Umowa powierzenia przetwarzania danych (DPA)

zgodnie z art. 28 ogólnego rozporządzenia o ochronie danych (RODO)

Version 1.0, stan na dzień 22 września 2026 r.

Strony

Klient (administrator w rozumieniu art. 4 pkt 7 RODO):

Firma / imię i nazwisko: _____

Adres: _____

Adres e-mail konta scryp: _____

scryp (podmiot przetwarzający w rozumieniu art. 4 pkt 8 RODO):

Gökhan Sagir, przedsiębiorca jednoosobowy, działający pod marką scryp
Erdbergstraße 121/9, 1030 Wiedeń, Austria
UID: ATU83108129
Kontakt w sprawach ochrony danych: datenschutz@scryp.at

Zwani dalej „Klientem” i „scryp”, łącznie „Stronami”.

Czego dotyczy niniejsza umowa

Klient korzysta ze scryp, aby zlecać transkrypcję i analizę nagrań audio i wideo. W nagraniach tych wypowiadają się osoby, za których dane osobowe odpowiada Klient. scryp przetwarza te dane wyłącznie w imieniu Klienta. Niniejsza umowa określa, co scryp może robić z tymi danymi, jak scryp je chroni i co ostatecznie się z nimi dzieje.

1. Przedmiot i zakres obowiązywania

1.1 Niniejsza umowa ma zastosowanie do wszystkich danych osobowych, które scryp przetwarza w imieniu Klienta przy świadczeniu usługi scryp zgodnie z Warunkami świadczenia usług (dostępnymi pod adresem www.scryp.at/agb). Umowa o korzystanie z usługi jest dalej zwana „Umową główną”. Aktualna wersja niniejszej umowy jest dostępna pod adresem www.scryp.at/avv.

1.2 Niniejsza umowa nie obejmuje danych samego stosunku umownego, tj. danych Klienta dotyczących konta, umowy, rozliczeń i obsługi klienta. Dane te scryp przetwarza jako samodzielny administrator zgodnie ze swoją Polityką prywatności (www.scryp.at/datenschutz).

1.3 Załączniki 1-3 stanowią integralną część niniejszej umowy. W razie sprzeczności między niniejszą umową a Umową główną w kwestiach ochrony danych pierwszeństwo ma niniejsza umowa.

1.4 Niniejsza umowa jest przeznaczona dla Klientów, którzy korzystają ze scryp w ramach działalności zawodowej, gospodarczej lub urzędowej. W przypadku korzystania wyłącznie do celów prywatnych RODO nie ma zastosowania zgodnie z art. 2 ust. 2 lit. c i umowa powierzenia przetwarzania danych nie jest wymagana.

2. Charakter, cel i zakres przetwarzania

2.1 Charakter i cel przetwarzania, rodzaje danych oraz kategorie osób, których dane dotyczą, opisano w Załączniku 1.

2.2 scryp przetwarza dane wyłącznie w państwach członkowskich Unii Europejskiej. Miejsca przetwarzania wskazano w Załączniku 1 i Załączniku 3.

2.3 Czas trwania przetwarzania odpowiada okresowi obowiązywania Umowy głównej, powiększonemu o terminy usunięcia danych określone w pkt 12.

3. Polecenia

3.1 scryp przetwarza dane wyłącznie na udokumentowane polecenie Klienta. Poleceniami Klienta są Umowa główna, niniejsza umowa oraz korzystanie przez Klienta z funkcji usługi (w szczególności przesyłanie, transkrypcja, analiza, edycja, udostępnianie, eksport i usuwanie). Każde użycie funkcji stanowi udokumentowane polecenie jednostkowe wykonania związanego z nią przetwarzania.

3.2 Dalsze polecenia Klient wydaje w formie pisemnej; wystarczy wiadomość e-mail na adres datenschutz@scryp.at. Do wydawania poleceń uprawnieni są właściciel konta oraz osoby, którym Klient powierza obsługę swojego konta scryp. Polecenia wykraczające poza zakres usługi uważa się za wniosek o zmianę zakresu świadczenia.

