Data Processing Agreement (DPA)

ALTIUS HOST LLC | Last Updated: November 12, 2026

1. Scope and Role of the Parties

This Data Processing Agreement ("DPA") forms an integral part of the Terms of Service between ALTIUS HOST LLC ("Processor", "we", "us") and the Client ("Controller", "you"). It is automatically accepted upon acceptance of the Terms of Service and applies whenever the Client uses our hosting infrastructure to process personal data that is subject to a data protection law imposing obligations on controllers and processors — including, without limitation, personal data of individuals located in the European Economic Area ("EEA"), the United Kingdom, or Switzerland.

For the avoidance of doubt:

- **The Client acts as the Data Controller** in respect of all personal data contained within websites, databases, email accounts, and applications hosted on our infrastructure.
- **ALTIUS HOST LLC acts as the Data Processor** in respect of that data, processing it solely to provide the contracted hosting services.
- ALTIUS HOST LLC acts as an independent **Controller** in respect of its own account, billing, and tax-compliance data, which is governed by our Privacy Policy rather than this DPA.

This DPA is entered into in accordance with Article 28 of Regulation (EU) 2016/679 ("GDPR") and, where applicable, the UK GDPR, the Swiss Federal Act on Data Protection, and any other data protection law requiring a written processing agreement. Where such a law imposes requirements beyond those set out here, those requirements apply to the extent of the difference.

2. Subject Matter, Duration, Nature and Purpose

Subject matter: The provision of managed web hosting, cloud infrastructure, and related technical services.

Duration: For the entire term of the Client's active service subscription, plus any retention period set out in Section 10 below.

Nature and purpose of processing: Storage, hosting, transmission, backup, and technical maintenance of Client data as necessary to deliver the contracted services, including — for Clients who order Managed Edge Security — configuration and monitoring of the Client's own Cloudflare account through member access granted by the Client. We do not access, analyse, or use Client content for any purpose other than service delivery, technical support requested by the Client, security incident response, and legal compliance.

Types of personal data: Determined entirely by the Client. This may include names, email addresses, postal addresses, telephone numbers, IP addresses, account credentials, transaction records, and any other data the Client chooses to store. For Managed Edge Security, this additionally includes the IP addresses, request metadata, and security-event records of visitors to the Client's website, as displayed in the Client's Cloudflare account.

Categories of data subjects: Determined entirely by the Client. This may include the Client's own customers, website visitors, employees, suppliers, and other individuals.

3. Instructions from the Controller

We process personal data only on documented instructions from the Client, including with regard to transfers to third countries, unless required to do otherwise by applicable law. Where we are required by law to process data

beyond the Client's instructions, we will inform the Client of that legal requirement before processing, unless the law prohibits such notification on important grounds of public interest.

The Client's instructions are constituted by: (a) the Terms of Service; (b) this DPA; (c) the Client's configuration of and use of the services; and (d) any written instructions submitted through our support channels.

We will inform the Client if, in our opinion, an instruction infringes the GDPR or other applicable data protection law.

4. Confidentiality

All personnel authorised to process personal data on our behalf are bound by written confidentiality obligations that survive the termination of their engagement. Access to Client data is granted strictly on a need-to-know basis and is limited to what is necessary for service delivery, technical support, and security incident response.

5. Security Measures (Article 32)

We implement and maintain appropriate technical and organisational measures, including:

- **Encryption in transit:** All data in transit is encrypted. TLS/HTTPS is enforced across every client-facing connection — the public website, the client portal, the checkout and payment flow, the hosting control panel, webmail, and API endpoints — as well as on all administrative access and on the transfer of backup archives between systems. Payment card data is transmitted directly to a PCI-compliant payment gateway over an encrypted channel and never traverses our infrastructure in plain form.
- **Data at rest:** Client data resides on servers in access-controlled data centres within the EEA. **Encryption is not applied at the storage layer:** production storage volumes are not encrypted at the disk level, and backups are stored unencrypted. Protection of data at rest therefore rests on physical data centre security, operating-system access controls, account isolation, and restricted, logged administrative access rather than on cryptographic measures.

Clients whose own risk assessment requires encryption at rest should implement it within their own environment — for example, application-level or database-level encryption, or encrypting exports before storing them elsewhere. We are happy to advise on configuration.

