

Personuppgiftsbiträdesavtal

Hostup AB · Version 2.0 · 26 september 2026

Denna version ersätter [version 1.0](#), som bara omfattade VPS. Den aktuella versionen finns alltid på <https://hostup.se/legal/dpa-sv.pdf>.

1. Parter

Personuppgiftsbiträde: Hostup AB, org.nr 559290-1325, Mässvägen 4, 125 30 Älvsjö ("Hostup"). Kontakt i dataskyddsfrågor: info@hostup.se eller supportformuläret på <https://cloud.hostup.se/contact>.

Personuppgiftsansvarig: den kund som använder Hostups tjänster och behandlar personuppgifter i dem ("Kunden"). Är Kunden själv personuppgiftsbiträde åt någon annan är Hostup Kundens underbiträde, och Kunden ansvarar för att ha den personuppgiftsansvariges tillstånd till det.

2. Bakgrund och syfte

2.1 Kunden använder Hostups tjänster för att lagra, skicka och på annat sätt behandla data. När datan innehåller personuppgifter behandlar Hostup dem för Kundens räkning. Detta avtal innehåller de villkor som artikel 28 i dataskyddsförordningen (EU) 2016/679 ("GDPR") kräver för den behandlingen.

2.2 Detta avtal är en del av Hostups [användarvillkor](#) och gäller för alla Hostups tjänster. I frågor om personuppgifter har detta avtal företräde framför användarvillkoren.

3. Definitioner

Begrepp som *personuppgifter*, *behandling*, *personuppgiftsansvarig*, *personuppgiftsbiträde*, *registrerad*, *personuppgiftsincident* och *tillsynsmyndighet* har samma betydelse som i GDPR. Dessutom gäller:

- **Tjänsterna:** de tjänster Kunden beställer av Hostup, bland annat VPS, webbhotell och återförsäljarwebbhotell, e-post, DNS, CDN och vidarebefordringar, objektlagring (S3), säkerhetskopior samt support och Hostups assistent.
- **Kundens personuppgifter:** personuppgifter som Kunden, eller den som använder Kundens tjänster, lagrar eller behandlar i Tjänsterna. Exempel: innehåll på servrar och webbplatser, databaser, e-post, filer i objektlagring, säkerhetskopior och loggar med besökarens IP-adresser.
- **Underbiträde:** en annan leverantör som Hostup anlitar och som behandlar Kundens personuppgifter för Hostups räkning.

4. Omfattning och roller

4.1 Hostup är personuppgiftsbiträde för Kundens personuppgifter i alla Tjänster. Vad som behandlas, varför, hur länge och om vilka registrerade beskrivs per tjänst i **bilaga 1**.

4.2 Hostup är självständigt personuppgiftsansvarig, och detta avtal gäller därför inte, för:

- a) Kundens egna konto-, kontakt- och faktureringsuppgifter, inklusive uppgifter om de personer Kunden ger tillgång till kontot;
- b) uppgifter om domäninnehavare och kontakter som lämnas till register och registrarer när domännamn registreras och administreras. Register och registrarer är personuppgiftsansvariga för de uppgifterna enligt sina egna villkor. Var uppgifterna hamnar följer av den toppdomän Kunden väljer; registret för .us finns till exempel i USA och registret för .hu i Ungern;

- c) loggar och uppgifter som Hostup behandlar för att skydda plattformen, förhindra bedrägerier, spam och missbruk och uppfylla rättsliga skyldigheter som bokföring.

Den behandlingen beskrivs i Hostups [integritetspolicy](#).

5. Kundens instruktioner

5.1 Hostup behandlar Kundens personuppgifter endast enligt Kundens dokumenterade instruktioner.

Instruktionerna är:

- a) detta avtal och dess bilagor;
- b) Kundens egna val när Kunden använder Tjänsterna: inställningar i Kundzonen, API-anrop, beställningar och uppsägningar;
- c) det Kunden ber om i ett supportärende.

En instruktion som går utöver Tjänsterna, eller som skulle kräva att Hostup ändrar hur Tjänsterna fungerar, kan avböjas.

5.2 Hostup får behandla Kundens personuppgifter på annat sätt endast när unionsrätten eller svensk rätt kräver det. Hostup informerar då Kunden före behandlingen, om inte lagen förbjuder det.