3.3 Jeżeli w ocenie scryp polecenie narusza RODO lub inne przepisy o ochronie danych, scryp niezwłocznie informuje o tym Klienta. scryp może wstrzymać wykonanie polecenia do czasu jego potwierdzenia lub zmiany przez Klienta.

3.4 scryp nie wykorzystuje danych do własnych celów. W szczególności nagrania, transkrypcje i analizy Klienta nie są wykorzystywane do trenowania ani ulepszania modeli AI i nie są przekazywane osobom trzecim, o ile niniejsza umowa nie stanowi inaczej.

3.5 Jeżeli organ lub sąd zażąda od scryp wydania danych Klienta, scryp niezwłocznie informuje o tym Klienta, o ile jest to prawnie dopuszczalne, odsyła ten organ do Klienta i wydaje wyłącznie to, do czego scryp jest ustawowo zobowiązany. scryp sprawdza przy tym, czy wydaniu danych nie sprzeciwia się ustawowy obowiązek zachowania tajemnicy ciążący na Kliencie (§ 6 ust. 5 DSG).

4. Obowiązki Klienta

4.1 Klient odpowiada za zgodność z prawem nagrań i ich przetwarzania. W szczególności zapewnia podstawę prawną (art. 6, a w przypadku szczególnych kategorii danych art. 9 RODO), poinformowanie osób, których dane dotyczą (art. 13 i 14 RODO), oraz to, aby żadne niepubliczne wypowiedzi nie były nagrywane bez zgody osób wypowiadających się (na przykład § 120 StGB w Austrii).

4.2 Jeżeli nagrania zawierają szczególne kategorie danych osobowych (na przykład dane dotyczące zdrowia) lub treści objęte tajemnicą zawodową, Klient sprawdza uprzednio, czy przetwarzanie jest dopuszczalne i czy wymagana jest ocena skutków dla ochrony danych (art. 35 RODO). scryp udostępnia w tym celu informacje zawarte w niniejszej umowie i jej załącznikach.

4.3 Klient utrzymuje aktualny adres e-mail swojego konta scryp. Na ten adres scryp kieruje wszystkie zawiadomienia wynikające z niniejszej umowy, w szczególności zgłoszenia zgodnie z pkt 10.

4.4 Klient ma prawo wydawać scryp polecenia, żądać dowodów oraz przeprowadzać audyty zgodnie z pkt 11.

5. Poufność i tajemnica zawodowa

5.1 scryp zezwala na dostęp do danych wyłącznie osobom zobowiązanym do zachowania tajemnicy danych (§ 6 DSG) i poufności oraz pouczonym o skutkach naruszenia (art. 28 ust. 3 lit. b, art. 29 RODO). Zobowiązanie to trwa również po zakończeniu wykonywania czynności.

5.2 scryp jest zaprojektowany tak, aby treści Klienta (nagrania, transkrypcje, analizy, nazwy plików i folderów) były przechowywane wyłącznie w postaci zaszyfrowanej, a w postaci jawnej występowały jedynie przez czas danego przetwarzania w pamięci operacyjnej serwerów przetwarzających. Osoby pracujące w scryp nie mają w toku bieżącej działalności dostępu do treści w postaci jawnej. Szczegóły zawiera Załącznik 2.

5.3 Jeżeli Klient podlega ustawowemu obowiązkowi zachowania tajemnicy (na przykład § 9 RAO, § 54 ÄrzteG, § 121 StGB), scryp jako osoba pomocnicza Klienta zobowiązuje się zachować w tajemnicy w taki sam sposób wszystkie treści, do których scryp uzyskuje dostęp w ramach świadczenia usługi. W przypadku Klientów podlegających prawu niemieckiemu stanowi to jednocześnie zobowiązanie do zachowania tajemnicy zgodnie z § 203 ust. 4 StGB (Niemcy). Na życzenie scryp potwierdza to zobowiązanie w odrębnym oświadczeniu.

