

Data Processing Agreement

Hostup AB · Version 2.0 · 26 September 2026

This version replaces [version 1.0](#), which covered VPS only. The current version is always available at <https://hostup.se/legal/dpa.pdf>.

1. Parties

Processor: Hostup AB, reg. no. 559290-1325, Mässvägen 4, 125 30 Älvsjö, Sweden ("Hostup"). Data protection contact: info@hostup.se or the support form at <https://cloud.hostup.se/contact>.

Controller: the customer who uses Hostup's services and processes personal data in them ("the Customer"). If the Customer is itself a processor for someone else, Hostup is the Customer's sub-processor, and the Customer is responsible for having its controller's authorisation for this.

2. Background and purpose

2.1 The Customer uses Hostup's services to store, send and otherwise process data. When that data contains personal data, Hostup processes it on the Customer's behalf. This agreement sets out the terms that Article 28 of the General Data Protection Regulation (EU) 2016/679 ("GDPR") requires for that processing.

2.2 This agreement forms part of Hostup's [Terms of Service](#) and applies to all of Hostup's services. In matters of personal data, this agreement prevails over the Terms of Service.

3. Definitions

Terms such as *personal data*, *processing*, *controller*, *processor*, *data subject*, *personal data breach* and *supervisory authority* have the meaning given in the GDPR. In addition:

- **Services:** the services the Customer orders from Hostup, including VPS, web hosting and reseller hosting, email, DNS, CDN and redirects, object storage (S3), backups, and support and Hostup's assistant.
- **Customer Personal Data:** personal data that the Customer, or anyone using the Customer's services, stores or processes in the Services. Examples: content on servers and websites, databases, email, files in object storage, backups, and logs containing visitors' IP addresses.
- **Sub-processor:** another provider engaged by Hostup that processes Customer Personal Data on Hostup's behalf.

4. Scope and roles

4.1 Hostup is the processor of Customer Personal Data in all Services. What is processed, why, for how long and about which data subjects is described per service in **Annex 1**.

4.2 Hostup is an independent controller, and this agreement therefore does not apply, for:

- a) the Customer's own account, contact and billing data, including data about the people the Customer gives access to the account;
- b) data about domain holders and contacts that is provided to registries and registrars when domain names are registered and managed. Registries and registrars are controllers of that data under their own terms. Where the data ends up follows from the top-level domain the Customer chooses; for example, the registry for .us is in the United States and the one for .hu in Hungary;

c) logs and data that Hostup processes to protect the platform and to prevent fraud, spam and abuse, and to meet legal obligations such as bookkeeping.

This processing is described in Hostup's [Privacy Policy](#).

5. The Customer's instructions

5.1 Hostup processes Customer Personal Data only on the Customer's documented instructions. The instructions are:

- a) this agreement and its annexes;
- b) the Customer's own choices when using the Services: settings in the client area, API calls, orders and cancellations;
- c) what the Customer asks for in a support ticket.

An instruction that goes beyond the Services, or that would require Hostup to change how the Services work, may be declined.

5.2 Hostup may process Customer Personal Data otherwise only where required by Union or Swedish law. Hostup then informs the Customer before the processing, unless the law prohibits it.

5.3 Hostup informs the Customer immediately if, in Hostup's opinion, an instruction infringes the GDPR or other data protection law. Hostup is not obliged to review the Customer's instructions or content for compliance with the law.

5.4 Hostup does not access the content of the Customer's services, except when:

- a) the Customer asks for or approves it, for example to troubleshoot in a support ticket;
- b) it is necessary to operate and protect the Services, for example automatic spam and malware filtering, or investigating abuse reported to Hostup;
- c) the law requires it.

5.5 Hostup does not log in to a VPS without the Customer's approval, except where section 5.4 b) or c) applies. Hostup sets the server's initial root password when the server is created and keeps it so that the Customer can see it in the client area. The Customer should change it; Hostup does not see a password the Customer sets inside the server.

6. The Customer's responsibilities

6.1 The Customer is responsible for having a legal basis for the processing, for informing data subjects, and for its instructions complying with the law.

6.2 The Customer is responsible for assessing whether the security measures described in Annex 3 are sufficient for the personal data it processes, in particular special categories of personal data under Article 9 GDPR, and for adding its own measures, such as encryption, where they are not.

6.3 On VPS, the Customer administers the operating system, software, updates, access and encryption. On web hosting, the Customer is responsible for its own software, such as WordPress and plugins.

6.4 The Customer is responsible for keeping its own copies of data that matters to it (Terms of Service sections 1.2 and 19.5).

