

Smlouva o zpracování osobních údajů (DPA)

podle čl. 28 obecného nařízení o ochraně osobních údajů (GDPR)

Version 1.0, stav ke dni 22. září 2026

Smluvní strany

Zákazník (správce ve smyslu čl. 4 bodu 7 GDPR):

Firma / jméno: _____

Adresa: _____

E-mail účtu scryp: _____

scryp (zpracovatel ve smyslu čl. 4 bodu 8 GDPR):

Gökhan Sagir, podnikající fyzická osoba, jednající pod značkou scryp

Erdbergstraße 121/9, 1030 Vídeň, Rakousko

UID: ATU83108129

Kontakt pro ochranu osobních údajů: datenschutz@scryp.at

Dále jen „zákazník“ a „scryp“, společně „smluvní strany“.

O co jde

Zákazník používá scryp k tomu, aby si nechal přepsat a vyhodnotit zvukové nahrávky a videonahrávky. V těchto nahrávkách hovoří lidé, za jejichž osobní údaje odpovídá zákazník. scryp tyto údaje zpracovává pouze z pověření zákazníka. Tato smlouva stanoví, co smí scryp s údaji dělat, jak je scryp chrání a co se s nimi nakonec stane.

1. Předmět a působnost

1.1 Tato smlouva se vztahuje na všechny osobní údaje, které scryp zpracovává z pověření zákazníka při poskytování služby scryp podle Podmínek poskytování služeb (VOP, dostupných na www.scryp.at/agb). Smlouva o používání služby je dále označována jako „hlavní smlouva“. Aktuální znění této smlouvy je k dispozici na www.scryp.at/avv.

1.2 Předmětem této smlouvy nejsou údaje samotného smluvního vztahu, tedy údaje o účtu, smlouvě, fakturaci a podpoře zákazníka. Tyto údaje zpracovává scryp jako samostatný správce podle svých Zásad ochrany osobních údajů (www.scryp.at/datenschutz).

1.3 Přílohy 1 až 3 jsou součástí této smlouvy. V případě rozporu mezi touto smlouvou a hlavní smlouvou má v otázkách ochrany osobních údajů přednost tato smlouva.

1.4 Tato smlouva je určena zákazníkům, kteří používají scryp v rámci profesní, podnikatelské nebo úřední činnosti. Při čistě soukromém používání se GDPR podle čl. 2 odst. 2 písm. c) nepoužije a smlouva o zpracování osobních údajů není zapotřebí.

2. Povaha, účel a rozsah zpracování

2.1 Povaha a účel zpracování, typy údajů a kategorie subjektů údajů jsou popsány v příloze 1.

2.2 scryp zpracovává údaje výhradně v členských státech Evropské unie. Místa zpracování jsou uvedena v příloze 1 a příloze 3.

2.3 Doba zpracování odpovídá době trvání hlavní smlouvy prodloužené o lhůty pro výmaz upravené v bodě 12.

3. Pokyny

3.1 scryp zpracovává údaje pouze na základě doložených pokynů zákazníka. Pokyny zákazníka tvoří hlavní smlouva, tato smlouva a používání funkcí služby zákazníkem (zejména nahrávání, přepis, vyhodnocování, úpravy, sdílení, export a mazání). Každé použití funkce je doloženým jednotlivým pokynem k provedení příslušného zpracování.

3.2 Další pokyny uděluje zákazník písemně; postačí e-mail na adresu datenschutz@scryp.at. K udělování pokynů jsou oprávněni držitel účtu a osoby, které zákazník pro svůj účet scryp pověří. Pokyny, které přesahují rozsah plnění služby, se považují za žádost o změnu plnění.

3.3 Je-li pokyn podle názoru scryp v rozporu s GDPR nebo jinými předpisy o ochraně osobních údajů, scryp o tom zákazníka neprodleně informuje. scryp smí provedení pokynu pozastavit, dokud jej zákazník nepotvrdí nebo nezmění.

3.4 scryp nepoužívá údaje pro vlastní účely. Zejména se nahrávky, přepisy a vyhodnocení zákazníka nepoužívají k trénování ani zlepšování modelů umělé inteligence a nepředávají se třetím osobám, pokud tato smlouva nestanoví jinak.