6. Bezpieczeństwo przetwarzania

6.1 scryp stosuje środki techniczne i organizacyjne zgodnie z art. 32 RODO, opisane w Załączniku 2.

6.2 scryp może rozwijać te środki i zastępować je środkami równoważnymi lub lepszymi. Poziom ochrony nie może przy tym ulec obniżeniu. Istotne zmiany scryp dokumentuje i przekazuje Klientowi. Aktualna wersja Załącznika 2 jest dostępna pod adresem www.scryp.at/avv.

6.3 scryp weryfikuje skuteczność środków co najmniej raz w roku i na żądanie informuje Klienta o wyniku.

7. Dalsze podmioty przetwarzające

7.1 Klient zatwierdza dalsze podmioty przetwarzające wymienione w Załączniku 3 (ogólna zgoda zgodnie z art. 28 ust. 2 RODO).

7.2 Jeżeli scryp zamierza dodać lub zastąpić dalszy podmiot przetwarzający, informuje o tym Klienta co najmniej 30 dni przed rozpoczęciem korzystania z jego usług wiadomością e-mail na adres konta scryp. Klient może w terminie 14 dni od otrzymania tego zawiadomienia wnieść pisemny sprzeciw z ważnej przyczyny związanej z ochroną danych; wystarczy wiadomość e-mail. Jeżeli Klient nie wniesie sprzeciwu, zmianę uważa się za zatwierdzoną.

7.3 Jeżeli po wniesieniu sprzeciwu Strony nie znajdą rozwiązania, Klient może wypowiedzieć Umowę główną ze skutkiem na dzień planowanego rozpoczęcia korzystania z usług tego podmiotu. Opłaty, które Klient uiścił z góry za okres po zakończeniu umowy, scryp zwraca proporcjonalnie.

7.4 scryp nakłada w drodze umowy na każdy dalszy podmiot przetwarzający te same obowiązki w zakresie ochrony danych, które ciążą na scryp na mocy niniejszej umowy, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych (art. 28 ust. 4 RODO). Jeżeli dalszy podmiot przetwarzający nie wywiązuje się ze swoich obowiązków, scryp odpowiada wobec Klienta za jego obowiązki jak za własne działania.

7.5 Usługi dodatkowe bez dostępu do danych Klienta, na przykład telekomunikacja, sprzątanie lub konserwacja bez dostępu do danych, nie stanowią podpowierzenia przetwarzania danych.

8. Miejsce przetwarzania i państwa trzecie

8.1 scryp przetwarza i przechowuje dane w Austrii i w Niemczech. scryp nie przekazuje danych do państw spoza Unii Europejskiej lub Europejskiego Obszaru Gospodarczego.

8.2 Jeżeli dalszy podmiot przetwarzający miałby przetwarzać dane w państwie trzecim, odbywa się to wyłącznie w zakresie opisanym w Załączniku 3 i wyłącznie na podstawie odpowiedniej gwarancji zgodnie z rozdziałem V RODO (na przykład decyzji Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony lub standardowych klauzul umownych UE).

9. Wsparcie Klienta

9.1 Prawa osób, których dane dotyczą: Klient może w większości przypadków samodzielnie realizować prawo dostępu, sprostowania, usunięcia i przenoszenia danych za pomocą funkcji usługi (wyświetlanie, edycja, eksport, usuwanie). Ponieważ scryp przechowuje treści wyłącznie w postaci zaszyfrowanej, scryp nie może ustalić, jakie osoby występują w nagraniu. Jeżeli osoba, której dane dotyczą, zwróci się do scryp, scryp niezwłocznie przekazuje jej żądanie Klientowi i nie odpowiada na nie samodzielnie, chyba że Klient wyda scryp takie polecenie.