6.5 The Customer answers for the persons it gives access to the Services, and for what they do with Customer Personal Data.

7. Confidentiality

7.1 Everyone working for Hostup who can access Customer Personal Data has signed a confidentiality agreement. This covers employees, and consultants and support staff who work in Hostup's systems on Hostup's instructions. Confidentiality continues after the employment or assignment ends.

7.2 Access to systems containing Customer Personal Data is granted per person and only to the extent the work requires.

7.3 Hostup does not disclose Customer Personal Data to third parties except under section 5 or 9. If an authority requests Customer Personal Data, Hostup refers the authority to the Customer where possible, and informs the Customer of the request unless the law prohibits it.

8. Security

8.1 Hostup takes the technical and organisational measures required by Article 32 GDPR. The measures are described per service in **Annex 3**.

8.2 Hostup may change the measures as technology develops, provided the level of protection is not reduced.

9. Sub-processors

9.1 The Customer gives Hostup general prior authorisation to engage sub-processors. The sub-processors are listed in **Annex 2** of the current version of this agreement, available at <https://hostup.se/legal/dpa.pdf> and in the client area under Account → Agreements & documents. Providers that do not process Customer Personal Data are not sub-processors and are not listed, for example providers of software licences, hardware and network connectivity. An external company whose staff have access to Customer Personal Data is a sub-processor, even when it works in Hostup's systems. Annex 2 has a non-public part: the Customer receives the full details of the sub-processors listed there on request, and may share them with its advisers, auditors and authorities.

9.2 Hostup enters into a written agreement with each sub-processor that gives Customer Personal Data at least the same protection as this agreement. Hostup is liable to the Customer for the sub-processor's processing as for its own.

9.3 **Changes.** Hostup keeps Annex 2 up to date. A new or replaced sub-processor is published in a new version of this agreement at least 14 days before the change takes effect, stating that date, and Hostup informs the Customer of the change, for example by email or in the client area. Where a sub-processor must be replaced without delay for security or operational reasons, Hostup uses a sub-processor already listed in Annex 2 for that purpose, and informs the Customer as soon as the change is made.

9.4 **Objection.** The Customer may object to a change before it takes effect, on grounds relating to data protection, by contacting support. Hostup then looks for a solution with the Customer. If none is found, the Customer may cancel the affected Services with effect from the date the change takes effect, so that the new sub-processor is not used for the Customer's data. That is the Customer's only remedy under this agreement for a change under section 9.3.

10. Transfers to third countries

10.1 VPS are stored in Sweden, as are all backups Hostup takes, in all Services. Websites and mailboxes are stored within the EU. This concerns where the data is stored. Some processing takes place elsewhere through the sub-processors in Annex 2, for example Cloudflare's network when the Customer uses the CDN, and MailChannels when email is delivered. Where processing takes place may vary with service, server and load.

10.2 Hostup transfers Customer Personal Data to a country outside the EU/EEA only in the cases listed in Annex 2, and only where the transfer is permitted under Chapter V GDPR. The basis may be an adequacy decision, for example the EU–US Data Privacy Framework for certified companies, or the European Commission's standard contractual clauses.

10.3 When the Customer itself sends data to recipients outside the EU/EEA, for example email to a recipient in another country, or publishes data on its website, the Customer chooses the recipient and is responsible for that disclosure. Section 10.2 covers the sub-processors Hostup chooses.

11. Assistance with data subject rights

11.1 The Customer can access, correct and delete data in the Services itself, for example through the client area, cPanel, SSH/SFTP and the API.

11.2 Where the Customer cannot do so itself, Hostup helps the Customer respond to a request from a data subject, as far as possible given the nature of the processing.

11.3 If a data subject contacts Hostup directly with a request concerning Customer Personal Data, Hostup refers the data subject to the Customer and informs the Customer. Hostup does not respond to the request itself.

12. Assistance with security, impact assessments and prior consultation

12.1 Hostup helps the Customer meet its obligations under Articles 32–36 GDPR, taking into account the nature of the processing and the information available to Hostup. This covers security, personal data breaches, data protection impact assessments and prior consultation with the supervisory authority.

12.2 Reasonable assistance under sections 11 and 12, and the information under sections 14.1 and 14.2, are provided without charge. Work that goes beyond what the nature of the processing and the information available to Hostup reasonably require, for example a data protection impact assessment carried out for the Customer, or investigations the Customer can do itself in the Services, is charged at an hourly rate agreed in advance.

13. Personal data breaches

13.1 Hostup notifies the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. Hostup does not wait until the investigation is complete.

