HOSTUP

Privacy Policy

Hostup AB · Version 2.0 · 26 September 2026

This policy describes how Hostup AB processes personal data about you as a customer, a contact person at a customer, or a visitor to hostup.se and the client area (cloud.hostup.se). It replaces the version of 1 March 2026.

Data that you store in your own services, for example on your server, in your website or in your email, we process on your behalf as a processor. That data is covered by our Data Processing Agreement, not by this policy.

---

1. Controller

1.1 Hostup AB, reg. no. 559290-1325, Mässvägen 4, 125 30 Älvsjö, Sweden, is the controller. You reach us at info@hostup.se or through the support form.

2. What we process, why and for how long

2.1 **Account and contract.** Name, email address, postal address, phone number, personal identity or organisation number, company name, language and currency, your settings, and the people you give access to the account. We need this to enter into and perform the contract with you (Article 6(1)(b) GDPR), for example to register domains and send invoices. If you are a contact person or user at a company that is our customer, the basis is instead our legitimate interest in managing the customer relationship (Article 6(1)(f)). We ask for a personal identity number only where needed: for BankID, debt collection against sole traders, and domains whose registry requires it. The data is kept for as long as you have an account with us. When the account is closed, we delete or anonymise what is no longer needed. We keep only what is needed for an unpaid invoice, a specific legal claim or a legal obligation such as section 2.2, and only for that purpose. After a closure at the customer's own request we keep a limited record for twelve months (Terms of Service section 2.6), and after a closure for intentional abuse for as long as it is needed to prevent the abuse from recurring, which we review regularly.

2.2 **Invoicing and bookkeeping.** Invoices, payments, payment references and credit notes. The legal basis is the contract and our obligation under the Swedish Bookkeeping Act (Article 6(1)(c)). Bookkeeping records are kept for seven years after the end of the financial year.

2.3 **Identity checks.** When you log in or sign with BankID, we receive your personal identity number and name from BankID. When a company is to be represented, we retrieve data on authorised signatories from the Swedish Companies Registration Office (Bolagsverket) through TIC. For some orders we may ask for an identity check through Stripe Identity, where you photograph your ID document and take a selfie that is compared with the document. The check is based on our legitimate interest in preventing fraud and account takeovers (Article 6(1)(f)). The comparison with the selfie is processing of biometric data and takes place only with your explicit consent in that step (Article 9(2)(a)); if you do not want that, contact us and we will find another way to verify you, for example BankID. The result of a check is kept for as long as the account exists. The images of the document and the selfie are stored by Stripe on our behalf, not in our systems, for as long as they may be needed to investigate fraud against us; we receive only the result of the check.

2.4 **Support and the assistant.** What you write in tickets, chats and to our AI assistant, attachments you upload, and the data in your services that we read to troubleshoot what you asked about. The basis is the contract, or for contact persons at companies our legitimate interest (Article 6(1)(f)). Tickets and chats are kept while the account exists and deleted when it is closed.

2.5 **Security and abuse.** IP address, browser, time and what was done, for every visit, login and API call. In the client area you can see your own event log. We use this to protect accounts and the platform, investigate abuse and fraud, and meet legal requirements (Article 6(1)(f) and 6(1)(c)). The event log is kept for 90 days. Technical logs containing IP addresses, such as web server and firewall logs, are kept for at most 90 days.

2.6 **Risk assessment of orders.** New orders and payments are risk-assessed automatically, based on among other things account data, country, payment method and order history, partly with the help of AI. A flag never stops an order for good: the order is paused for manual review by our staff, who may ask you for an identity check. The basis is our legitimate interest in preventing fraud (Article 6(1)(f)).

2.7 **Messages about your services.** We send email about your services, for example about renewals, invoices and incidents, to perform the contract. We do not send marketing.

2.8 **Ad measurement.** If you come to us through an ad and have accepted marketing cookies, we store the ad's click ID, where you came from and what you ordered, and report the order to the ad platform (Google or Reddit) together with a hashed version of your email address, which the platform uses to match the order to the ad click. The basis is your consent (Article 6(1)(a)), which you withdraw under Cookie settings. We keep the data for 90 days; the ad platform keeps what it receives under its own terms.

