer's websites, serving its DNS zones and protecting the outbound calls of its AI agents, as configured by the Customer.

The details are in [Annex I](#).

3. Documented instructions

OpenWAF processes personal data only on the Customer's documented instructions, unless the law requires otherwise; in that case OpenWAF will inform the Customer before processing, unless the law prohibits it. The configuration the Customer sets through the dashboard, the API, the CLI or the MCP server, together with this DPA and the Terms of Service, constitutes the Customer's instructions. OpenWAF will tell the Customer if, in its opinion, an instruction infringes data protection law.

The Customer is responsible for having a legal basis for the processing, for informing the visitors of its websites and the people it authorises in the access gate, and for the lawfulness of its instructions.

4. Confidentiality

OpenWAF ensures that the people authorised to process personal data have committed themselves to confidentiality or are under an appropriate legal obligation of confidentiality, and that this obligation continues after their engagement ends.

5. Security

OpenWAF applies the technical and organisational measures described in [Annex II](#), appropriate to the risk in accordance with article 32 GDPR. OpenWAF may update those measures as long as the overall level of security is not reduced. The current status of our security programme is published on our [security page](#).

6. Sub-processors

The Customer gives OpenWAF a general written authorisation to engage the sub-processors listed in [Annex III](#), which are also published on the [Sub-processors](#) page. OpenWAF will inform the Customer by e-mail to the account's owners at least 30 days before adding or replacing a sub-processor. The Customer may object within that period on reasonable data-protection grounds; if the parties do not reach a solution, the Customer may terminate the service. OpenWAF imposes on each sub-processor, by contract, data protection obligations that offer at least the same level of protection as this DPA and remains responsible to the Customer for their performance.

Providers that the Customer itself chooses and contracts, such as the AI model providers it configures in AI egress with its own API keys, or its own origin servers, are not OpenWAF sub-processors: OpenWAF forwards data to them only on the Customer's instruction.

7. Assistance to the Customer

Taking into account the nature of the processing, OpenWAF will help the Customer, as far as possible:

- to answer requests from data subjects exercising their rights. If OpenWAF receives such a request directly, it will forward it to the Customer without undue delay and will not answer it itself, unless the Customer instructs it to;

- to meet its obligations on security, breach notification, data protection impact assessments and prior consultation with the supervisory authority (articles 32 to 36 GDPR), with the information available to OpenWAF.

8. Personal data breaches

OpenWAF will notify the Customer of any personal data breach affecting the Customer's data without undue delay, and in any event within 72 hours, after becoming aware of it, by e-mail to the account's owners. The notification will include, as far as available, the information listed in article 33(3) GDPR: the nature of the breach, the categories and approximate number of data subjects and records concerned, a contact point, the likely consequences and the measures taken or proposed. Information not available at first may be provided in phases. OpenWAF will take reasonable steps to contain the breach and mitigate its effects, and will not inform third parties of a breach affecting the Customer's data without the Customer's agreement, unless the law requires it.

9. International transfers

Customer data are stored and processed in the European Union (Germany and, for the Madrid edge node, Spain). AI Services LLC is established in the United States, its staff and contractors may access the data from outside the European Economic Area (EEA), and some sub-processors in Annex III are established in the United States. For any such transfer:

- the parties incorporate by reference the [Standard Contractual Clauses](#) approved by Commission Implementing Decision (EU) 2021/914 ("SCCs"): Module 2 (controller to processor) where the Customer is a controller, and Module 3 (processor to processor) where the Customer is a processor. The Customer is the data exporter and OpenWAF the data importer;
- in the SCCs: clause 7 (docking clause) applies; in clause 9, option 2 (general written authorisation) applies, with the notice period of section 6; the optional wording of clause 11 does not apply; in clause 17, option 1 applies and the governing law is the law of Spain; in clause 18, the courts of Spain are chosen; the competent supervisory authority under clause 13 is the one indicated in Annex I.C; Annexes I, II and III of this DPA complete the annexes of the SCCs;
- for data subject to the UK GDPR, the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner (version B1.0) applies, completed with the information in this DPA; for data subject to the Swiss Federal Act on Data Protection, the SCCs apply with the Swiss Federal Data Protection and Information Commissioner as competent authority and references to the GDPR read as references to that Act;
- in case of conflict between this DPA and the SCCs, the SCCs prevail.