5.3 Hostup informerar Kunden omedelbart om en instruktion enligt Hostups uppfattning strider mot GDPR eller annan dataskyddslagstiftning. Hostup är inte skyldigt att granska om Kundens instruktioner eller innehåll är förenliga med lag.

5.4 Hostup tar inte del av innehållet i Kundens tjänster, utom när:

- a) Kunden ber om eller godkänner det, till exempel för felsökning i ett supportärende;
- b) det behövs för att driva och skydda Tjänsterna, till exempel automatisk filtrering av spam och skadlig kod eller utredning av missbruk som anmälts till Hostup;
- c) lagen kräver det.

5.5 Hostup loggar inte in på en VPS utan Kundens godkännande, utom när punkt 5.4 b eller c är tillämplig. Hostup sätter serverns första root-lösenord när servern skapas och sparar det så att Kunden kan se det i Kundzonen. Kunden bör byta det; ett lösenord som Kunden själv sätter i servern ser Hostup inte.

6. Kundens ansvar

6.1 Kunden ansvarar för att det finns en rättslig grund för behandlingen, för att informera de registrerade och för att Kundens instruktioner följer lagen.

6.2 Kunden ansvarar för att bedöma om säkerhetsåtgärderna i bilaga 3 är tillräckliga för de personuppgifter Kunden behandlar, särskilt för särskilda kategorier av personuppgifter enligt artikel 9 i GDPR, och för att vidta egna åtgärder, till exempel kryptering, där de inte är det.

6.3 På VPS administrerar Kunden operativsystem, programvara, uppdateringar, åtkomst och kryptering. På webshotell ansvarar Kunden för sin egen programvara, till exempel WordPress och tillägg.

6.4 Kunden ansvarar för att ha egna kopior av data som är viktig för Kunden (användarvillkoren punkt 1.2 och 19.5).

6.5 Kunden ansvarar för de personer Kunden ger tillgång till Tjänsterna och för vad de gör med Kundens personuppgifter.

7. Sekretess

7.1 Alla som arbetar för Hostup och kan komma åt Kundens personuppgifter har skrivit under ett sekretessavtal. Det gäller anställda samt konsulter och supportpersonal som arbetar i Hostups system enligt Hostups instruktioner. Sekretessen gäller även efter att anställningen eller uppdraget har upphört.

7.2 Åtkomst till system med Kundens personuppgifter ges per person och bara i den omfattning arbetet kräver.

7.3 Hostup lämnar inte ut Kundens personuppgifter till tredje part utom enligt punkt 5 eller 9. Begär en myndighet ut Kundens personuppgifter hänvisar Hostup myndigheten till Kunden om det är möjligt och informerar Kunden om begäran, om inte lagen förbjuder det.

8. Säkerhet

8.1 Hostup vidtar de tekniska och organisatoriska åtgärder som artikel 32 i GDPR kräver. Åtgärderna beskrivs per tjänst i **bilaga 3**.

8.2 Hostup får ändra åtgärderna i takt med den tekniska utvecklingen, förutsatt att skyddsnivån inte sänks.

9. Underbiträden

9.1 Kunden ger Hostup ett allmänt förhandstillstånd att anlita underbiträden. Underbiträdena anges i **bilaga 2** till den aktuella versionen av detta avtal, som finns på <https://hostup.se/legal/dpa-sv.pdf> och i Kundzonen under Konto → Avtal & dokument. Leverantörer som inte behandlar Kundens personuppgifter är inte underbiträden och anges inte, till exempel leverantörer av programvarulicenser, hårdvara och nätanslutning. Ett externt företag vars personal har åtkomst till Kundens personuppgifter är ett underbiträde, även när det arbetar i Hostups system. Bilaga 2 har en icke offentlig del: Kunden får på begäran de fullständiga uppgifterna om de underbiträden som anges där, och får lämna dem vidare till sina rådgivare, revisorer och myndigheter.

9.2 Hostup ingår ett skriftligt avtal med varje underbiträde som ger Kundens personuppgifter minst samma skydd som detta avtal. Hostup ansvarar mot Kunden för underbitrådets behandling som för sin egen.

9.3 **Ändringar.** Hostup håller bilaga 2 aktuell. Ett nytt eller utbytt underbiträde publiceras i en ny version av detta avtal minst 14 dagar innan ändringen börjar gälla, med uppgift om det datumet, och Hostup informerar Kunden om ändringen, till exempel via e-post eller i Kundzonen. Måste ett underbiträde bytas ut utan dröjsmål av säkerhets- eller driftskäl använder Hostup ett underbiträde som redan anges i bilaga 2 för det ändamålet, och informerar Kunden så snart ändringen är gjord.