2.9 **Affiliates.** If you order after clicking a link from one of our affiliates and have accepted marketing cookies, Addrevenue receives the order's ID, amount and currency so that the affiliate is paid. The basis is your consent. We keep the link between the order and the affiliate until the commission has been settled.

3. Cookies

3.1 The client area and hostup.se set the following cookies.

Cookie	What it does	Lifetime	Category
secure_session	Keeps you logged in	12 hours	Necessary
mfa_trust	Remembers a device you approved for two-factor login	30 days	Necessary
bankid-login-hint	Remembers that you usually log in with BankID	1 year	Necessary
hu_search_pass	Lets your domain search through after the bot check	45 minutes	Necessary
cc_cookie	Stores your choices in the cookie banner	6 months	Necessary
preferred-language, preferred_currency_id, price_display_mode	Your language, currency and whether prices show with or without VAT	90 days to 1 year	Necessary
Cloudflare (__cf_bm, cf_clearance)	Protects the site against bots and attacks	30 minutes (__cf_bm) to 1 year (cf_clearance)	Necessary
hu_attr	The ad's click ID and where you came from	90 days	Marketing
Addrevenue (adr_, _ar)	Links an order to an affiliate link	30 days	Marketing

3.2 Necessary cookies are required for the service to work and need no consent. Marketing cookies are set only if you have accepted them. Visitors in the EU/EEA choose in the cookie banner; you can change your choices at any time under Cookie settings at the bottom of hostup.se and in the client area, or delete cookies in your browser.

3.3 We use no web analytics and no statistics cookies, and we do not record visits. Errors in the client area may be reported to our own error-tracking system (Sentry, which we run ourselves), with the technical details needed

to fix them.

4. Who we share data with

4.1 We never sell personal data. We share it with the following recipients, to the extent the service you use requires it.

4.2 **Payment.** Stripe Payments Europe (Ireland) for cards, Klarna, SEPA and Alipay, and Swish through your bank. Card details are stored by Stripe, never by us; we receive payment references, the card's last four digits and expiry date, and what else is needed to handle the payment. To match incoming payments to invoices, we retrieve transactions from our bank account through Enable Banking (Finland).

4.3 **Invoicing and bookkeeping.** Fortnox (Sweden) for bookkeeping, Qvalia (Sweden) for e-invoices via Peppol to organisations, and Kravia (Sweden) for reminders and debt collection when a company does not pay an invoice; private individuals are not sent to debt collection. Kravia receives the data needed to collect the debt, for sole traders including the personal identity number.

4.4 **Identity.** BankID through twoday (Sweden), company data from Bolagsverket through TIC (Sweden), and identity checks through Stripe Identity.

4.5 **Domains.** When you register a .se or .nu domain, the holder's details are passed to Internetstiftelsen. For all other top-level domains they are passed to Openprovider (Netherlands) and to the top-level domain's registry, for example Traficom for .fi. Registries and registrars are responsible for their own processing, under their own terms. As a provider of domain registration we are required by law to keep a register of the domain names we have registered, with the holder's and contacts' details, and to disclose data when the law requires it (Article 6(1)(c)). Which country the data ends up in follows from the top-level domain you choose; for .us the registry is in the United States. Some registries require the holder's details to be shown publicly in whois.

4.6 **Operating our systems.** Obehosting (Obenet) runs the data centre in Älvsjö where our own hardware stands. Hetzner (EU) and Oracle Cloud (Sweden) provide servers for parts of our systems and the web hosting; Oracle Cloud also runs our primary DNS server, from which Cloudflare fetches the zones. Cloudflare (United States) protects and delivers traffic to hostup.se and the client area, runs our DNS service, checks that logins and domain searches are not from bots (Turnstile), and stores attachments in support tickets on servers within the EU. Amazon Web Services (Stockholm region) sends our email, for example invoices, ticket replies and one-time codes. Google Workspace (Google) receives email sent to our addresses at hostup.se. Vonage (United States) sends text messages about overdue invoices, new replies in your tickets and, to Swedish numbers, domains about to expire, and a single message when we cannot reach you by email; Vonage also places calls when you have asked for one. MailChannels (Canada) delivers outgoing email from the web hosting and is the backup for the email relay for VPS.

