Databehandleraftale (DPA)

i henhold til artikel 28 i den generelle forordning om databeskyttelse (GDPR)

Version 1.0, pr. 22. september 2026

Parter

Kunden (dataansvarlig, jf. artikel 4, nr. 7, i GDPR):

Virksomhed / navn: _____

Adresse: _____

scryp-kontoens e-mailadresse: _____

scryp (databehandler, jf. artikel 4, nr. 8, i GDPR):

Gökhan Sagir, selvstændig erhvervsdrivende, handlende under varemærket scryp
Erdbergstraße 121/9, 1030 Wien, Østrig
UID: ATU83108129
Kontakt vedrørende databeskyttelse: datenschutz@scryp.at

I det følgende ”Kunden” og ”scryp”, tilsammen ”Parterne”.

Hvad aftalen handler om

Kunden anvender scryp til at få lyd- og videooptagelser transskriberet og analyseret. I disse optagelser taler mennesker, hvis personoplysninger Kunden er ansvarlig for. scryp behandler kun disse oplysninger på vegne af Kunden. Denne aftale fastlægger, hvad scryp må gøre med oplysningerne, hvordan scryp beskytter dem, og hvad der til sidst sker med dem.

1. Genstand og anvendelsesområde

1.1 Denne aftale gælder for alle personoplysninger, som scryp behandler på vegne af Kunden ved leveringen af tjenesten scryp i henhold til servicevilkårene (tilgængelige på www.scryp.at/agb). Aftalen om brug af tjenesten benævnes i det følgende ”Hovedaftalen”. Den til enhver tid gældende version af denne aftale er tilgængelig på www.scryp.at/avv.

1.2 Denne aftale omfatter ikke oplysningerne om selve aftaleforholdet, dvs. Kundens konto-, aftale-, fakturerings- og supportoplysninger. Disse behandler scryp som selvstændig dataansvarlig i henhold til sin privatlivspolitik (www.scryp.at/datenschutz).

1.3 Bilag 1 til 3 er en del af denne aftale. Ved uoverensstemmelser mellem denne aftale og Hovedaftalen har denne aftale forrang i spørgsmål om databeskyttelse.

1.4 Denne aftale er beregnet til kunder, der anvender scryp som led i erhvervsmæssig, forretningsmæssig eller offentlig virksomhed. Ved rent privat brug finder GDPR ikke anvendelse, jf. artikel 2, stk. 2, litra c), og der kræves ingen databehandleraftale.

2. Behandlingens art, formål og omfang

2.1 Behandlingens art og formål, typerne af oplysninger og kategorierne af registrerede er beskrevet i bilag 1.

2.2 scryp behandler oplysningerne udelukkende i Den Europæiske Unions medlemsstater. Behandlingsstederne er angivet i bilag 1 og bilag 3.

2.3 Behandlingens varighed svarer til Hovedaftalens løbetid med tillæg af de slettefrister, der er fastsat i punkt 12.

3. Instrukser

3.1 scryp behandler kun oplysningerne efter dokumenteret instruks fra Kunden. Kundens instrukser udgøres af Hovedaftalen, denne aftale og Kundens brug af tjenestens funktioner (navnlig upload, transskription, analyse, redigering, deling, eksport og sletning). Enhver brug af en funktion udgør en dokumenteret enkeltinstruks om at udføre den tilhørende behandling.

3.2 Yderligere instrukser giver Kunden skriftligt; e-mail til datenschutz@scryp.at er tilstrækkelig. Instruksberettigede er kontoindehaveren og de personer, som Kunden lader anvende sin scryp-konto. Instrukser, der går ud over tjenestens ydelsesomfang, anses for en anmodning om ændring af ydelsen.

3.3 Er en instruks efter scryps opfattelse i strid med GDPR eller andre databeskyttelsesregler, underretter scryp straks Kunden. scryp kan udsætte udførelsen, indtil Kunden bekræfter eller ændrer instruksen.

3.4 scryp anvender ikke oplysningerne til egne formål. Navnlig anvendes Kundens optagelser, transskriptioner og analyser ikke til træning eller forbedring af AI-modeller og videregives ikke til tredjemand, medmindre andet følger af denne aftale.