9.4 **Invändning.** Kunden kan invända mot en ändring innan den börjar gälla, av skäl som rör dataskydd, genom att kontakta supporten. Hostup söker då en lösning tillsammans med Kunden. Hittas ingen kan Kunden säga upp de berörda Tjänsterna från den dag ändringen börjar gälla, så att det nya underbiträdet inte används för Kundens uppgifter. Det är Kundens enda åtgärd enligt detta avtal vid en ändring enligt punkt 9.3.

10. Överföring till tredjeland

10.1 VPS lagras i Sverige, liksom alla säkerhetskopior som Hostup tar, i alla Tjänster. Webbplatser och e-postkonton lagras inom EU. Det gäller var uppgifterna lagras. Viss behandling sker på andra platser genom underbiträdena i bilaga 2, till exempel i Cloudflares nätverk när Kunden använder CDN och hos MailChannels när e-post levereras. Var behandlingen sker kan variera med tjänst, server och belastning.

10.2 Hostup överför Kundens personuppgifter till ett land utanför EU/EES endast i de fall som anges i bilaga 2, och endast när överföringen är tillåten enligt kapitel V i GDPR. Grunden kan vara ett beslut om adekvat skyddsnivå, till exempel EU–US Data Privacy Framework för certifierade företag, eller EU-kommissionens standardavtalsklausuler.

10.3 När Kunden själv skickar uppgifter till mottagare utanför EU/EES, till exempel e-post till en mottagare i ett annat land, eller publicerar uppgifter på sin webbplats, väljer Kunden mottagaren och ansvarar för det utlämnandet. Punkt 10.2 gäller de underbiträden som Hostup väljer.

11. Hjälp med de registrerades rättigheter

11.1 Kunden kan själv ta del av, rätta och radera uppgifter i Tjänsterna, till exempel via Kundzonen, cPanel, SSH/SFTP och API:et.

11.2 När Kunden inte kan göra det själv hjälper Hostup Kunden att besvara en begäran från en registrerad, så långt det är möjligt med hänsyn till behandlingens art.

11.3 Kontaktar en registrerad Hostup direkt med en begäran som gäller Kundens personuppgifter hänvisar Hostup den registrerade till Kunden och informerar Kunden. Hostup besvarar inte själv begäran.

12. Hjälp med säkerhet, konsekvensbedömningar och förhandssamråd

12.1 Hostup hjälper Kunden att fullgöra sina skyldigheter enligt artiklarna 32–36 i GDPR, med hänsyn till behandlingens art och den information Hostup har tillgång till. Det omfattar säkerhet, personuppgiftsincidenter, konsekvensbedömningar och förhandssamråd med tillsynsmyndigheten.

12.2 Skälig hjälp enligt punkt 11 och 12, och informationen enligt punkt 14.1 och 14.2, är kostnadsfri. Arbete som går utöver vad behandlingens art och den information Hostup har tillgång till rimligen kräver, till exempel en konsekvensbedömning som görs åt Kunden eller utredningar som Kunden själv kan göra i Tjänsterna, debiteras per timme enligt ett i förväg överenskommet pris.

13. Personuppgiftsincidenter

13.1 Hostup underrättar Kunden utan onödigt dröjsmål efter att ha fått kännedom om en personuppgiftsincident som berör Kundens personuppgifter. Hostup väntar inte tills utredningen är klar.

13.2 Underrättelsen skickas till kontots e-postadress och läggs som ett ärende i Kundzonen. Den innehåller den information som artikel 33.3 i GDPR kräver, så långt den är känd: vad som har hänt, kategorier av och ungefärligt antal registrerade och poster som berörs, sannolika konsekvenser, de åtgärder Hostup har vidtagit eller föreslår och en kontaktperson. Information som inte finns vid den första underrättelsen lämnas så snart den finns. Kunden håller kontots e-postadress aktuell. En underrättelse innebär inte att Hostup medger fel eller ansvar.

13.3 Hostup vidtar utan dröjsmål skäliga åtgärder för att begränsa incidenten och dess följder och dokumenterar incidenten.

13.4 Kunden anmäler som personuppgiftsansvarig incidenten till tillsynsmyndigheten och informerar de registrerade när det krävs. Är Kunden själv personuppgiftsbiträde skickar Kunden underrättelsen vidare till sin personuppgiftsansvarige.