3.5 Požaduje-li od scryp úřad nebo soud vydání údajů zákazníka, informuje scryp zákazníka neprodleně, pokud je to právně přípustné, odkáže daný orgán na zákazníka a vydá pouze to, k čemu je scryp ze zákona povinen. scryp přitom prověří, zda vydání nebrání zákonná povinnost mlčenlivosti zákazníka (§ 6 odst. 5 DSG).

4. Povinnosti zákazníka

4.1 Zákazník odpovídá za zákonnost nahrávek a jejich zpracování. Zajistí zejména právní základ (čl. 6, u zvláštních kategorií čl. 9 GDPR), informování subjektů údajů (čl. 13 a 14 GDPR) a to, aby nebyly bez souhlasu hovořících osob nahrávány neveřejné projevy (například § 120 StGB v Rakousku).

4.2 Obsahují-li nahrávky zvláštní kategorie osobních údajů (například údaje o zdravotním stavu) nebo obsah podléhající profesnímu tajemství, zákazník předem prověří, zda je zpracování přípustné a zda je nutné posouzení vlivu na ochranu osobních údajů (čl. 35 GDPR). scryp k tomu poskytuje informace obsažené v této smlouvě a jejích přílohách.

4.3 Zákazník udržuje e-mailovou adresu svého účtu scryp aktuální. Na tuto adresu zasílá scryp veškerá sdělení podle této smlouvy, zejména ohlášení podle bodu 10.

4.4 Zákazník má právo udělovat scryp pokyny, požadovat doložení souladu a provádět audity podle bodu 11.

5. Důvěrnost a profesní tajemství

5.1 scryp umožňuje přístup k údajům pouze osobám, které jsou zavázány k zachování datového tajemství (§ 6 DSG) a k mlčenlivosti a byly poučeny o důsledcích jejich porušení (čl. 28 odst. 3 písm. b), čl. 29 GDPR). Tento závazek trvá i po skončení činnosti.

5.2 scryp je koncipován tak, aby se obsah zákazníka (nahrávky, přepisy, vyhodnocení, názvy souborů a složek) ukládal pouze v zašifrované podobě a v otevřené podobě se nacházel pouze po dobu příslušného zpracování v operační paměti zpracovatelských serverů. Osoby na straně scryp nemají za běžného provozu přístup k obsahu v otevřené podobě. Podrobnosti jsou uvedeny v příloze 2.

5.3 Podléhá-li zákazník zákonné povinnosti mlčenlivosti (například § 9 RAO, § 54 ÄrzteG, § 121 StGB), zavazuje se scryp jako pomocná osoba zákazníka zachovávat stejným způsobem tajnost veškerého obsahu, který se scryp v

rámci poskytování plnění zpřístupní. U zákazníků podléhajících německému právu to platí zároveň jako závazek k zachování mlčenlivosti podle § 203 odst. 4 StGB (Německo). Na žádost scryp tento závazek potvrdí samostatným prohlášením.

6. Zabezpečení zpracování

6.1 scryp přijímá technická a organizační opatření podle čl. 32 GDPR, která jsou popsána v příloze 2.

6.2 scryp smí tato opatření dále rozvíjet a nahrazovat je rovnocennými nebo lepšími. Úroveň ochrany přitom nesmí klesnout. Podstatné změny scryp zdokumentuje a sdělí zákazníkovi. Aktuální znění přílohy 2 je k dispozici na www.scryp.at/avv.

6.3 scryp ověřuje účinnost opatření nejméně jednou ročně a na žádost sdělí zákazníkovi výsledek.

7. Další zpracovatelé

7.1 Zákazník schvaluje další zpracovatele uvedené v příloze 3 (obecné povolení podle čl. 28 odst. 2 GDPR).

7.2 Chce-li scryp přidat nebo nahradit dalšího zpracovatele, informuje zákazníka nejméně 30 dnů před jeho nasazením e-mailem na adresu účtu scryp. Zákazník může do 14 dnů od doručení tohoto oznámení písemně vznést námitku ze závažného důvodu týkajícího se ochrany osobních údajů; postačí e-mail. Nevznese-li zákazník námitku, považuje se změna za schválenou.