- **Isolation:** CloudLinux isolated environments providing account-level separation between tenants on shared infrastructure.
- **Privileged access control:** Multi-factor authentication is enforced on every administrative interface through which Client data can be reached, including the server control panel, the client portal and billing system, and our accounts with each infrastructure provider. Role-based permissions apply to administrative accounts, and privileged operations are logged.
- **Client-side authentication:** Multi-factor authentication is available to Clients on both their hosting control panel and their client portal account. We strongly recommend enabling it; account compromise arising from the Client's own credential handling is the Client's responsibility under the Terms of Service.
- **Network security:** Perimeter firewalling and intrusion detection via **ConfigServer Security & Firewall (CSF/LFD)**, with real-time malware scanning, exploit detection, brute-force protection, and application-layer firewalling via **Imunify360** and **ModSecurity**. These measures operate on our own infrastructure and apply to every hosted account by default.
- **Edge protection is not a default measure.** Content delivery network, edge web application firewalling, and edge DDoS mitigation are **not** applied to hosted accounts by default: hosting origin servers accept web traffic directly. Edge protection is available only as the separately ordered Managed Edge Security service described in Schedule A of the Terms of Service, and is then delivered through the Client's own Cloudflare account rather than through infrastructure we control.

- **Backup and recovery:** Automated daily backups held on separate backup storage within the EEA on a rolling seven (7) day rotation; the backup storage also keeps daily snapshots of itself for seven (7) days. Backups of a terminated account are retained for thirty (30) days after termination and are then permanently deleted (Section 10). Backups are provided on a best-effort basis without warranty as to existence, completeness, integrity, or restorability, and reside on leased third-party infrastructure outside our direct physical control. Point-in-time and long-term archival recovery are not provided. The Controller is responsible for maintaining independent backups where its retention, integrity assurance, or recoverability requirements exceed this.
- **Physical security:** Data centres operate under certified access control, video surveillance, and environmental protection regimes.
- **Monitoring and patching:** Continuous infrastructure monitoring and timely application of security updates.

The Client remains responsible for the security of its own application layer, including software updates, plugin management, credential hygiene, and independent backups of its own data.

6. Sub-processors

The Client provides general written authorisation for us to engage sub-processors. We impose data protection obligations on each sub-processor that are no less protective than those set out in this DPA, and we remain fully liable to the Client for the performance of each sub-processor's obligations.

The sub-processors we engage, together with those we have disclosed in advance of engaging, are listed below. This list is maintained on this page and is accurate as at the date shown at the top of this document:

Sub-processor	Purpose	Location	Status
Hetzner Online GmbH	Physical server infrastructure and backup storage	Germany, Finland	Active
WHMCS Ltd	Client portal, billing, and support ticketing; processes personal data from hosted content only where the Client includes it in a support ticket	United States (Houston, Texas)	Active
OVH SAS	Physical server infrastructure	France, Netherlands	Planned — not yet in use
MailBaby (InterServer, Inc.)	Outbound mail relay for hosted accounts	United States	Active

Sub-processor	Purpose	Location	Status
Cloud Linux Software, Inc. (CloudLinux)	Server security software (Imunify360) and account isolation software (CloudLinux OS). To detect and block attacks and malware, Imunify360 sends CloudLinux information about suspicious activity on hosted websites, including visitor IP addresses, requested URLs, request headers, the data submitted in requests identified as attacks, and the names and attributes of files flagged as malicious. Automatic upload of hosted files for analysis is disabled	United States, with processing in Germany, Finland, Poland, and the United States	Active
WebPros International GmbH and its group affiliates	Server monitoring and read-only administrative access to hosting accounts through the WebPros Dashboard and its MCP interface, used by our staff for administration and support; and the AI Assistant in the cPanel Meridian interface, which processes the Client's questions and the account information needed to answer them, using third-party AI model providers engaged by WebPros as its own sub-processors, and may retain conversations for quality and support purposes	Switzerland, with group affiliates in other countries including the United States	Active
Anthropic, PBC	AI assistant (Claude, under Anthropic's commercial terms) used by our staff for server administration, log review, and configuration support; processes Client data only to the extent contained in the information reviewed	United States	Active

Other service providers. The following providers support our own website, account management, fraud prevention, and domain registration. They process account, billing, and website-visitor data for which we act as an independent Controller under our Privacy Policy, and they do not process the personal data contained in your hosted content:

Provider	Purpose	Location
Cloudflare, Inc.	DNS and edge protection for our own website and corporate systems; not applied to hosted Client accounts by default (see Section 5)	Global
Namecheap, Inc.	Domain registration and management	United States
MaxMind, Inc.	Fraud risk scoring at registration and checkout	United States
Intuition Machines, Inc. (hCaptcha)	Bot protection on login and registration forms	United States
Stripe, LLC	Payment processing and payment fraud screening	United States

Planned sub-processors. An entry marked *planned* is disclosed in advance so that you have notice of it before it is engaged, and so that you can raise any objection at the outset rather than mid-term. No Client data is processed by a planned sub-processor until it is brought into service, at which point this list is updated and its status changes to active. You may object to a planned sub-processor at any time under the paragraph below, on the same terms as an addition.