13.2 The notification is sent to the account's email address and added as a ticket in the client area. It contains the information required by Article 33(3) GDPR, as far as it is known: what happened, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures Hostup has taken or proposes, and a contact person. Information not available at the first notification is provided as soon as it is. The Customer keeps the account's email address up to date. A notification is not an admission of fault or liability.

13.3 Hostup takes, without delay, reasonable measures to contain the breach and its consequences, and documents the breach.

13.4 The Customer, as controller, notifies the supervisory authority and informs data subjects where required. If the Customer is itself a processor, it passes the notification on to its controller.

14. Information and audits

14.1 Hostup makes available the information needed to demonstrate compliance with Article 28 GDPR: this agreement and its annexes, the incident history at status.hostup.se, and written answers to reasonable questions that these documents do not already answer. Customer-specific questionnaires, forms and audit templates need not be filled in; Hostup answers them by reference to this agreement and supplements in writing what the agreement does not already answer. For sub-processors, including the operator of the data centre, Hostup provides the information it receives from them, such as certifications and audit reports.

14.2 An audit is carried out first as a review of documentation: Hostup answers the written questions of the Customer or its auditor and provides, under confidentiality, the documentation, extracts and reports that concern the Customer's processing. Where that is not enough and a further audit, including an inspection, is necessary under Article 28(3)(h) GDPR, Hostup allows and contributes to it.

14.3 The Services run on shared infrastructure, and Hostup's hardware stands in a data centre operated by a third party. An audit therefore never gives access to other customers' systems or data, never gives independent

access to production systems, and never gives a right to open racks or handle equipment. An inspection is arranged and accompanied by Hostup. The following also applies:

- a) the Customer gives at least 30 days' notice, unless the law, a supervisory authority or concrete indications of non-compliance require a shorter period;
- b) the audit takes place during office hours and is limited to the matter it concerns. It takes place at most once every twelve months, with the same exceptions as in a);
- c) it is carried out by the Customer or by an independent auditor bound by confidentiality who does not compete with Hostup;
- d) the Customer bears the costs of the audit, including reasonable compensation for the working time Hostup spends on it beyond providing the information under sections 14.1 and 14.2. Conditions and costs must not make the right of audit ineffective;
- e) the powers of supervisory authorities are not affected.

14.4 The measures Hostup applies are described in Annex 3, and sections 14.1 and 14.2 are how Hostup shows that they are in place.

15. End of the Services

15.1 Before a service ends, the Customer can retrieve its data itself, for example by copying the data from a VPS over SSH or restoring a backup to a new VPS, taking a full backup of a web hosting account, retrieving email over IMAP, downloading files from object storage and exporting DNS zones from the client area. This is how the Customer chooses the return of its data. If the Customer cannot retrieve the data with these functions, Hostup helps on request before the service ends (section 12.2).

15.2 When a service ends, at the Customer's request or under the Terms of Service (including for non-payment), Hostup deletes Customer Personal Data in that service. The time limits per service are set out in Annex 1. Copies in Hostup's backups are deleted when their retention period expires. Data that Union or Swedish law requires Hostup to keep is kept only for that purpose.

15.3 Hostup confirms the deletion in writing if the Customer asks.

16. Liability

16.1 Between the parties, the limitation of liability in Terms of Service section 1.7 applies.

16.2 This agreement does not limit a data subject's right to compensation under Article 82 GDPR. Each party bears any administrative fines that a supervisory authority imposes on that party.

16.3 The indemnity in Terms of Service section 9.1 also covers claims and costs that arise from the Customer's breach of this agreement or of its obligations as controller, for example through instructions that infringe the law, subject to the conditions and limitations in that section.

17. Term and amendments

17.1 This agreement applies for as long as Hostup processes Customer Personal Data.

17.2 Hostup may amend this agreement. An amendment is published as a new version of this agreement at least 30 days before it takes effect, and Hostup informs the Customer of a material amendment by email or in the client area. Changes of sub-processors follow section 9. An amendment required by law, or one that does not reduce the Customer's protection, may take effect earlier. A Customer who does not accept an amendment may cancel the affected Services with effect from the date the amendment applies.

17.3 Each version has a version number and a date. Previous versions remain available, for example version 2.0 at <https://hostup.se/legal/dpa-2.0.pdf>, so the Customer can see which wording applied at a given time.

18. Conclusion of the agreement

18.1 This agreement is concluded electronically, which is written form under Article 28(9) GDPR. It applies between Hostup and every customer using the Services, from the time the Customer accepts the Terms of Service.

18.2 The agreement is available as a PDF in the client area under Account → Agreements & documents, in Swedish and English. If the versions differ, the Swedish version prevails.