3.5 Kræver en myndighed eller en domstol, at scryp udleverer Kundens oplysninger, underretter scryp straks Kunden, i det omfang det er retligt tilladt, henviser myndigheden til Kunden og udleverer kun det, som scryp er retligt forpligtet til. scryp undersøger i den forbindelse, om en lovbestemt tavshedspligt for Kunden er til hinder for udleveringen (§ 6, stk. 5, i den østrigske DSG).

4. Kundens forpligtelser

4.1 Kunden er ansvarlig for, at optagelserne og behandlingen af dem er lovlige. Kunden sørger navnlig for et retsgrundlag (artikel 6 og ved særlige kategorier artikel 9 i GDPR), for information af de registrerede (artikel 13 og 14 i GDPR) og for, at ikke-offentlige udtalelser ikke optages uden de talendes samtykke (f.eks. § 120 StGB i Østrig).

4.2 Indeholder optagelser særlige kategorier af personoplysninger (f.eks. helbredsoplysninger) eller indhold, der er omfattet af en erhvervsmæssig tavshedspligt, undersøger Kunden på forhånd, om behandlingen er tilladt, og om der kræves en konsekvensanalyse vedrørende databeskyttelse (artikel 35 i GDPR). scryp stiller til dette formål oplysningerne i denne aftale og dens bilag til rådighed.

4.3 Kunden holder e-mailadressen for sin scryp-konto opdateret. Til denne adresse sender scryp alle meddelelser i henhold til denne aftale, navnlig underretninger i henhold til punkt 10.

4.4 Kunden har ret til at give scryp instrukser, kræve dokumentation og gennemføre revisioner i henhold til punkt 11.

5. Fortrolighed og tavshedspligt

5.1 scryp giver kun adgang til oplysningerne til personer, der er forpligtet til at iagttage datahemmeligheden (§ 6 i den østrigske DSG) og til fortrolighed og er vejledt om følgerne af en overtrædelse (artikel 28, stk. 3, litra b), og artikel 29 i GDPR). Forpligtelsen gælder også efter arbejdsforholdets ophør.

5.2 scryp er opbygget således, at Kundens indhold (optagelser, transskriptioner, analyser, fil- og mappenavne) kun lagres i krypteret form og kun foreligger i klartekst i behandlingsservernes arbejdshukommelse, mens den

pågældende behandling varer. Personer hos scryp har under den løbende drift ingen adgang til indhold i klartekst. Nærmere oplysninger findes i bilag 2.

5.3 Er Kunden underlagt en lovbestemt tavshedspligt (f.eks. § 9 RAO, § 54 ÄrzteG, § 121 StGB i Østrig), forpligter scryp sig som Kundens medhjælper til på samme måde at hemmeligholde alt indhold, som scryp får adgang til i forbindelse med ydelsen. For kunder, der er underlagt tysk ret, gælder dette samtidig som en forpligtelse til hemmeligholdelse i henhold til § 203, stk. 4, StGB (Tyskland). Efter anmodning bekræfter scryp denne forpligtelse i en særskilt erklæring.

6. Behandlingssikkerhed

6.1 scryp træffer de tekniske og organisatoriske foranstaltninger i henhold til artikel 32 i GDPR, som er beskrevet i bilag 2.

6.2 scryp kan videreudvikle disse foranstaltninger og erstatte dem med tilsvarende eller bedre foranstaltninger. Beskyttelsesniveauet må derved ikke forringes. Væsentlige ændringer dokumenterer scryp og meddeler dem til Kunden. Den til enhver tid gældende version af bilag 2 er tilgængelig på www.scryp.at/avv.

6.3 scryp kontrollerer mindst én gang årligt, om foranstaltningerne er effektive, og meddeler efter anmodning Kunden resultatet.

7. Underdatabehandlere

7.1 Kunden godkender de underdatabehandlere, der er anført i bilag 3 (generel godkendelse i henhold til artikel 28, stk. 2, i GDPR).