9.2 Bezpieczeństwo, naruszenia ochrony danych, ocena skutków dla ochrony danych i uprzednie konsultacje z organem nadzorczym (art. 32-36 RODO): scryp wspiera Klienta informacjami, którymi scryp dysponuje, w szczególności niniejszą umową, Załącznikiem 2 oraz informacjami o incydencie zgodnie z pkt 10.

9.3 Za wsparcie wykraczające poza udostępnienie informacji i funkcji opisanych w niniejszej umowie scryp może, po uprzednim zapowiedzeniu, żądać stosownego wynagrodzenia według nakładu pracy. Nie dotyczy to sytuacji, w której wsparcie jest konieczne z powodu błędu scryp.

10. Zgłaszanie naruszeń ochrony danych osobowych

10.1 Jeżeli scryp poweźmie wiadomość o naruszeniu ochrony danych osobowych dotyczącym danych Klienta, scryp zgłasza je Klientowi bez zbędnej zwłoki, najpóźniej w ciągu 48 godzin od powzięcia wiadomości, wiadomością e-mail na adres konta scryp.

10.2 Zgłoszenie zawiera, w zakresie znanym scryp: charakter naruszenia, rodzaje danych, których dotyczy, i przybliżoną liczbę osób, których dane dotyczą, prawdopodobne konsekwencje, podjęte i proponowane środki oraz punkt kontaktowy w scryp. Informacje, które nie są jeszcze dostępne, scryp przekazuje sukcesywnie bez zbędnej zwłoki.

10.3 scryp dokumentuje naruszenie i wspiera Klienta przy zgłoszeniu do organu nadzorczego oraz zawiadomieniu osób, których dane dotyczą. Zgłoszeń do organów lub zawiadomień osób, których dane dotyczą, w imieniu Klienta scryp dokonuje wyłącznie na jego polecenie. Zgłoszenie do Klienta nie stanowi przyznania się do winy.

11. Dowody i audyty

11.1 scryp udostępnia Klientowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 RODO. Należą do nich niniejsza umowa, opis środków w Załączniku 2, rejestr, o którym mowa w art. 30 ust. 2 RODO, certyfikaty dalszych podmiotów przetwarzających oraz pisemne odpowiedzi na uzasadnione pytania Klienta.

11.2 Jeżeli dowody te w konkretnym przypadku nie są wystarczające, Klient może przeprowadzić audyt, w tym inspekcję, samodzielnie lub przez zobowiązanego do zachowania poufności audytora, który nie jest konkurentem scryp. Audyty odbywają się najwyżej raz w roku kalendarzowym, po zapowiedzeniu z wyprzedzeniem co najmniej 30 dni, w zwykłych godzinach pracy i bez zakłócania działalności. W przypadku konkretnych przesłanek wskazujących na naruszenie lub na żądanie organu nadzorczego audyt jest możliwy również w krótszym terminie i częściej.

11.3 Audyt nie obejmuje danych innych klientów ani centrów danych dalszych podmiotów przetwarzających. W ich przypadku obowiązują ich certyfikaty i sprawozdania z audytów. Każda ze Stron ponosi własne koszty audytu.

12. Usunięcie i zwrot danych

12.1 W okresie obowiązywania umowy Klient może w każdej chwili samodzielnie usuwać swoje dane i eksportować je w powszechnie stosowanych formatach. Usunięte treści są natychmiast usuwane z aktywnego zbioru danych.

12.2 Przesłane pliki oryginalne scryp usuwa automatycznie po zakończeniu przetwarzania, z reguły w ciągu kilku minut, najpóźniej jednak 72 godziny po przesłaniu. Przechowywane pozostają wyłącznie zaszyfrowana wersja do odtwarzania, zaszyfrowana transkrypcja i zaszyfrowane analizy.

12.3 Po zakończeniu Umowy głównej treści pozostają dostępne dla Klienta do eksportu jeszcze przez maksymalnie 90 dni. Następnie scryp usuwa je automatycznie wraz ze wszystkimi kopiami. Jeżeli Klient usunie swoje konto, wszystkie dane są usuwane natychmiast.