14. Information och granskning

14.1 Hostup tillhandahåller den information som behövs för att visa att artikel 28 i GDPR följs: detta avtal med bilagor, incidenthistoriken på status.hostup.se och skriftliga svar på rimliga frågor som dokumenten inte redan besvarar. Kunds specifika frågeformulär, blanketter och granskningsmallar behöver inte fyllas i; Hostup besvarar dem med hänvisning till detta avtal och kompletterar skriftligt det som avtalet inte redan besvarar. För underbiträden, inklusive den som driver datacentret, lämnar Hostup den information Hostup får från dem, till exempel certifieringar och granskningsrapporter.

14.2 En granskning sker i första hand som en dokumentgranskning: Hostup besvarar skriftliga frågor från Kunden eller dess granskare och lämnar, under sekretess, den dokumentation, de utdrag och de rapporter som gäller Kundens behandling. Räcker det inte och en ytterligare granskning, även en inspektion, behövs enligt artikel 28.3 h i GDPR, möjliggör Hostup den och bidrar till den.

14.3 Tjänsterna körs på delad infrastruktur, och Hostups hårdvara står i ett datacenter som drivs av någon annan. En granskning ger därför aldrig åtkomst till andra kunders system eller uppgifter, aldrig egen åtkomst till produktionssystem och aldrig rätt att öppna rack eller hantera utrustning. En inspektion ordnas och följs av Hostup. Dessutom gäller följande:

- a) Kunden meddelar granskningen minst 30 dagar i förväg, om inte lag, en tillsynsmyndighet eller konkreta tecken på bristande efterlevnad kräver en kortare tid;

- b) granskningen sker under kontorstid och begränsas till den fråga den gäller. Den sker högst en gång per tolv månadersperiod, med samma undantag som i a;
- c) den utförs av Kunden eller av en oberoende granskare med tystnadsplikt som inte konkurrerar med Hostup;
- d) Kunden står för kostnaderna för granskningen, inklusive skälig ersättning för den arbetstid Hostup lägger på den utöver att lämna informationen enligt punkt 14.1 och 14.2. Villkor och kostnader får inte göra rätten till granskning verkningslös;
- e) tillsynsmyndigheters befogenheter påverkas inte.

14.4 De åtgärder Hostup vidtar beskrivs i bilaga 3, och punkt 14.1 och 14.2 är hur Hostup visar att de finns på plats.

15. När Tjänsterna upphör

15.1 Innan en tjänst upphör kan Kunden själv hämta ut sina uppgifter, till exempel genom att kopiera uppgifterna från en VPS via SSH eller återställa en säkerhetskopia till en ny VPS, ta en fullständig säkerhetskopia av ett webbhotellskonto, hämta e-post via IMAP, ladda ner filer från objektlagringen och exportera DNS-zoner från Kundzonen. På så sätt väljer Kunden återlämnandet av sina uppgifter. Kan Kunden inte hämta ut uppgifterna med dessa funktioner hjälper Hostup till på begäran innan tjänsten upphör (punkt 12.2).

15.2 När en tjänst upphör, på Kundens begäran eller enligt användarvillkoren (även vid utebliven betalning), raderar Hostup Kundens personuppgifter i den tjänsten. Tidsgränserna per tjänst anges i bilaga 1. Kopior i Hostups säkerhetskopior raderas när deras lagringstid löper ut. Uppgifter som Hostup enligt unionsrätten eller svensk lag måste spara sparas bara för det ändamålet.

15.3 Hostup bekräftar raderingen skriftligen om Kunden ber om det.

16. Ansvar

16.1 Mellan parterna gäller ansvarsbegränsningen i användarvillkoren punkt 1.7.

16.2 Detta avtal begränsar inte en registrerads rätt till ersättning enligt artikel 82 i GDPR. Varje part står för de administrativa sanktionsavgifter som en tillsynsmyndighet beslutar om för den parten.

16.3 Skadeslösheten i användarvillkoren punkt 9.1 omfattar även krav och kostnader som beror på att Kunden bryter mot detta avtal eller mot sina skyldigheter som personuppgiftsansvarig, till exempel genom instruktioner som strider mot lag, med de förutsättningar och begränsningar som anges i den punkten.