7.2 Ønsker scryp at tilføje eller udskifte en underdatabehandler, underretter scryp Kunden mindst 30 dage før ibrugtagningen pr. e-mail til scryp-kontoens adresse. Kunden kan inden 14 dage efter modtagelsen af denne meddelelse gøre skriftlig indsigelse af en væsentlig databeskyttelsesretlig grund; e-mail er tilstrækkelig. Gør Kunden ikke indsigelse, anses ændringen for godkendt.

7.3 Finder Parterne ikke en løsning efter en indsigelse, kan Kunden opsige Hovedaftalen med virkning fra tidspunktet for den planlagte ibrugtagning. Vederlag, som Kunden har forudbetalt for tiden efter ophøret, tilbagebetaler scryp forholdsmæssigt.

7.4 scryp pålægger ved aftale enhver underdatabehandler de samme databeskyttelsesforpligtelser, som påhviler scryp i henhold til denne aftale, navnlig tilstrækkelige garantier for passende tekniske og organisatoriske foranstaltninger (artikel 28, stk. 4, i GDPR). Opfylder en underdatabehandler ikke sine forpligtelser, hæfter scryp over for Kunden for dennes forpligtelser som for egne handlinger.

7.5 Biydelser uden adgang til kundeoplysninger, f.eks. telekommunikation, rengøring eller vedligeholdelse uden dataadgang, udgør ikke underdatabehandling.

8. Behandlingssted og tredjelande

8.1 scryp behandler og lagrer oplysningerne i Østrig og Tyskland. scryp foretager ingen overførsel til lande uden for Den Europæiske Union eller Det Europæiske Økonomiske Samarbejdsområde.

8.2 Skulle en underdatabehandler behandle oplysninger i et tredjeland, sker dette kun i det omfang, der er beskrevet i bilag 3, og kun med en passende garanti i henhold til kapitel V i GDPR (f.eks. en tilstrækkelighedsafgørelse fra Europa-Kommissionen eller EU's standardkontraktbestemmelser).

9. Bistand til Kunden

9.1 De registreredes rettigheder: Kunden kan i de fleste tilfælde selv opfylde anmodninger om indsigt, berigtigelse, sletning og dataportabilitet via tjenestens funktioner (visning, redigering, eksport, sletning). Da scryp kun opbevarer indhold i krypteret form, kan scryp ikke fastslå, hvilke personer der forekommer i en optagelse. Henvender en registreret sig til scryp, videresender scryp straks henvendelsen til Kunden og besvarer den ikke selv, medmindre Kunden instruerer scryp herom.

9.2 Sikkerhed, brud på persondatasikkerheden, konsekvensanalyse vedrørende databeskyttelse og høring af tilsynsmyndigheden (artikel 32 til 36 i GDPR): scryp bistår Kunden med de oplysninger, som scryp råder over, navnlig denne aftale, bilag 2 og oplysningerne om en hændelse i henhold til punkt 10.

9.3 For bistand, der går ud over tilrådighedsstillelsen af de oplysninger og funktioner, der er beskrevet i denne aftale, kan scryp efter forudgående varsel kræve et rimeligt vederlag efter medgået tid. Dette gælder ikke, hvis bistanden bliver nødvendig på grund af en fejl fra scryps side.

10. Underretning om brud på persondatasikkerheden

10.1 Bliver scryp bekendt med et brud på persondatasikkerheden, der vedrører Kundens oplysninger, underretter scryp Kunden herom uden unødig forsinkelse og senest 48 timer efter at være blevet bekendt med bruddet, pr. e-mail til scryp-kontoens adresse.

10.2 Underretningen indeholder, i det omfang det er kendt: bruddets karakter, de berørte typer af oplysninger og det omtrentlige antal berørte registrerede, de sandsynlige konsekvenser, de trufne og foreslåede foranstaltninger samt et kontaktpunkt hos scryp. Oplysninger, der endnu ikke foreligger, eftersender scryp uden unødig forsinkelse.

10.3 scryp dokumenterer bruddet og bistår Kunden med anmeldelsen til tilsynsmyndigheden og underretningen af de registrerede. Anmeldelser til myndigheder eller underretninger af registrerede på Kundens vegne foretager scryp kun efter Kundens instruks. Underretningen af Kunden udgør ikke en erkendelse af skyld.