10. Deletion and return of data

- Security events, real-user monitoring measurements, AI-bot reports and AI egress block events expire and are deleted 30 days after they are recorded.
- When the account is closed, OpenWAF deletes the Customer's data from its live systems, including its configuration, access-gate e-mail addresses, certificate private keys and AI egress provider keys, within 30 days, unless the law requires it to keep them. Copies in backups are deleted when the backups expire, at most 6 months later, and are not restored to live systems in the meantime except to recover from an incident.
- Before closing the account, the Customer may retrieve its configuration through the API or the CLI, or ask OpenWAF at support@openwaf.dev for a copy. On request, OpenWAF will confirm the

deletion in writing.

11. Information and audits

OpenWAF will make available to the Customer the information necessary to demonstrate compliance with article 28 GDPR, including a description of its security programme and its status, and will allow and contribute to audits, including inspections, by the Customer or an independent auditor it appoints.

Audits require reasonable prior notice, are carried out at the Customer's cost, are subject to confidentiality, must not compromise the security of other customers and may take place once a year, unless there has been a personal data breach or a supervisory authority requires it. Where OpenWAF obtains an independent audit report in the future, the Customer agrees to rely on it first, to the extent it covers the matters to be audited.

12. Records of processing

OpenWAF keeps a record of the categories of processing it carries out on behalf of its customers, as required by article 30(2) GDPR, and will make it available to the competent supervisory authority on request.

13. CCPA/CPRA service provider terms

To the extent the California Consumer Privacy Act as amended by the California Privacy Rights Act applies to personal information OpenWAF processes for the Customer, OpenWAF acts as the Customer's service provider and will not: sell or share that personal information; retain, use or disclose it for any purpose other than providing the service described in section 2, or outside the direct business relationship with the Customer; or combine it with personal information it receives from other sources, except as the law permits. OpenWAF will comply with the obligations that apply to it under the CCPA/CPRA, provide the same level of privacy protection the law requires, and notify the Customer if it can no longer meet them. The Customer may take reasonable steps to stop and remediate unauthorised use. OpenWAF certifies that it understands these restrictions.

14. Liability and order of precedence

The liability of each party under this DPA is governed by the [Terms of Service](#), to the extent permitted by law and without limiting the rights of data subjects under the SCCs. In case of conflict between this DPA and the Terms of Service on the processing of personal data, this DPA prevails.

Annex I. Details of the processing

A. List of parties

Data exporter

The Customer, as identified in its account (name, address and contact e-mail of the account owner).
Role: controller or, for agencies acting for their clients, processor. Activities: use of OpenWAF Cloud for its domains and websites. Signature and date: acceptance at sign-up, recorded as described in section 1.

Data importer

AI Services LLC (OpenWAF), 99 Wall Street #2351, New York, NY 10005, USA. Contact: support@openwaf.dev; security: security@openwaf.dev. Role: processor or sub-processor. Activities: the services described in section 2. Signature and date: as for the data exporter.

B. Description of the processing

Categories of data subjects

Visitors of the Customer's websites and users of its DNS zones; people the Customer authorises in the access gate; users of the Customer's AI agents, if AI egress is enabled; the Customer's staff and members of its account.

Categories of personal data

IP addresses; request metadata, including hostname, path, method and headers such as the user agent; TLS fingerprint; country and autonomous system number (ASN) derived from the IP address; security-event details (time, status, action, rule, attack type and message); access-gate e-mail addresses and one-time codes; real-user monitoring measurements (page path, performance metrics, country and device class, without storing the IP address or user agent); AI-bot classification of requests; for AI egress, the content of the requests of the Customer's AI agents, inspected in memory and not stored, and block events (time, agent, target, detection identifiers, client IP address, method and path, never the request body). DNS queries are processed to answer them. Responses of the Customer's websites may be cached on edge nodes as the Customer configures.

Special categories of data

None intended. The service is not designed to process special categories of data; any such data in the content of requests are processed only in transit or in the cache the Customer configures.