We will give the Client at least thirty (30) days' prior notice of the addition or replacement of any sub-processor. The Client may object on reasonable data protection grounds within that period; if the objection cannot be resolved, the Client may terminate the affected services without penalty and receive a pro-rata refund of prepaid fees.

Note to the Client: Our client portal, billing, and support platform is hosted in the United States, and our payment processing, banking, fraud screening, and bot protection providers are likewise United States entities. These systems hold **account, billing, and support data** — in respect of which we act as an independent Controller under our Privacy Policy — and **not** the personal data contained within your hosted websites, databases, or applications, which remains at rest within the EEA as described in Section 7.

Where you submit personal data relating to your own data subjects through a support ticket, that data is transmitted to and stored on the United States platform. We ask Clients not to include end-user personal data in support tickets except where strictly necessary to resolve a technical issue.

Client-initiated integrations. Where the Client connects its account or website to third-party services of its own choosing — including AI assistants and agents, and the cPanel MCP connection activated through the Client's own WebPros account — those services act on the Client's instructions under their own terms. They are not sub-processors engaged by us, and this DPA does not apply to data the Client sends to them. Where we ourselves use such a provider to operate or support the services — for example for server monitoring or AI-assisted administration — that provider acts as our sub-processor and is listed in the table above. The AI Assistant in the cPanel Meridian interface is enabled by us rather than connected by the Client, and WebPros processes data through it as our sub-processor.

Client's own Cloudflare account. Where the Client orders Managed Edge Security, Cloudflare provides its services to the Client directly under the Client's own agreement with Cloudflare, and is not our sub-processor for that service. We access the Client's Cloudflare account as an invited member on the Client's instructions, and any processing we carry out through that access — including review of security-event records — is covered by this DPA.

7. International Transfers

Client content data — the websites, databases, email, and applications you host with us — is stored at rest exclusively within the European Economic Area. Infrastructure is currently located in **Germany and Finland**, with planned expansion to **France and the Netherlands** as set out in the sub-processor list above. All locations, current and planned, are within the EEA. Hosted content is not transferred to or stored in the United States as part of normal service delivery.

Outbound mail relay. Where a hosted account sends email, the message is handed to our outbound mail relay, MailBaby, for delivery, and therefore passes through infrastructure located in the United States while in transit. Messages are relayed and delivered rather than stored: the relay holds a message only for as long as delivery requires, and keeps delivery logs — including the sender, the recipient, and the subject line — for up to sixty (60) days. Mailboxes, archives, and incoming mail remain on our EEA infrastructure. Clients for whom transit outside the EEA is unacceptable should configure their own outbound mail provider, and we will assist with the configuration.

Control panel AI Assistant. Where the Client uses the AI Assistant in the cPanel Meridian interface, its questions and the account information needed to answer them are processed by WebPros and the third-party AI model providers it engages, which may do so outside the EEA, including in the United States. The AI Assistant does not move the Client's websites, databases, or mailboxes, which remain on our EEA infrastructure. Clients for whom such processing is unacceptable should not use the AI Assistant.

Server security service. To detect and block attacks, Imunify360 sends information about suspicious requests and files — including visitor IP addresses, requested URLs, and request details — to CloudLinux, which may process it outside the EEA, including in the United States. Hosted websites, databases, and mailboxes are not transferred, and automatic upload of hosted files for analysis is disabled.

Account, billing, and support data is different. Our client portal, billing system, and support ticketing platform are hosted in the United States. Account details, invoices, and support correspondence are therefore stored and processed there. Where this involves a transfer of personal data from the EEA or the United Kingdom, it is carried out under the Standard Contractual Clauses referred to below.

Managed Edge Security. Hosted accounts are not served through any content delivery network operated by us or on our behalf. Where the Client orders Managed Edge Security, Cloudflare operates within the Client's own Cloudflare account under the Client's own agreement with Cloudflare, as described in Section 6. In that case, content the Client has made publicly available may be cached transiently at Cloudflare edge locations outside the EEA in order to serve visitors in those regions. Such caching is temporary and does not change where the Client's hosted data is stored, which remains within the EEA.

Where administrative or support access from outside the EEA is necessary (for example, technical support performed by our personnel), such transfers are carried out under the European Commission's Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), Module Three (processor to processor) or Module Two (controller to processor) as applicable, which are incorporated into this DPA by reference. Where the UK Addendum, the Swiss adaptations, or an equivalent transfer instrument is required for a particular transfer, that instrument applies in addition and is likewise incorporated by reference. We have conducted a transfer impact assessment covering these access scenarios and maintain supplementary measures including encryption, access logging, and minimisation of administrative access.

Transfers to sub-processors located outside the EEA, including the outbound mail relay, the server security service, and the administration tools listed in Section 6, are carried out under Module Three of the Standard Contractual Clauses concluded with the sub-processor, or under the EU–U.S. Data Privacy Framework where the sub-processor is certified under it. The details required by the Standard Contractual Clauses are set out in the Annex to this DPA.