7.3 Nenajdou-li smluvní strany po vznesení námítky řešení, může zákazník vypovědět hlavní smlouvu k okamžiku plánovaného nasazení. Úplaty, které zákazník uhradil předem za dobu po ukončení, scryp poměrně vrátí.

7.4 scryp uloží každému dalšímu zpracovateli smluvně stejné povinnosti v oblasti ochrany osobních údajů, jaké má podle této smlouvy scryp, zejména dostatečné záruky vhodných technických a organizačních opatření (čl. 28 odst. 4 GDPR). Neplní-li další zpracovatel své povinnosti, odpovídá scryp zákazníkovi za jeho povinnosti jako za vlastní jednání.

7.5 Vedlejší služby bez přístupu k údajům zákazníka, například telekomunikace, úklid nebo údržba bez přístupu k údajům, nejsou zpracováním dalším zpracovatelem.

8. Místo zpracování a třetí země

8.1 scryp zpracovává a ukládá údaje v Rakousku a Německu. K předávání do zemí mimo Evropskou unii nebo Evropský hospodářský prostor ze strany scryp nedochází.

8.2 Pokud by další zpracovatel zpracovával údaje ve třetí zemi, děje se tak pouze v rozsahu popsaném v příloze 3 a pouze s vhodnou zárukou podle kapitoly V GDPR (například rozhodnutí Evropské komise o odpovídající ochraně nebo standardní smluvní doložky EU).

9. Součinnost poskytovaná zákazníkovi

9.1 Práva subjektů údajů: Zákazník může práva na přístup, opravu, výmaz a přenositelnost údajů ve většině případů naplnit sám prostřednictvím funkcí služby (zobrazení, úpravy, export, výmaz). Protože scryp uchovává obsah pouze v zašifrované podobě, nemůže scryp zjistit, které osoby se v nahrávce vyskytují. Obrátí-li se subjekt údajů na scryp, postoupí scryp žádost neprodleně zákazníkovi a sám na ni neodpovídá, ledaže k tomu zákazník scryp udělí pokyn.

9.2 Zabezpečení, porušení zabezpečení osobních údajů, posouzení vlivu na ochranu osobních údajů a konzultace s dozorovým úřadem (čl. 32 až 36 GDPR): scryp podporuje zákazníka informacemi, které má scryp k dispozici, zejména touto smlouvou, přílohou 2 a údaji o incidentu podle bodu 10.

9.3 Za součinnost, která přesahuje poskytnutí informací a funkcí popsaných v této smlouvě, si scryp může po předchozím oznámení nechat přiměřeně uhradit odměnu podle vynaloženého úsilí. To neplatí, je-li součinnost nutná kvůli chybě na straně scryp.

10. Ohlašování případů porušení zabezpečení osobních údajů

10.1 Dozví-li se scryp o porušení zabezpečení osobních údajů, které se týká údajů zákazníka, ohlásí to zákazníkovi bez zbytečného odkladu, nejpozději do 48 hodin od okamžiku, kdy se o něm dozvěděl, e-mailem na adresu účtu scryp.

10.2 Ohlášení obsahuje, pokud je známo: povahu porušení, dotčené typy údajů a přibližný počet dotčených osob, pravděpodobné důsledky, přijatá a navrhovaná opatření a kontaktní místo u scryp. Informace, které dosud nejsou k dispozici, scryp doplní bez zbytečného odkladu.

10.3 scryp porušení zdokumentuje a podporuje zákazníka při ohlášení dozorovému úřadu a při oznámení subjektům údajů. Ohlášení úřadům nebo oznámení subjektům údajů za zákazníka činí scryp pouze na jeho pokyn. Ohlášení zákazníkovi nepředstavuje uznání zavinění.

11. Doložení souladu a audit

11.1 scryp poskytne zákazníkovi veškeré informace potřebné k doložení toho, že byly splněny povinnosti podle čl. 28 GDPR. Patří k nim tato smlouva, popis opatření v příloze 2, záznamy podle čl. 30 odst. 2 GDPR, certifikace dalších zpracovatelů a písemné odpovědi na odůvodněné dotazy zákazníka.