11. Dokumentation og revisioner

11.1 scryp stiller alle oplysninger til rådighed for Kunden, der er nødvendige for at påvise overholdelse af forpligtelserne i henhold til artikel 28 i GDPR. Hertil hører denne aftale, beskrivelsen af foranstaltningerne i bilag 2, fortegnelsen i henhold til artikel 30, stk. 2, i GDPR, underdatabehandlernes certificeringer og skriftlige svar på begrundede spørgsmål fra Kunden.

11.2 Er denne dokumentation i det konkrete tilfælde ikke tilstrækkelig, kan Kunden selv eller gennem en revisor, der er forpligtet til fortrolighed og ikke er konkurrent til scryp, gennemføre en revision, herunder inspektion. Revisioner finder sted højst én gang pr. kalenderår, med et varsel på mindst 30 dage, inden for normal arbejdstid og uden forstyrrelse af driften. Ved konkrete holdepunkter for en overtrædelse eller efter anmodning fra en tilsynsmyndighed kan revisionen også gennemføres med kort varsel og hyppigere.

11.3 Revisionen omfatter ikke andre kunders oplysninger og ikke underdatabehandlernes datacentre. For disse gælder deres certificeringer og revisionsrapporter. Hver part bærer sine egne omkostninger ved revisionen.

12. Sletning og tilbagelevering af oplysningerne

12.1 I løbetiden kan Kunden til enhver tid selv slette sine oplysninger og eksportere dem i gængse formater. Slettet indhold fjernes straks fra det aktive datalager.

12.2 Uploadede originalfiler sletter scryp automatisk efter afslutningen af behandlingen, som regel inden for få minutter og senest 72 timer efter uploaden. Kun den krypterede afspilningsversion, den krypterede transskription og de krypterede analyser bevares.

12.3 Efter Hovedaftalens ophør er indholdet fortsat tilgængeligt for Kunden til eksport i op til 90 dage. Derefter sletter scryp det automatisk, inklusive alle kopier. Sletter Kunden sin konto, slettes alle oplysninger straks.

12.4 Sikkerhedskopier tjener kun til gendannelse af det samlede system. De indeholder udelukkende Kundens indhold i krypteret form og overskrives senest efter 30 dage. Der foretages ingen gendannelse af enkelte slettede kundeoplysninger fra sikkerhedskopier.

12.5 Oplysninger, som scryp fortsat skal opbevare på grund af lovbestemte opbevaringspligter (f.eks. fakturaoplysninger i henhold til § 132 i den østrigske BAO), er undtaget fra sletningen. De spærres og slettes efter fristens udløb.

12.6 Efter anmodning bekræfter scryp sletningen skriftligt; e-mail er tilstrækkelig.

13. Ansvar

13.1 Over for de registrerede hæfter Parterne i henhold til artikel 82 i GDPR.

13.2 I forholdet mellem Parterne gælder Hovedaftalens ansvarsbestemmelser, i det omfang loven tillader det. For underdatabehandlere hæfter scryp som for egne handlinger (punkt 7.4).

13.3 Har en part betalt erstatning til registrerede, kan den kræve den del tilbage fra den anden part, der svarer til dennes andel af ansvaret for skaden (artikel 82, stk. 5, i GDPR).

13.4 Fastholder Kunden en instruks, selv om scryp i henhold til punkt 3.3 har gjort Kunden opmærksom på, at den er ulovlig, friholder Kunden scryp for alle krav fra tredjemand og bøder, der beror på denne instruks.

14. Løbetid, suspension og ophør

14.1 Denne aftale gælder, så længe scryp behandler oplysninger for Kunden, dvs. i Hovedaftalens løbetid og indtil sletningen i henhold til punkt 12 er afsluttet.

14.2 For kunder omfattet af punkt 1.4 er brug af tjenesten uden denne aftale ikke forudset. Opsigelse af denne aftale gælder derfor samtidig som opsigelse af Hovedaftalen.

14.3 Overtræder scryp denne aftale, kan Kunden kræve, at scryp suspenderer den berørte behandling, indtil overtrædelsen er afhjulpet. Afhjælper scryp ikke en væsentlig overtrædelse inden en måned efter påkrav, kan Kunden ophæve Hovedaftalen uden varsel.