19. Governing law and disputes

19.1 This agreement is governed by Swedish law. Disputes are resolved under Terms of Service section 6.

Annex 1 – Processing per service

Common to all services

- **Purpose:** providing, operating, protecting and supporting the Services the Customer has ordered.
- **Data subjects and personal data:** determined by the Customer. Typically the Customer's customers, users, employees and website visitors, with for example contact details, email and file content, data in the Customer's databases, IP addresses and logs. If the Customer stores special categories of personal data, section 6.2 applies.
- **Location:** VPS and all backups in Sweden. Websites and mailboxes within the EU, on Hostup's own servers in Sweden or at the sub-processors in Annex 2. Otherwise as set out in section 10.
- **Duration:** for as long as the service exists, and then until deletion as set out in the table. Remaining copies are not used and are deleted within the periods in the table, unless the law requires them to be kept. A switch under Terms of Service section 21 follows the periods there.

Service	What Hostup does with the data	When the service ends
VPS	Stores the server's disks and runs the server. Takes snapshots and backups according to the Customer's settings. Carries the server's network traffic.	The server and its snapshots are deleted immediately when the service ends, its backups 7 days later. For non-payment, the service ends as set out in Terms of Service section 4.2.2.
Web hosting, reseller hosting and email	Stores and runs websites, databases and email accounts. Keeps the web server's logs, which contain visitors' IP addresses. Takes daily backups and scans automatically for malware. Outgoing email is delivered through Hostup's own relay or through MailChannels.	The account is deleted when it is closed. Copies in backups are deleted within one week.
Email relay for VPS (relay.hostup.se)	Receives and delivers outgoing email from the Customer's server. Checks it automatically for spam and abuse, partly with AI.	Queued email and logs are deleted after one month.
DNS and email forwarding for domains	Stores the domain's DNS records on Hostup's primary DNS server; Cloudflare answers the DNS queries. Forwards email according to the rules the Customer sets up.	The zone and the rules are deleted when the domain leaves Hostup or when the Customer removes them.
CDN, website firewall and redirects	Routes traffic to the Customer's website through Cloudflare, which caches content and blocks attacks, when the Customer turns the feature on.	Cloudflare stops handling the traffic when the Customer turns the feature off. Cached copies expire according to the site's cache settings.

Service	What Hostup does with the data	When the service ends
Object storage (S3, beta)	Stores the Customer's files in three copies.	Deleted, including old versions, when the service ends.
Support and Hostup's assistant	Handles tickets, chats and attachments. In connection with the Customer's ticket or question, support and the assistant read data in the Customer's services to troubleshoot, for example error logs, email logs and DNS records. AI sorts tickets and writes replies and draft replies. Email to Hostup's addresses is received in Google Workspace, and email about tickets is sent through Amazon SES.	Tickets are kept for as long as the account exists and deleted when the account is closed.

Annex 2 – Sub-processors

Hostup engages the following sub-processors. Which of them process data in a given case depends on the service and the server. Registries, registrars and providers of payment and bookkeeping are not sub-processors (section 4.2); they are listed in the [Privacy Policy](#).

Sub-processor	Used for	Country	Transfer basis
Obehosting AB (Obenet)	Data centre in Älvsjö housing Hostup's own hardware, and network connectivity with an SLA.	Sweden	–
Hetzner Online GmbH	Servers for part of the web hosting and email, and for part of Hostup's internal systems.	EU	–
Oracle Svenska AB (Oracle Cloud)	Servers for part of the web hosting and email, and Hostup's primary DNS server, from which Cloudflare fetches the zones.	Sweden	–
Cloudflare, Inc.	DNS, CDN, website protection, redirects and email forwarding. Storage of attachments in support tickets, within the EU.	United States (global network)	EU–US Data Privacy Framework, EU standard contractual clauses
MailChannels Corporation	Delivery of outgoing email from web hosting, and backup for the email relay for VPS.	Canada	EU adequacy decision for Canada
Together Computer, Inc. (Together AI)	AI in support, in the assistant and in spam checks for the VPS relay. Storage of prompts and responses is turned off, and they are not used for training.	United States	EU standard contractual clauses
Pinecone Systems, Inc.	Search in Hostup's knowledge base with the text of the Customer's question, in support and the assistant.	United States	EU standard contractual clauses
Anthropic, PBC	When Together AI is not available, we use Anthropic's models for support and the assistant instead. This is rare. Data is not used for training.	United States	EU standard contractual clauses
Google LLC (Google Workspace and Gemini)	Email to Hostup's addresses at hostup.se, for example info@hostup.se, is received in Google Workspace. When Together AI is not available we may also use Google's models for support and the assistant; this is rare, and the data is not used for training.	United States	EU–US Data Privacy Framework
Consultants under assignment agreements	Technical support and operations for all services, including VPS, when Hostup needs extra capacity or expertise. Limited access, only to what the assignment requires, under an assignment agreement with confidentiality and on Hostup's instructions.	Sweden	–