12.4 Kopie zapasowe służą wyłącznie odtworzeniu całego systemu. Zawierają treści Klienta wyłącznie w postaci zaszyfrowanej i są nadpisywane najpóźniej po 30 dniach. Pojedyncze usunięte dane Klienta nie są odtwarzane z kopii zapasowych.

12.5 Dane, które scryp musi nadal przechowywać ze względu na ustawowe obowiązki przechowywania (na przykład dane do faktur zgodnie z § 132 BAO), są wyłączone z usunięcia. Są one blokowane i usuwane po upływie terminu.

12.6 Na żądanie scryp potwierdza usunięcie na piśmie; wystarczy wiadomość e-mail.

13. Odpowiedzialność

13.1 Wobec osób, których dane dotyczą, Strony odpowiadają zgodnie z art. 82 RODO.

13.2 W stosunkach między Stronami obowiązują, w zakresie dozwolonym przez prawo, postanowienia Umowy głównej dotyczące odpowiedzialności. Za dalsze podmioty przetwarzające scryp odpowiada jak za własne działania (pkt 7.4).

13.3 Jeżeli jedna ze Stron zapłaciła odszkodowanie osobom, których dane dotyczą, może żądać od drugiej Strony zwrotu tej części odszkodowania, która odpowiada jej udziałowi w odpowiedzialności za szkodę (art. 82 ust. 5 RODO).

13.4 Jeżeli Klient podtrzymuje polecenie, mimo że scryp wskazał mu zgodnie z pkt 3.3 na jego niezgodność z prawem, Klient zwalnia scryp z odpowiedzialności z tytułu wszelkich roszczeń osób trzecich i administracyjnych kar pieniężnych wynikających z tego polecenia.

14. Okres obowiązywania, zawieszenie i zakończenie

14.1 Niniejsza umowa obowiązuje tak długo, jak scryp przetwarza dane dla Klienta, tj. przez okres obowiązywania Umowy głównej oraz do zakończenia usunięcia danych zgodnie z pkt 12.

14.2 Korzystanie z usługi bez niniejszej umowy nie jest przewidziane dla Klientów w rozumieniu pkt 1.4. Wypowiedzenie niniejszej umowy uważa się zatem jednocześnie za wypowiedzenie Umowy głównej.

14.3 Jeżeli scryp narusza niniejszą umowę, Klient może żądać, aby scryp zawiesił dane przetwarzanie do czasu usunięcia naruszenia. Jeżeli scryp nie usunie istotnego naruszenia w ciągu miesiąca od wezwania, Klient może wypowiedzieć Umowę główną ze skutkiem natychmiastowym.

15. Postanowienia końcowe

15.1 Niniejsza umowa jest zawierana w formie elektronicznej (art. 28 ust. 9 RODO). W przypadku Klientów w rozumieniu pkt 1.4 staje się ona częścią umowy poprzez włączenie do Warunków świadczenia usług z chwilą zawarcia Umowy głównej; stroną umowy jest wówczas właściciel konta scryp z danymi zapisanymi na tym koncie. Ponadto może ona zostać zawarta przez podpisanie niniejszego dokumentu przez obie Strony, również w formie kopii elektronicznej.

15.2 Zmiany niniejszej umowy wymagają formy pisemnej; wystarczy wiadomość e-mail. scryp może dostosowywać Załącznik 2 zgodnie z pkt 6.2 oraz Załącznik 3 zgodnie z pkt 7.2. Inne zmiany scryp zapowiada wiadomością e-mail co najmniej 30 dni przed ich wejściem w życie; do tego czasu Klient może wnieść sprzeciw i wypowiedzieć Umowę główną ze skutkiem na ten dzień. scryp przechowuje każdą wersję niniejszej umowy z numerem wersji i datą.