8. Assistance to the Controller

We will provide reasonable assistance to the Client in relation to:

- **Data subject rights (Articles 12–23):** Responding to requests for access, rectification, erasure, restriction, portability, and objection. Where we receive a request directly from a data subject relating to Client content, we will not respond substantively but will forward it to the Client without undue delay.
- **Security, breach notification, and impact assessments (Articles 32–36):** Providing information reasonably available to us.

9. Personal Data Breach Notification

We will notify the Client without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a personal data breach affecting Client data. The notification will describe the nature of the breach, the categories and approximate number of data subjects and records concerned insofar as known, the likely consequences, and the measures taken or proposed to address it.

10. Deletion and Return of Data

Upon termination or expiry of the services, the Client may export its data through the client portal before the termination takes effect. Following termination, Client data is deleted from our servers, and backups of the account are retained for **thirty (30) days** to allow for recovery, after which they are permanently deleted; any residual copies in the daily snapshots of our backup storage are removed within a further seven (7) days. The retrieval of data after a switching request is governed by Schedule C of the Terms of Service.

We will not retain Client content data beyond these periods unless required by applicable law. Billing and tax records are retained separately under our own legal obligations as described in the Privacy Policy. For Managed Edge Security, our member access to the Client's Cloudflare account ends with the service, and we do not retain copies of security-event records beyond those included in reports delivered to the Client.

11. Audits and Information

We will make available to the Client all information reasonably necessary to demonstrate compliance with Article 28 GDPR, including relevant third-party certifications and audit reports held by us or our sub-processors.

Where the Client requires an audit beyond the provision of such documentation, the Client may request one no more than once per calendar year, subject to thirty (30) days' written notice, execution of a confidentiality agreement, conduct during normal business hours, and no unreasonable disruption to our operations or to other clients. The Client bears the cost of any such audit. In the case of a supervisory authority exercising its powers, the foregoing limitations do not apply.

12. Liability

Each party's liability under this DPA is subject to the limitations and exclusions set out in the Terms of Service, except where such limitation is not permitted by applicable data protection law.

13. Contact

Data protection enquiries, data subject requests, and sub-processor objections should be directed to:

Data Protection Contact

ALTIUS HOST LLC

8206 Louisiana Blvd NE, Ste A #9372

Albuquerque, NM 87113, United States

Email: privacy@altius.host

14. Precedence

In the event of a conflict between this DPA and the Terms of Service in relation to the processing of personal data, this DPA prevails.

Annex — Details for the Standard Contractual Clauses

A. List of parties

Data exporter: the Client, as identified in its account with us. Role: controller (Module Two) or, where the Client itself processes the data on behalf of another controller, processor (Module Three). Contact details: those registered in the Client's account. The Client's acceptance of the Terms of Service constitutes its signature of the Standard Contractual Clauses.

Data importer: ALTIUS HOST LLC, 8206 Louisiana Blvd NE, Ste A #9372, Albuquerque, NM 87113, United States. Contact: privacy@altius.host. Role: processor. Publication of this DPA as part of our Terms of Service constitutes our signature of the Standard Contractual Clauses.

B. Description of the transfer

- *Categories of data subjects and of personal data:* as set out in Section 2.
- *Sensitive data:* determined by the Client. The measures set out in Section 5 apply to all data, including any sensitive data the Client chooses to host.
- *Frequency of the transfer:* continuous, for the duration of the services.
- *Nature of the processing:* hosting, storage, backup, transmission (including outbound mail relay), technical support, and administrative access, as described in Sections 2 and 7.
- *Purpose:* provision of the contracted services.
- *Retention:* as set out in Section 10.
- *Transfers to sub-processors:* the subject matter, nature, and duration are the same as above, limited to the purpose stated for each sub-processor in Section 6.

C. Competent supervisory authority

Determined in accordance with Clause 13 of the Standard Contractual Clauses: the supervisory authority of the Member State in which the Client is established; where the Client is not established in the EEA but is subject to the GDPR under Article 3(2), the supervisory authority of the Member State in which its representative is established or, where no representative is required, of one of the Member States in which the data subjects concerned are located.

D. Technical and organisational measures

The measures described in Section 5 of this DPA.

E. Sub-processors

The sub-processors listed in Section 6 of this DPA.

F. Selected options

Clause 7 (docking clause) applies. Clause 9: Option 2 (general written authorisation), with the notice period set out in Section 6. Clause 11: the optional wording does not apply. Clause 13: as set out in Part C above. Clause 17: Option 1, the law of Ireland. Clause 18: the courts of Ireland.

For your administrative records, an official PDF copy of this Data Processing Agreement is available for download.