Sub-processor	Used for	Country	Transfer basis
Support partners under service agreements	Additional technical support for web hosting and domains when a case cannot be solved by Hostup's own team. Limited access, only to the case at hand, under a service agreement and on Hostup's instructions. Does not apply to VPS.	Outside the EU/EEA	EU standard contractual clauses
Amazon Web Services EMEA SARL (Amazon SES)	Delivery of email from Hostup's systems: ticket replies and notifications, and account emails.	Sweden (AWS region Stockholm)	EU standard contractual clauses (AWS data processing addendum)

Annex 3 – Security measures

Organisation

- Employees and consultants have signed confidentiality agreements.
- Access is granted per person and only to what the work requires. It is removed when the employment or assignment ends.
- Administrative access uses personal accounts and SSH keys, from approved IP addresses or through Cloudflare Zero Trust with a one-time code.
- When staff log in to a customer's client area, a stated reason is required and the login is logged.
- Hostup logs in to the Customer's VPS only with the Customer's approval or in the exceptional cases set out in sections 5.4 and 5.5.
- A technician is on call around the clock. Incidents that affect many customers are published at status.hostup.se.

Data centre in Älvsjö

- The building is operated by Obenet. Hostup rents the racks and owns all hardware and network equipment in them.
- Hostup's office is in the same building, and Hostup staff are on site almost every day.
- Intrusion protection rated Larmklass 3 and Skyddsklass 3 (Swedish standards), access control around the clock.
- Redundant power (A and B feeds), UPS and backup generator.
- Disks taken out of service are wiped, or destroyed if they cannot be wiped, before they leave Hostup.

Network

- Own network with its own AS number (AS214640) and several independent connections.
- Protection against denial-of-service attacks in several layers: Hostup's own detection and filtering in its own network, then filtering at Obenet, and in a very large attack the traffic can be routed through Cloudflare.
- A per-VPS firewall controlled by the Customer, private networks between the Customer's servers, and protection against spoofed IP addresses between servers.

VPS

- Each server runs isolated in its own virtual machine (KVM).
- Storage is NVMe in Ceph, set up to keep every block on three separate servers.
- Backups are written to Hostup's own backup server in Älvsjö, on different hardware from the storage the servers run on. The Customer controls schedule and deletion in the client area.

- Hostup does not encrypt the server's disks or backups at rest in the standard service. The Customer can encrypt the server itself, for example with LUKS when installing from its own ISO image, and is then responsible for settings and keys. What the Customer encrypts on the disk stays encrypted in the backups; parts it has not encrypted, such as a boot partition, are stored as they are.
- The Customer is responsible for the operating system, updates and firewall inside the server.

Web hosting and email

- Each account is isolated from other accounts on the server (CloudLinux CageFS) and has its own resource limits.
- Automatic malware scanning and a web application firewall on the server (Imunify360).
- Server software is updated regularly, security updates first.
- Daily backups, stored in Sweden.
- TLS certificates are issued automatically for the Customer's domains. IMAP, POP3 and SMTP can be used with TLS, and webmail is served over HTTPS.

Object storage (S3, beta)

- Objects are stored in Ceph in three copies and accessed over HTTPS with the Customer's access keys.
- Object storage has no separate backup.

Email relay for VPS

- The relay accepts email only from Hostup's VPS and checks it automatically for spam and abuse.

DNS and domains

- DNS is answered by Cloudflare's network from zones on Hostup's primary DNS server. DNSSEC can be turned on.
- Registry lock for .se and .nu domains.

All services

- The rules on access, confidentiality, incidents and deletion in this agreement apply to all Services, including object storage, the email relay and support.

The Customer's own security tools in the client area

- Login with BankID, with the option to allow BankID only.
- Two-factor authentication: passkeys, security keys (YubiKey), authenticator apps, one-time codes by email, and backup codes.
- Team members and delegated access with per-service permissions, and API keys that can be revoked.
- An event log of logins and changes, and an overview of active sessions.

AI in support

- Together AI processes tickets and chats with storage of prompts and responses turned off, and without using them for training.
- When Together AI is not available, Anthropic or Google takes over, which is rare. Neither uses the data for training; they may keep it for a limited time to detect misuse.
- The assistant reads data in the Customer's services only in connection with the Customer's ticket or question.