15.3 Zastosowanie ma prawo austriackie; RODO pozostaje nienaruszone. Jeżeli Klient jest przedsiębiorcą, wszystkie spory wynikające z niniejszej umowy podlegają wyłącznej właściwości sądu rzeczowo właściwego w Wiedniu. Bezwzględnie obowiązujące ustawowe przepisy o właściwości sądu pozostają nienaruszone.

15.4 Jeżeli którekolwiek postanowienie okaże się nieważne, pozostała część umowy pozostaje w mocy. W miejsce nieważnego postanowienia wchodzi regulacja ustawowa najbliższa jego celowi.

15.5 Osobą kontaktową we wszystkich sprawach dotyczących niniejszej umowy jest po stronie scryp datenschutz@scryp.at. Po stronie Klienta jest to adres e-mail konta scryp, o ile Klient nie wskaże inaczej.

15.6 scryp udostępnia niniejszą umowę w kilku językach. Wiążąca jest wersja niemiecka; tłumaczenia służą zrozumieniu. W razie rozbieżności obowiązuje brzmienie niemieckie.

Podpisy

Za Klienta	**Za scryp**
Miejscowość, data	Miejscowość, data
Imię i nazwisko, funkcja	Gökhan Sagir, przedsiębiorca jednoosobowy
Podpis	Podpis

Załącznik 1: Opis przetwarzania

Punkt	Opis
Przedmiot	Świadczenie usługi scryp: transkrypcja nagrań audio i wideo z rozpoznawaniem mowy i rozpoznawaniem mówców, w planie Ultra dodatkowo funkcje AI (analiza wspomagana przez sztuczną inteligencję: podsumowanie, protokół, lista zadań, tekst do mediów społecznościowych), a także przechowywanie, edycja, eksport i udostępnianie wyników.
Cel	Klient zleca przekształcanie własnych nagrań w tekst i ich analizę, na przykład spotkań, wywiadów, dyktand, rozmów doradczych, wykładów lub podcastów.
Charakter przetwarzania	Przyjmowanie zaszyfrowanych plików, krótkotrwałe odszyfrowanie w pamięci operacyjnej serwerów przetwarzających, automatyczna transkrypcja i analiza, szyfrowanie wyników, zaszyfrowane przechowywanie, udostępnienie na koncie Klienta, usunięcie.
Rodzaje danych	Nagrania głosu i wideo (głos, wypowiadane treści), wygenerowane z nich transkrypcje i analizy, przypisania mówców, nadane przez Klienta nazwy plików i folderów, techniczne metadane (czas trwania, rozmiar pliku, znaczniki czasu, rozpoznany język, status przetwarzania), w przypadku udostępnionych transkrypcji link udostępniania. Wszystkie treści są przechowywane w postaci zaszyfrowanej; jedynie techniczne metadane występują w postaci jawnej.
Szczególne kategorie (art. 9 RODO)	Możliwe, w zależności od treści nagrań Klienta (na przykład dane dotyczące zdrowia w dyktandach lekarskich, informacje z rozmów doradczych lub rozmów z klientami kancelarii). scryp nie zna treści. Dopuszczalność sprawdza Klient zgodnie z pkt 4.2.
Gwarancje dla szczególnych kategorii	Szyfrowanie w przeglądarce Klienta, postać jawna wyłącznie w pamięci operacyjnej własnych serwerów scryp w Wiedniu, brak przekazywania treści dalszym podmiotom przetwarzającym w postaci jawnej, brak dostępu osób do treści w toku bieżącej działalności, obowiązek zachowania tajemnicy zgodnie z pkt 5, brak trenowania modeli AI danymi Klientów.
Osoby, których dane dotyczą	Osoby, które wypowiadają się w nagraniach lub są w nich wymieniane (na przykład pracownicy, klienci, pacjenci, mocodawcy, rozmówcy, uczestnicy spotkań i wydarzeń), a także użytkownicy konta Klienta.
Miejsca przetwarzania	Transkrypcja i analiza AI: własne serwery GPU scryp w Wiedniu, Austria. Aplikacja internetowa, interfejsy, baza danych, zaszyfrowana pamięć plików i kopie zapasowe: centrum danych Hetzner Online GmbH w Norymberdze, Niemcy.
Czas trwania	Okres obowiązywania Umowy głównej powiększony o terminy usunięcia danych zgodnie z pkt 12.