15. Afsluttende bestemmelser

15.1 Denne aftale indgås i elektronisk form (artikel 28, stk. 9, i GDPR). For kunder omfattet af punkt 1.4 bliver den gennem indarbejdelsen i servicevilkårene en del af aftalen ved indgåelsen af Hovedaftalen; aftalepart er da indehaveren af scryp-kontoen med de oplysninger, der er registreret dér. Derudover kan den indgås ved begge parters underskrift af dette dokument, også som elektronisk kopi.

15.2 Ændringer af denne aftale skal ske skriftligt; e-mail er tilstrækkelig. scryp kan tilpasse bilag 2 i henhold til punkt 6.2 og bilag 3 i henhold til punkt 7.2. Andre ændringer varsler scryp pr. e-mail mindst 30 dage før ikrafttrædelsen; Kunden kan indtil da gøre indsigelse og opsige Hovedaftalen med virkning fra dette tidspunkt. scryp opbevarer hver version af denne aftale med versionsnummer og dato.

15.3 Østrigsk ret finder anvendelse; GDPR berøres ikke heraf. Er Kunden erhvervsdrivende, er den sagligt kompetente domstol i Wien eneste værneting for alle tvister, der udspringer af denne aftale. Ufravigelige lovbestemte værneting berøres ikke heraf.

15.4 Skulle en bestemmelse være ugyldig, forbliver resten af aftalen gyldig. Den ugyldige bestemmelse erstattes af den lovregel, der kommer dens formål nærmest.

15.5 Kontaktpunkt for alle spørgsmål vedrørende denne aftale er hos scryp datenschutz@scryp.at. På Kundens side er det scryp-kontoens e-mailadresse, medmindre Kunden meddeler andet.

15.6 scryp stiller denne aftale til rådighed på flere sprog. Den tyske version er bindende; oversættelser tjener til forståelse. Ved uoverensstemmelser gælder den tyske ordlyd.

Underskrifter

For Kunden	**For scryp**
Sted, dato	Sted, dato
Navn, stilling	Gökhan Sagir, selvstændig erhvervsdrivende
Underskrift	Underskrift

Bilag 1: Beskrivelse af behandlingen

Punkt	Beskrivelse
Genstand	Levering af tjenesten scryp: transskription af lyd- og videooptagelser med talegenkendelse og talergenkendelse, i Ultra-planen desuden AI-funktioner (AI-understøttet analyse: resumé, referat, opgaveliste, tekst til sociale medier), samt lagring, redigering, eksport og deling af resultaterne.
Formål	Kunden får egne optagelser omdannet til tekst og analyseret, f.eks. møder, interviews, diktater, rådgivningssamtaler, foredrag eller podcasts.
Behandlingens art	Modtagelse af krypterede filer, kortvarig dekryptering i behandlingsservernes arbejdshukommelse, automatisk transskription og analyse, kryptering af resultaterne, krypteret lagring, tilrådighedsstillelse i Kundens konto, sletning.
Typer af oplysninger	Taleoptagelser og videoer (stemme, talt indhold), transskriptioner og analyser genereret heraf, tilknytning af talere, fil- og mappenavne tildelt af Kunden, tekniske metadata (varighed, filstørrelse, tidspunkter, registreret sprog, behandlingsstatus), ved delte transskriptioner delingslinket. Alt indhold lagres krypteret; kun de tekniske metadata foreligger i klartekst.
Særlige kategorier (artikel 9 i GDPR)	Muligt, afhængigt af indholdet af Kundens optagelser (f.eks. helbredsoplysninger i lægediktater, oplysninger i rådgivnings- eller klientsamtaler). scryp kender ikke indholdet. Kunden vurderer lovligheden i henhold til punkt 4.2.
Garantier for særlige kategorier	Kryptering i Kundens browser, klartekst kun i arbejdshukommelsen på scryps egne servere i Wien, ingen videregivelse af indhold i klartekst til underdatabehandlere, ingen adgang for personer til indhold under den løbende drift, tavshedspligt i henhold til punkt 5, ingen træning af AI-modeller med kundeoplysninger.
Registrerede	Personer, der taler eller nævnes i optagelserne (f.eks. medarbejdere, kunder, patienter, klienter, interviewpersoner, deltagere i møder og arrangementer), samt brugerne af kundekontoen.
Behandlingssteder	Transskription og AI-analyse: scryps egne GPU-servere i Wien, Østrig. Webapplikation, grænseflader, database, krypteret fillager og sikkerhedskopier: Hetzner Online GmbH's datacenter i Nürnberg, Tyskland.
Varighed	Hovedaftalens løbetid med tillæg af slettefrister i henhold til punkt 12.