11.2 Nepostačují-li tyto doklady v jednotlivém případě, může zákazník sám nebo prostřednictvím auditora zavázaného k mlčenlivosti, který není konkurentem scryp, provést audit včetně inspekce. Audity se konají nejvýše jednou za kalendářní rok, po oznámení nejméně 30 dnů předem, v obvyklé pracovní době a bez narušení provozu. Při konkrétních indiciích nasvědčujících porušení nebo na žádost dozorového úřadu je audit možný i v kratší lhůtě a častěji.

11.3 Audit se nevztahuje na údaje jiných zákazníků ani na datová centra dalších zpracovatelů. Pro ta platí jejich certifikace a zprávy o auditech. Každá smluvní strana nese vlastní náklady auditu.

12. Výmaz a vrácení údajů

12.1 Během doby trvání smlouvy může zákazník své údaje kdykoli sám vymazat a exportovat v běžných formátech. Vymazaný obsah je okamžitě odstraněn z aktivních dat.

12.2 Nahrané původní soubory scryp automaticky vymaže po dokončení zpracování, zpravidla během několika minut, nejpozději však 72 hodin po nahrání. Uloženy zůstávají pouze zašifrovaná verze pro přehrávání, zašifrovaný přepis a zašifrovaná vyhodnocení.

12.3 Po skončení hlavní smlouvy zůstává obsah zákazníkovi k dispozici pro export ještě po dobu až 90 dnů. Poté jej scryp včetně všech kopií automaticky vymaže. Odstraní-li zákazník svůj účet, jsou všechny údaje vymazány okamžitě.

12.4 Záložní kopie slouží pouze k obnovení celého systému. Obsah zákazníka obsahují výhradně v zašifrované podobě a jsou přepsány nejpozději po 30 dnech. Obnovení jednotlivých vymazaných údajů zákazníka ze záložních kopií se neprovádí.

12.5 Údaje, které scryp musí nadále uchovávat na základě zákonných povinností uchovávání (například fakturační údaje podle § 132 BAO), jsou z výmazu vyňaty. Jsou zablokovány a po uplynutí lhůty vymazány.

12.6 Na žádost scryp výmaz písemně potvrdí; postačí e-mail.

13. Odpovědnost

13.1 Vůči subjektům údajů odpovídají smluvní strany podle čl. 82 GDPR.

13.2 Ve vzájemném vztahu smluvních stran platí ustanovení hlavní smlouvy o odpovědnosti, pokud to zákon připouští. Za další zpracovatele odpovídá scryp jako za vlastní jednání (bod 7.4).

13.3 Nahradila-li některá smluvní strana újmu subjektům údajů, může od druhé smluvní strany požadovat zpět tu část, která odpovídá jejímu podílu na odpovědnosti za újmu (čl. 82 odst. 5 GDPR).

13.4 Trvá-li zákazník na pokynu, ačkoli jej scryp podle bodu 3.3 upozornil na jeho protiprávnost, zproští zákazník scryp veškerých nároků třetích osob a pokut, které se na tomto pokynu zakládají.

14. Doba trvání, pozastavení a ukončení

14.1 Tato smlouva platí, dokud scryp zpracovává údaje pro zákazníka, tedy po dobu trvání hlavní smlouvy a až do dokončení výmazu podle bodu 12.

14.2 Používání služby bez této smlouvy není u zákazníků podle bodu 1.4 předpokládáno. Výpověď této smlouvy se proto zároveň považuje za výpověď hlavní smlouvy.

14.3 Poruší-li scryp tuto smlouvu, může zákazník požadovat, aby scryp dotčené zpracování pozastavil, dokud nebude porušení odstraněno. Neodstraní-li scryp závažné porušení do jednoho měsíce od výzvy, může zákazník hlavní smlouvu vypovědět bez výpovědní doby.

15. Závěrečná ustanovení

15.1 Tato smlouva se uzavírá v elektronické podobě (čl. 28 odst. 9 GDPR). U zákazníků podle bodu 1.4 se stává součástí smlouvy začleněním do Podmínek poskytování služeb (VOP) uzavřením hlavní smlouvy; smluvní stranou je pak držitel účtu scryp s údaji v něm uloženými. Vedle toho může být uzavřena oboustranným podpisem tohoto dokumentu, a to i jako elektronická kopie.