17. Avtalstid och ändringar

17.1 Detta avtal gäller så länge Hostup behandlar Kundens personuppgifter.

17.2 Hostup får ändra detta avtal. En ändring publiceras som en ny version av avtalet minst 30 dagar innan den börjar gälla, och Hostup informerar Kunden om en väsentlig ändring via e-post eller i Kundzonen. Byte av underbiträden följer punkt 9. En ändring som krävs enligt lag, eller som inte försämrar Kundens skydd, får börja gälla tidigare. En Kund som inte godtar en ändring kan säga upp de berörda Tjänsterna från den dag ändringen börjar gälla.

17.3 Varje version har ett versionsnummer och ett datum. Tidigare versioner finns kvar, till exempel version 2.0 på <https://hostup.se/legal/dpa-2.0-sv.pdf>, så att Kunden kan se vilken lydelse som gällde vid en viss tidpunkt.

18. Avtalets ingående

18.1 Detta avtal ingås elektroniskt, vilket är skriftlig form enligt artikel 28.9 i GDPR. Det gäller mellan Hostup och varje kund som använder Tjänsterna, från den tidpunkt Kunden godkänner användarvillkoren.

18.2 Avtalet finns som PDF i Kundzonen under Konto → Avtal & dokument, på svenska och engelska. Om versionerna skiljer sig åt gäller den svenska.

19. Tillämplig lag och tvister

19.1 Svensk lag gäller för detta avtal. Tvister avgörs enligt användarvillkoren punkt 6.

Bilaga 1 – Behandling per tjänst

Gemensamt för alla tjänster

- **Ändamål:** att tillhandahålla, driva, skydda och ge support för de Tjänster Kunden har beställt.
- **Registrerade och personuppgifter:** bestäms av Kunden. Oftast Kundens kunder, användare, anställda och besökare på webbplatser, med till exempel kontaktuppgifter, innehåll i e-post och filer, uppgifter i Kundens databaser, IP-adresser och loggar. Lagrar Kunden särskilda kategorier av personuppgifter gäller punkt 6.2.
- **Plats:** VPS och alla säkerhetskopior i Sverige. Webbplatser och e-postkonton inom EU, på Hostups egna servrar i Sverige eller hos underbiträdena i bilaga 2. I övrigt enligt punkt 10.
- **Tid:** så länge tjänsten finns, och därefter fram till radering enligt tabellen. Kvarvarande kopior används inte och raderas inom de tider som anges i tabellen, om inte lag kräver att de sparas. Ett byte enligt användarvillkoren punkt 21 följer tiderna där.

Tjänst	Vad Hostup gör med uppgifterna	När tjänsten upphör
VPS	Lagrar serverns diskar och kör servern. Tar ögonblicksbilder och säkerhetskopior enligt Kundens inställningar. För serverns nätverkstrafik.	Servern och dess ögonblicksbilder raderas direkt när tjänsten upphör, säkerhetskopiorna 7 dagar senare. Vid utebliven betalning avslutas tjänsten enligt användarvillkoren punkt 4.2.2.
Webbhotell, återförsäljarwebbhotell och e-post	Lagrar och kör webbplatser, databaser och e-postkonton. Sparar webbserverns loggar, som innehåller besökares IP-adresser. Tar dagliga säkerhetskopior och söker automatiskt efter skadlig kod. Utgående e-post levereras via Hostups egen relay eller via MailChannels.	Kontot raderas när det avslutas. Kopior i säkerhetskopior raderas inom en vecka.
E-postrelay för VPS (relay.hostup.se)	Tar emot och levererar utgående e-post från Kundens server. Kontrollerar den automatiskt mot spam och missbruk, delvis med AI.	E-post i kö och loggar raderas efter en månad.
DNS och vidarebefordring av e-post för domäner	Lagrar domänens DNS-poster på Hostups primära DNS-server; Cloudflare besvarar DNS-frågorna. Vidarebefordrar e-post enligt de regler Kunden lägger upp.	Zonen och reglerna raderas när domänen lämnar Hostup eller när Kunden tar bort dem.
CDN, brandvägg för webbplatser och vidarebefordringar	Leder trafiken till Kundens webbplats via Cloudflare, som cachar innehåll och blockerar attacker, när Kunden slår på funktionen.	Cloudflare slutar hantera trafiken när Kunden stänger av funktionen. Cachade kopior löper ut enligt webbplatsens cacheinställningar.
Objektlagring (S3, beta)	Lagrar Kundens filer i tre kopior.	Raderas, även äldre versioner, när tjänsten upphör.