Bilag 2: Tekniske og organisatoriske foranstaltninger (artikel 32 i GDPR)

Pr. 22. september 2026. Foranstaltningerne beskriver scryps normale drift.

1. Kryptering og zero-knowledge-arkitektur

- Optagelser krypteres allerede i Kundens browser med AES-256-GCM, før de overføres til scryp. For hver fil genereres en egen filnøgle (FEK).
- Filnøgler krypteres med kontoens hovednøgle (MEK). Hovednøglen er kun tilgængelig med Kundens adgangskode (afledning med PBKDF2-SHA256, 600.000 iterationer). scryp kender hverken adgangskoden eller hovednøglen i klartekst.
- Til transskriptionen sender browseren filnøglen til scryp krypteret med en servernøgle (RSA-4096, OAEP). Behandlingsserveren dekrypterer optagelsen udelukkende i arbejdshukommelsen. Midlertidige filer ligger i et RAM-filsystem og kasseres efter opgaven; ukrypteret indhold skrives på intet tidspunkt til et lagermedie.
- Transskriptioner og analyser krypteres umiddelbart efter oprettelsen med filnøglen og lagres kun i krypteret form. Fil- og mappenavne krypteres i browseren.
- Ved deling af en transskription krypteres filnøglen med en nøgle, der er afledt af delingsadgangskoden. Modtagere dekrypterer udelukkende i deres egen browser.
- Undtagelse ved URL-upload: Henter Kunden en optagelse via en internetadresse, downloader behandlingsserveren filen direkte, behandler den i arbejdshukommelsen og sletter den derefter; transskription og afspilningsversion lagres krypteret som ellers.
- Alle forbindelser er krypteret med TLS 1.2 eller 1.3.

2. Fysisk adgangskontrol

- Webapplikation, database, fillager og sikkerhedskopier drives i Hetzner Online GmbH's datacenter i Nürnberg (ISO/IEC 27001-certificeret, BSI C5 Type 2-attestering) med operatørens adgangskontrol, videoovervågning og sikkerhedspersonale.
- GPU-serverne til transskription og AI-analyse står i scryps egne, aflåste lokaler i Wien. Kun berettigede personer har adgang; adgangen er mekanisk aflåst og derudover biometrisk sikret.
- Alle lagermedier i disse servere er fuldt krypteret. Ved tyveri eller udtagning af et lagermedie forbliver oplysningerne ulæselige uden nøglen. Ukrypteret indhold foreligger på disse servere kun i arbejdshukommelsen under en igangværende opgave og skrives aldrig til et lagermedie.

3. System- og dataadgangskontrol

- Serveradgang kun for scryps administratorer via krypterede SSH-forbindelser med personlige nøgler henholdsvis tilfældigt genererede, stærke adgangskoder; adgang efter princippet om færrest mulige rettigheder.
- Separat administrationsgrænseflade med egen indlogning, begrænset til godkendte IP-adresser. Administrationsgrænsefladen viser kun konto- og opgavemetadata, intet indhold.
- Brugerkonti: Adgangskoder hashes med Argon2id; beskyttelse mod indlogningsforsøg gennem ratebegrænsning og midlertidig spærring; sessioner kører uden cookies med kortlivede tokens.
- Beskyttelse af grænsefladerne mod misbrug og overbelastning gennem ratebegrænsning og automatiske spærringer.
- Automatiserede tjenester (behandlingsservere) autentificerer sig med egne, roterbare adgangsoplysninger og modtager kun de nøgler, der er nødvendige for den pågældende opgave.