15.2 Změny této smlouvy vyžadují písemnou formu; postačí e-mail. scryp smí upravovat přílohu 2 podle bodu 6.2 a přílohu 3 podle bodu 7.2. Jiné změny scryp oznámí e-mailem nejméně 30 dnů před jejich účinností; zákazník může do té doby vznést námitku a hlavní smlouvu k tomuto okamžiku vypovědět. scryp uchovává každé znění této smlouvy s číslem verze a datem.

15.3 Použije se rakouské právo; GDPR tím není dotčeno. Je-li zákazník podnikatelem, je pro všechny spory z této smlouvy výlučně příslušný věcně příslušný soud ve Vídni. Kogentní zákonná ustanovení o soudní příslušnosti zůstávají nedotčena.

15.4 Bude-li některé ustanovení neplatné, zůstává zbytek smlouvy v platnosti. Na místo neplatného ustanovení nastupuje zákonná úprava, která se nejvíce blíží jeho účelu.

15.5 Kontaktním místem pro všechny otázky týkající se této smlouvy je na straně scryp adresa datenschutz@scryp.at. Na straně zákazníka je jím e-mailová adresa účtu scryp, pokud zákazník nesdělí jinak.

15.6 scryp poskytuje tuto smlouvu v několika jazycích. Závazné je německé znění; překlady slouží k porozumění. V případě odchylek platí německý text.

Podpisy

Za zákazníka

Místo, datum

Jméno, funkce

Podpis

Za scryp

Místo, datum

Gökhan Sagir, podnikající fyzická osoba

Podpis

Příloha 1: Popis zpracování

Bod	Popis
Předmět	Poskytování služby scryp: přepis zvukových nahrávek a videonahrávek pomocí rozpoznávání řeči a rozpoznávání mluvčích, v tarifu Ultra navíc funkce umělé inteligence (vyhodnocení s podporou umělé inteligence: shrnutí, zápis, seznam úkolů, text pro sociální sítě), jakož i ukládání, úpravy, export a sdílení výsledků.
Účel	Zákazník si nechává vlastní nahrávky převést do textu a vyhodnotit, například porady, rozhovory, diktáty, poradenské rozhovory, přednášky nebo podcasty.
Povaha zpracování	Příjem zašifrovaných souborů, krátkodobé dešifrování v operační paměti zpracovatelských serverů, automatický přepis a vyhodnocení, zašifrování výsledků, zašifrované uložení, zpřístupnění v účtu zákazníka, výmaz.
Typy údajů	Hlasové nahrávky a videa (hlas, mluvený obsah), z nich vytvořené přepisy a vyhodnocení, přiřazení mluvčích, názvy souborů a složek zadané zákazníkem, technická metadata (délka, velikost souboru, časové údaje, rozpoznání jazyk, stav zpracování), u sdílených přepisů odkaz pro sdílení. Veškerý obsah se ukládá v zašifrované podobě; v otevřené podobě jsou pouze technická metadata.
Zvláštní kategorie (čl. 9 GDPR)	Možné, v závislosti na obsahu nahrávek zákazníka (například údaje o zdravotním stavu v lékařských diktátech, údaje z poradenských rozhovorů nebo z jednání s klienty). scryp obsah nezná. Přípustnost prověřuje zákazník podle bodu 4.2.
Záruky pro zvláštní kategorie	Šifrování v prohlížeči zákazníka, otevřená podoba pouze v operační paměti vlastních serverů scryp ve Vídni, žádné předávání obsahu dalším zpracovatelům v otevřené podobě, žádný přístup osob k obsahu za běžného provozu, povinnost mlčenlivosti podle bodu 5, žádné trénování modelů umělé inteligence na údajích zákazníků.
Subjekty údajů	Osoby, které v nahrávkách hovoří nebo jsou v nich zmíněny (například zaměstnanci, zákazníci, pacienti, klienti, respondenti rozhovorů, účastníci porad a akcí), a uživatelé zákaznického účtu.
Místa zpracování	Přepis a vyhodnocení umělou inteligencí: vlastní GPU servery scryp ve Vídni, Rakousko. Webová aplikace, rozhraní, databáze, zašifrované úložiště souborů a záložní kopie: datové centrum společnosti Hetzner Online GmbH v Norimberku, Německo.
Doba trvání	Doba trvání hlavní smlouvy prodloužená o lhůty pro výmaz podle bodu 12.