4.7 **AI.** Our AI assistant, sorting and translation of tickets, draft replies and risk assessments use language models. Where it is economically feasible, we run the models on our own servers. Otherwise Together AI (United States) is our main AI partner; storage of questions and answers is turned off for our organisation at Together, and they are not used to train models. When Together is not available, we use Anthropic or Google (United States) instead. This is rare. They do not use the data to train models either, but may keep it for a limited time to detect misuse. The provider receives only what the question needs, for example the text of your ticket. To find the right answer in our knowledge base, your question is sent to Pinecone (United States) for search.

4.8 **Staff and partners.** Our own staff, and the consultants and support partners who work in our systems on our behalf, see the data their work requires. All have signed confidentiality agreements. Our staff receive alerts about tickets in Telegram. An alert carries the ticket number and never the customer's name. When our AI has prepared a reply, the alert also shows the draft so that staff can review it before it is sent. When a problem lies with a vendor, for example cPanel, we may need to share technical details of that specific problem with the vendor's support, without personal data where possible.

4.9 **Marketing.** Addrevenue (Sweden) for affiliates, and Google and Reddit (United States) for ad measurement, both only with your consent under sections 2.8 and 2.9.

4.10 **Authorities.** When the law requires it, for example a court order or a request from the police that we are obliged to follow. We never disclose more than the order covers.

5. Transfers outside the EU/EEA

5.1 Our own systems, the client area, invoicing and all backups are in Sweden and the EU. Some recipients above are outside the EU/EEA:

- **United States:** Cloudflare, Google and Stripe are certified under the EU–US Data Privacy Framework, which the European Commission has recognised as providing an adequate level of protection (Decision 2023/1795). For Together AI, Anthropic, Pinecone, Vonage, Amazon Web Services and Reddit, the European Commission's standard contractual clauses apply.
- **Canada:** MailChannels is covered by the European Commission's adequacy decision for Canada.
- **Domain registries outside the EU/EEA**, for example for .us: we pass the holder's details to Openprovider within the EU, which as registrar passes them on to the registry under its own terms, and only what the registry requires for the domain you have ordered.

5.2 Some of our other suppliers and partners may also be outside the EU/EEA. The data is then protected by the European Commission's standard contractual clauses or another safeguard the GDPR allows.

5.3 Write to info@hostup.se if you want more information about the safeguards for a transfer or a copy of them, with confidential parts redacted.

6. Your rights

6.1 You have the right to access the data we hold about you, to have it corrected or erased, to request that processing be restricted, to receive your data in a machine-readable format, and to object to processing based on legitimate interest. Where we rely on your consent, you can withdraw it at any time; consent to marketing cookies you withdraw under Cookie settings.

6.2 Most of this you do yourself in the client area: change contact details, view your event log, download your invoices and close the account. For anything else, contact us through the support form or info@hostup.se. We reply within one month. If the request is complex, or we have received many requests, the time may be extended by up to two further months; we tell you within the first month, with the reason. Some rights have limits, for example we cannot erase data that the Bookkeeping Act requires us to keep, and we tell you if a limit applies.

6.3 If you think we process your data wrongly, you can complain to the Swedish Authority for Privacy Protection, imy.se.

7. Security

7.1 The client area offers BankID login, passkeys, security keys and two-factor login with an authenticator app or one-time codes, and an event log where you see every login and change. Connections to hostup.se and the client area use HTTPS. Access to personal data is granted per person and only as the work requires. The security measures for your services are described in Annex 3 of the Data Processing Agreement.

8. Children

8.1 Our services are for businesses and for private individuals aged 18 or over.

9. Changes

9.1 We may change this policy. The current version, with its date, is always at hostup.se/en/legal; for major changes we inform you in the client area.