Tjänst	Vad Hostup gör med uppgifterna	När tjänsten upphör
Support och Hostups assistent	Hanterar ärenden, chattar och bilagor. I samband med Kundens ärende eller fråga läser supporten och assistenten uppgifter i Kundens tjänster för att felsöka, till exempel felloggar, e-postloggar och DNS-poster. AI sorterar ärenden och skriver svar och utkast till svar. E-post till Hostups adresser tas emot i Google Workspace, och e-post om ärenden skickas via Amazon SES.	Ärenden sparas så länge kontot finns och raderas när kontot avslutas.

Bilaga 2 – Underbiträden

Hostup anlitar följande underbiträden. Vilka av dem som behandlar uppgifter i ett visst fall beror på tjänst och server. Register, registrarer och leverantörer av betalning och bokföring är inte underbiträden (punkt 4.2); de anges i [integritetspolicy](#)n.

Underbiträde	Används för	Land	Grund för överföring
Obehosting AB (Obenet)	Datacenter i Älvsjö där Hostups egen hårdvara står, och nätverksanslutning med SLA.	Sverige	–
Hetzner Online GmbH	Serverar för en del av webbhotellet och e-posten, och för en del av Hostups interna system.	EU	–
Oracle Svenska AB (Oracle Cloud)	Serverar för en del av webbhotellet och e-posten, och Hostups primära DNS-server, som Cloudflare hämtar zonerna från.	Sverige	–
Cloudflare, Inc.	DNS, CDN, webbplatssskydd, vidarebefordringar och vidarebefordring av e-post. Lagring av bilagor i supportärenden, inom EU.	USA (globalt nätverk)	EU–US Data Privacy Framework, EU:s standardavtalsklausuler
MailChannels Corporation	Leverans av utgående e-post från webbhotellet, och reserv för e-postrelayn för VPS.	Kanada	EU:s beslut om adekvat skyddsnivå för Kanada
Together Computer, Inc. (Together AI)	AI i supporten, i assistenten och i spamkontrollen för VPS-relayn. Lagring av frågor och svar är avstängd, och de används inte för träning.	USA	EU:s standardavtalsklausuler
Pinecone Systems, Inc.	Sökning i Hostups kunskapsbas med texten i Kundens fråga, i supporten och assistenten.	USA	EU:s standardavtalsklausuler
Anthropic, PBC	När Together AI inte är tillgängligt använder vi i stället Anthropics modeller för supporten och assistenten. Det händer sällan. Uppgifterna används inte för träning.	USA	EU:s standardavtalsklausuler
Google LLC (Google Workspace och Gemini)	E-post till Hostups adresser på hostup.se, till exempel info@hostup.se, tas emot i Google Workspace. När Together AI inte är tillgängligt kan vi också använda Googles modeller för supporten och assistenten; det händer sällan, och uppgifterna används inte för träning.	USA	EU–US Data Privacy Framework
Konsulter med uppdragsavtal	Teknisk support och drift för alla tjänster, även VPS, när Hostup behöver förstärkning eller särskild kompetens. Begränsad åtkomst, bara till det uppdraget kräver, enligt uppdragsavtal med sekretess och Hostups instruktioner.	Sverige	–

Underbiträde	Används för	Land	Grund för överföring
Supportpartner med serviceavtal	Utökad teknisk support för webbhotell och domäner när Hostups eget team inte kan lösa ett ärende. Begränsad åtkomst, bara till det aktuella ärendet, enligt serviceavtal och Hostups instruktioner. Gäller inte VPS.	Utanför EU/EES	EU:s standardavtalsklausuler
Amazon Web Services EMEA SARL (Amazon SES)	Leverans av e-post från Hostups system: ärendesvar och aviseringar samt e-post om kontot.	Sverige (AWS-region Stockholm)	EU:s standardavtalsklausuler (AWS personuppgiftsbiträdesavtal)

Bilaga 3 – Säkerhetsåtgärder

Organisation

- Anställda och konsulter har skrivit under sekretessavtal.
- Åtkomst ges per person och bara till det arbetet kräver. Den tas bort när anställningen eller uppdraget upphör.
- Administrativ åtkomst sker med personliga konton och SSH-nycklar, från godkända IP-adresser eller via Cloudflare Zero Trust med engångskod.
- När personal loggar in i en kunds Kundzon krävs ett angivet skäl, och inloggningen loggas.
- Hostup loggar in på Kundens VPS bara med Kundens godkännande eller i de undantagsfall som anges i punkt 5.4 och 5.5.
- En tekniker har jour dygnet runt. Incidenter som berör många kunder publiceras på status.hostup.se.