Příloha 2: Technická a organizační opatření (čl. 32 GDPR)

Stav ke dni 22. září 2026. Opatření popisují běžný provoz scryp.

1. Šifrování a architektura zero-knowledge

- Nahrávky se šifrují již v prohlížeči zákazníka pomocí AES-256-GCM, ještě před přenosem do scryp. Pro každý soubor se vytváří samostatný klíč souboru (FEK).
- Klíče souborů jsou zašifrovány hlavním klíčem účtu (MEK). Hlavní klíč je přístupný pouze s heslem zákazníka (odvození pomocí PBKDF2-SHA256, 600 000 iterací). scryp nezná v otevřené podobě heslo ani hlavní klíč.
- Pro přepis předává prohlížeč klíč souboru do scryp zašifrovaný serverovým klíčem (RSA-4096, OAEP). Zpracovatelský server dešifruje nahrávku výhradně v operační paměti. Dočasné soubory se nacházejí v souborovém systému v paměti RAM a po dokončení úlohy jsou zahozeny; nezašifrovaný obsah se nikdy nezapisuje na datové nosiče.
- Přepisy a vyhodnocení se ihned po vytvoření zašifrují klíčem souboru a ukládají se pouze v zašifrované podobě. Názvy souborů a složek se šifrují v prohlížeči.
- Při sdílení přepisu je klíč souboru zašifrován klíčem odvozeným z hesla pro sdílení. Příjemci dešifrují výhradně ve svém vlastním prohlížeči.
- Výjimka pro nahrávání prostřednictvím URL: Načte-li zákazník nahrávku z internetové adresy, zpracovatelský server soubor stáhne přímo, zpracuje jej v operační paměti a poté jej vymaže; přepis a verze pro přehrávání se ukládají zašifrované jako obvykle.
- Všechna spojení jsou šifrována protokolem TLS 1.2 nebo 1.3.

2. Kontrola vstupu

- Webová aplikace, databáze, úložiště souborů a záložní kopie běží v datovém centru společnosti Hetzner Online GmbH v Norimberku (certifikace ISO/IEC 27001, osvědčení BSI C5 typu 2) s kontrolou vstupu, kamerovým dohledem a bezpečnostním personálem provozovatele.
- GPU servery pro přepis a vyhodnocení umělou inteligencí jsou umístěny ve vlastních uzavřených prostorách scryp ve Vídni. Vstup mají pouze oprávněné osoby; přístup je mechanicky uzamčen a navíc biometricky zabezpečen.
- Všechny datové nosiče těchto serverů jsou plně šifrovány. Při krádeži nebo vyjmutí datového nosiče zůstávají údaje bez klíče nečitelné. Nezašifrovaný obsah se na těchto serverech nachází pouze během probíhající úlohy v operační paměti a nikdy se nezapisuje na datový nosič.

3. Kontrola přístupu a oprávnění

- Přístup k serverům mají pouze administrátoři scryp prostřednictvím šifrovaných spojení SSH s osobními klíči, respektive náhodně generovanými silnými hesly; přístup podle zásady nejnižších oprávnění.
- Oddělené administrační rozhraní s vlastním přihlášením, omezené na schválené IP adresy. Administrační rozhraní zobrazuje pouze metadata účtů a úloh, nikoli obsah.
- Uživatelské účty: hesla se hashují pomocí Argon2id; ochrana před pokusy o přihlášení omezením počtu požadavků a dočasným zablokováním; relace běží bez souborů cookie s krátkodobými tokeny.
- Ochrana rozhraní před zneužitím a přetížením omezením počtu požadavků a automatickým blokováním.
- Automatizované služby (zpracovatelské servery) se ověřují vlastními, obměnitelnými přístupovými údaji a získávají pouze klíče potřebné pro příslušnou úlohu.