Frequency

Continuous, while the service is in use.

Retention

Security events, real-user monitoring measurements, AI-bot reports and AI egress block events: 30 days. Configuration and account data: while the account exists, and up to 30 days after it is closed. Backups: database backups 90 days, system backups at most 6 months.

Transfers to sub-processors

As described in Annex III, for the duration of the processing.

C. Competent supervisory authority

The supervisory authority of the EU Member State where the Customer is established or, if the Customer is not established in the EU, the Spanish Data Protection Agency (AEPD).

Annex II. Technical and organisational measures

- **Location:** control plane, databases, DNS servers and mail server hosted in the European Union (Hetzner, Germany); edge nodes in Germany (Hetzner) and Spain (Vultr, Madrid).
- **Encryption in transit:** TLS for visitors, origins and the configuration documents sent to edge nodes, with hybrid X25519 + ML-KEM-768 key exchange preferred; origin certificate verification (full strict) and mutual TLS towards origins where the Customer enables it.
- **Encryption at rest:** private keys of uploaded and imported certificates and the ACME account encrypted with AES-256-GCM; file-system backups encrypted on the client side before they leave the server.

- **Integrity of configuration:** configuration documents signed with Ed25519 and verified by edge nodes before use; nodes keep serving the last valid configuration if the control plane is unreachable.
- **Access control:** passwordless sign-in (one-time e-mail codes, or Google or GitHub accounts with a verified e-mail address); sessions in HttpOnly, Secure cookies with CSRF protection; roles and scoping of members and tokens to one client or zone; API tokens stored only as hashes, with mandatory expiry (at most 365 days); OAuth 2.1 with PKCE for the MCP server.
- **Tenant isolation:** customer data are reached only through each organisation's own scope, covered by automated cross-tenant tests.
- **Secrets management:** AI egress provider keys and infrastructure secrets kept in a dedicated secrets manager (OpenBao), with least-privilege roles: the control plane can write provider keys but not read them, and the gateway can read them but not write them.
- **Change management:** versioning of the configuration with history, comparison and rollback; mandatory reason for every change and audit log of who changed what, when and why.
- **Network security:** hidden DNS primary reachable only by the public secondaries; host and provider firewalls; administrative access restricted by firewall rules; databases reachable only from our own hosts.
- **Availability:** several edge nodes with health-checked DNS answers that remove a failed node in about a minute; two DNS secondaries in separate data centres; continuous external monitoring of edge nodes, DNS, control plane and certificates with alerting; daily backups to separate storage in the EU.
- **Vulnerability management:** daily automated scanning of deployed code, dependencies, container images and operating-system packages, prioritised with the CISA Known Exploited Vulnerabilities catalogue and EPSS; secret scanning in the continuous integration of our public open-source repository and before every publication of this website.
- **Data minimisation:** automatic expiry of events after 30 days; no storage of IP address or user agent for real-user monitoring; AI egress never stores request bodies.
- **Organisation:** an information security management system aligned with ISO/IEC 27001:2022 with documented policies (access control, cryptography, suppliers, secure development, logging, backup and continuity, incident response, vulnerability management), a risk register and a documented incident response procedure; access limited to the people who need it.

Annex III. Sub-processors

Sub-processor	Location	Processing of Customer data
Hetzner Online GmbH	Germany (EU)	Infrastructure: control plane, databases, DNS servers, edge nodes, mail server (access-gate e-mails) and backup storage.
The Constant Company, LLC (Vultr)	Madrid, Spain (EU)	Infrastructure of the Madrid edge node: traffic of visitors routed to that node (TLS termination, WAF, cache).
Cloudflare, Inc.	USA (global network)	Network proxy in front of the dashboard, the control-plane endpoint our edge nodes use to fetch their configuration (configuration documents, which may include access-gate e-mail addresses and certificate private keys) and the AI egress endpoint (requests of the Customer's AI agents, if enabled). Content is decrypted at Cloudflare in transit.

Sub-processor	Location	Processing of Customer data
Internet Security Research Group (Let's Encrypt)	USA	Issuing TLS certificates. Receives hostnames only.