Datacentret i Älvsjö

- Byggnaden drivs av Obenet. Hostup hyr racken och äger all hårdvara och nätverksutrustning i dem.
- Hostups kontor ligger i samma byggnad, och Hostups personal är på plats nästan alla dagar.
- Inbrottsskydd enligt Larmklass 3 och Skyddsklass 3, passerkontroll dygnet runt.
- Redundant strömförsörjning (A- och B-matning), UPS och reservkraftverk.
- Diskar som tas ur bruk raderas, eller förstörs om de inte går att radera, innan de lämnar Hostup.

Nätverk

- Eget nät med eget AS-nummer (AS214640) och flera oberoende förbindelser.
- Skydd mot överbelastningsattacker i flera steg: Hostups egen upptäckt och filtrering i det egna nätet, därefter filtrering hos Obenet, och vid en mycket stor attack kan trafiken ledas via Cloudflare.
- Brandvägg per VPS som Kunden styr, privata nät mellan Kundens servrar och skydd mot förfälskade IP-adresser mellan servrar.

VPS

- Varje server körs isolerad i en egen virtuell maskin (KVM).
- Lagringen är NVMe i Ceph, som är inställt på att hålla varje block på tre olika servrar.
- Säkerhetskopior skrivs till Hostups egen backupserver i Älvsjö, på annan hårdvara än lagringen servrarna körs på. Kunden styr schema och radering i Kundzonen.
- Hostup krypterar inte serverns diskar eller säkerhetskopior i vila i standardtjänsten. Kunden kan kryptera servern själv, till exempel med LUKS vid installation från en egen ISO-avbild, och ansvarar då för inställningar och nycklar. Det Kunden krypterar på disken förblir krypterat i säkerhetskopiorna; delar som inte är krypterade, till exempel en startpartition, lagras som de är.
- Kunden ansvarar för operativsystem, uppdateringar och brandvägg inne i servern.

Webbhotell och e-post

- Varje konto är isolerat från andra konton på servern (CloudLinux CageFS) och har egna resursgränser.
- Automatisk sökning efter skadlig kod och brandvägg för webbapplikationer på servern (Imunify360).
- Serverprogramvaran uppdateras regelbundet, säkerhetsuppdateringar först.
- Dagliga säkerhetskopior, lagrade i Sverige.
- TLS-certifikat utfärdas automatiskt för Kundens domäner. IMAP, POP3 och SMTP kan användas med TLS, och webbmejlerna levereras över HTTPS.

Objektlagring (S3, beta)

- Objekt lagras i Ceph i tre kopior och nås via HTTPS med Kundens åtkomstnycklar.
- Objektlagringen har ingen separat säkerhetskopia.

E-postrelay för VPS

- Relayn tar bara emot e-post från Hostups VPS och kontrollerar den automatiskt mot spam och missbruk.

DNS och domäner

- DNS besvaras av Cloudflares nätverk utifrån zonerna på Hostups primära DNS-server. DNSSEC kan slås på.
- Registry lock för .se- och .nu-domäner.

Alla tjänster

- Avtalets regler om åtkomst, sekretess, incidenter och radering gäller för alla Tjänster, även objektlagring, e-postrelayn och support.

Kundens egna säkerhetsverktyg i Kundzonen

- Inloggning med BankID, med möjlighet att bara tillåta BankID.
- Tvåfaktorsinloggning: passkeys, säkerhetsnycklar (YubiKey), autentiseringsappar, engångskoder via e-post och reservkoder.
- Teammedlemmar och delegerad åtkomst med behörigheter per tjänst, och API-nycklar som kan återkallas.
- En händelselogg över inloggningar och ändringar, och en översikt över aktiva sessioner.

AI i supporten

- Together AI behandlar ärenden och chattar med lagring av frågor och svar avstängd, och utan att använda dem för träning.
- När Together AI inte är tillgängligt tar Anthropic eller Google över, vilket händer sällan. Ingen av dem använder uppgifterna för träning; de kan spara dem en begränsad tid för att upptäcka missbruk.
- Assistenten läser uppgifter i Kundens tjänster bara i samband med Kundens ärende eller fråga.