4. Adskillelseskontrol og pseudonymisering

- Kryptografisk adskillelse: Hver kunde har sin egen hovednøgle, hver fil sin egen filnøgle. En kundes indhold kan ikke læses med fremmede nøgler.
- Logisk adskillelse af produktions-, database-, cache- og overvågningssystemer i separate netværkszoner.
- Behandlingsopgaver til GPU-serverne indeholder hverken navne eller e-mailadresser, kun de tekniske data, der er nødvendige for opgaven.

5. Integritet og sporbarhed

- Alle ændringer af applikation og infrastruktur sker via versionsstyret kildekode og automatiseret, sporbar udrulning; software-images fastlægges ud fra deres kontrolsum.
- Kontohændelser (f.eks. indlogning, sletning, abonnementsændringer) logges med tidspunkt, uden IP-adresser.
- Systemlogfiler indeholder intet indhold og slettes efter 14 dage. IP-adresser lagres ikke og logges ikke. Til afværgelse af misbrug tælles adgange kun via et kortlivet pseudonym, som dannes med en hemmelig nøgle, ikke kan regnes tilbage og udløber efter højst en time.

6. Tilgængelighed og robusthed

- Højtilgængelig klynge af tre servere med belastningsfordeling; database med synkron replikering på tre noder; cache med automatisk failover.
- Daglig krypteret sikkerhedskopiering af databasen med gendannelse til ethvert tidspunkt inden for de seneste 30 dage; klyngekonfigurationen sikkerhedskopieres hver sjette time. Sikkerhedskopierne ligger i datacentret i Nürnberg.
- Udrulning af nye versioner uden driftsafbrydelse; beskyttelse mod overbelastningsangreb på netværks- og applikationsniveau.
- Løbende overvågning med automatisk alarmering ved forstyrrelser.

7. Sletning og dataminimering

- Uploadede originalfiler slettes efter behandlingen, som regel inden for få minutter; en automatisk regel fjerner efterladte uploads senest efter 72 timer.
- Kunden sletter til enhver tid selv indhold og konto; sletningen har øjeblikkelig virkning i det aktive datalager. Efter et abonnements ophør slettes indhold automatisk efter 90 dage.
- Ingen cookies, ingen sporings- eller analyseværktøjer fra tredjeparter, ingen lagring af IP-adresser.

8. Organisation

- Alle personer, der arbejder for scryp, er forpligtet til at iagttage datahemmeligheden og til fortrolighed og er instrueret i sikkerhedsarkitekturen.
- scryp fører en fortegnelse over behandlingsaktiviteter (artikel 30 i GDPR). Konsekvensanalyse vedrørende databeskyttelse, fortegnelse og disse foranstaltninger gennemgås mindst årligt og ved væsentlige ændringer.
- Hændelsesproces: opdagelse gennem overvågning, vurdering, inddæmning, underretning af berørte kunder i henhold til aftalens punkt 10, efterbehandling.
- Underdatabehandlere kontrolleres for deres garantier før ibrugtagningen og forpligtes aftalemæssigt i henhold til artikel 28, stk. 4, i GDPR.

Bilag 3: Underdatabehandlere

Pr. 22. september 2026.

Underdatabehandler	Ydelse	Oplysninger	Behandlingssted	Garanti
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Tyskland	Drift af serverne til webapplikation, grænseflader og database; krypteret objektlager; sikkerhedskopier	Alle oplysninger nævnt i bilag 1, indhold udelukkende i krypteret form	Nürnberg, Tyskland (EU)	Databehandleraftale; ISO/IEC 27001; BSI C5
Mailjet GmbH (Sinch-koncernen), Alt Moabit 2, 10557 Berlin, Tyskland	Afsendelse af system-e-mails (f.eks. meddelelsen ”Transskription færdig”)	Kontoens e-mailadresse, opgavens dato, link til kontoen; intet indhold, ingen filnavne	Frankrig (EU)	Databehandleraftale; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, Irland	Modtagelse og behandling af supporthenvendelser pr. e-mail (Microsoft 365)	Kun oplysninger, som Kunden selv sender i en supporthenvendelse	EU; fjernadgang fra tredjelande mulig	Databehandleraftale; EU's standardkontraktbestemmelser; EU-US Data Privacy Framework