4. Kontrola oddělení a pseudonymizace

- Kryptografické oddělení: každý zákazník má vlastní hlavní klíč, každý soubor vlastní klíč souboru. Obsah jednoho zákazníka nelze číst cizími klíči.
- Logické oddělení produkčních, databázových, cache a monitorovacích systémů v oddělených síťových zónách.
- Úlohy zpracování zadávané GPU serverům neobsahují žádná jména ani e-mailové adresy, pouze technické údaje potřebné pro úlohu.

5. Integrita a sledovatelnost

- Všechny změny aplikace a infrastruktury probíhají prostřednictvím verzovaného zdrojového kódu a automatizovaného, sledovatelného nasazování; softwarové obrazy jsou určeny svým kontrolním součtem.
- Události účtu (například přihlášení, výmaz, změny předplatného) se protokolují s časovým údajem, bez IP adres.
- Systémové protokoly neobsahují žádný obsah a mažou se po 14 dnech. IP adresy se neukládají ani neprotokolují. Pro obranu před zneužitím se přístupy počítají pouze pomocí krátkodobého pseudonymu vytvořeného s tajným klíčem, který nelze zpětně odvodit a který zaniká nejpozději po jedné hodině.

6. Dostupnost a odolnost

- Vysoce dostupný cluster tří serverů s rozložením zátěže; databáze se synchronní replikací na tři uzly; cache s automatickým failoverem.
- Denní šifrovaná záloha databáze s možností obnovení k libovolnému okamžiku posledních 30 dnů; konfigurace clusteru zálohována každých šest hodin. Zálohy jsou uloženy v datovém centru v Norimberku.
- Nasazování nových verzí bez přerušení provozu; ochrana před útoky přetížením na síťové i aplikační úrovni.
- Průběžný monitoring s automatickým upozorněním při poruchách.

7. Výmaz a minimalizace údajů

- Nahrané původní soubory se po zpracování mažou, zpravidla během několika minut; automatické pravidlo odstraňuje nedokončená nahrání nejpozději po 72 hodinách.
- Zákazník kdykoli sám maže obsah i účet; výmaz se v aktivních datech projeví okamžitě. Po skončení předplatného se obsah po 90 dnech automaticky vymaže.
- Žádné soubory cookie, žádné sledovací ani analytické nástroje třetích stran, žádné ukládání IP adres.

8. Organizace

- Všechny osoby činné pro scryp jsou zavázány k zachování datového tajemství a mlčenlivosti a jsou seznámeny s bezpečnostní architekturou.
- scryp vede záznamy o činnostech zpracování (čl. 30 GDPR). Posouzení vlivu na ochranu osobních údajů, záznamy a tato opatření se přezkoumávají nejméně jednou ročně a při podstatných změnách.
- Proces řešení incidentů: detekce prostřednictvím monitoringu, vyhodnocení, zamezení šíření, ohlášení dotčeným zákazníkům podle bodu 10 smlouvy, následné vyhodnocení.
- Další zpracovatelé jsou před nasazením prověřeni z hlediska svých záruk a smluvně zavázáni podle čl. 28 odst. 4 GDPR.

Příloha 3: Další zpracovatelé

Stav ke dni 22. září 2026.

Další zpracovatel	Služba	Údaje	Místo zpracování	Záruka
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Německo	Provoz serverů pro webovou aplikaci, rozhraní a databázi; zašifrované objektové úložiště; záložní kopie	Všechny údaje uvedené v příloze 1, obsah výhradně v zašifrované podobě	Norimberk, Německo (EU)	Smlouva o zpracování osobních údajů; ISO/IEC 27001; BSI C5
Mailjet GmbH (Sinch- Konzern), Alt Moabit 2, 10557 Berlin, Německo	Odesílání systémových e-mailů (například oznámení „Přepis dokončen“)	E-mailová adresa účtu, datum úlohy, odkaz na účet; žádný obsah, žádné názvy souborů	Francie (EU)	Smlouva o zpracování osobních údajů; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, Irsko	Příjem a vyřizování požadavků na podporu e-mailem (Microsoft 365)	Pouze údaje, které zákazník sám uvede v požadavku na podporu	EU; možný vzdálený přístup ze třetích zemí	Smlouva o zpracování osobních údajů; standardní smluvní doložky EU; rámec EU- USA pro ochranu osobních údajů (DPF)