Załącznik 2: Środki techniczne i organizacyjne (art. 32 RODO)

Stan na dzień 22 września 2026 r. Środki opisują normalny tryb działania scryp.

1. Szyfrowanie i architektura zero-knowledge

- Nagrania są szyfrowane algorytmem AES-256-GCM już w przeglądarce Klienta, zanim zostaną przesłane do scryp. Dla każdego pliku generowany jest odrębny klucz pliku (FEK).
- Klucze plików są szyfrowane kluczem głównym konta (MEK). Klucz główny jest dostępny wyłącznie przy użyciu hasła Klienta (wyprowadzanie za pomocą PBKDF2-SHA256, 600 000 iteracji). scryp nie zna ani hasła, ani klucza głównego w postaci jawnej.
- Na potrzeby transkrypcji przeglądarka przekazuje do scryp klucz pliku zaszyfrowany kluczem serwera (RSA-4096, OAEP). Serwer przetwarzający odszyfrowuje nagranie wyłącznie w pamięci operacyjnej. Pliki tymczasowe znajdują się w systemie plików w pamięci RAM i są odrzucane po zakończeniu zlecenia; niezaszyfrowane treści nie są w żadnym momencie zapisywane na nośnikach danych.
- Transkrypcje i analizy są szyfrowane kluczem pliku bezpośrednio po utworzeniu i przechowywane wyłącznie w postaci zaszyfrowanej. Nazwy plików i folderów są szyfrowane w przeglądarce.
- Przy udostępnianiu transkrypcji klucz pliku jest szyfrowany kluczem wyprowadzonym z hasła udostępniania. Odbiorcy odszyfrowują dane wyłącznie we własnej przeglądarce.
- Wyjątek dotyczący przesyłania z adresu URL: jeżeli Klient pobiera nagranie z adresu internetowego, serwer przetwarzający pobiera plik bezpośrednio, przetwarza go w pamięci operacyjnej, a następnie usuwa; transkrypcja i wersja do odtwarzania są jak zwykle przechowywane w postaci zaszyfrowanej.
- Wszystkie połączenia są szyfrowane protokołem TLS 1.2 lub 1.3.

2. Kontrola dostępu fizycznego

- Aplikacja internetowa, baza danych, pamięć plików i kopie zapasowe działają w centrum danych Hetzner Online GmbH w Norymberdze (certyfikat ISO/IEC 27001, atest BSI C5 typu 2) z kontrolą dostępu fizycznego, monitoringiem wideo i personelem ochrony operatora.
- Serwery GPU do transkrypcji i analizy AI znajdują się we własnych, zamkniętych pomieszczeniach scryp w Wiedniu. Dostęp mają wyłącznie osoby upoważnione; wejście jest zamykane mechanicznie i dodatkowo zabezpieczone biometrycznie.
- Wszystkie nośniki danych tych serwerów są w całości zaszyfrowane. W przypadku kradzieży lub wymontowania nośnika dane pozostają bez klucza nieczytelne. Niezaszyfrowane treści występują na tych serwerach wyłącznie w pamięci operacyjnej podczas realizowanego zlecenia i nigdy nie są zapisywane na nośniku danych.

3. Kontrola dostępu do systemów i danych

- Dostęp do serwerów wyłącznie dla administratorów scryp przez szyfrowane połączenia SSH z osobistymi kluczami lub losowo generowanymi, silnymi hasłami; dostęp zgodnie z zasadą najmniejszych uprawnień.
- Odrębny panel administracyjny z własnym logowaniem, ograniczony do dopuszczonych adresów IP. Panel administracyjny wyświetla wyłącznie metadane kont i zleceń, nie treści.
- Konta użytkowników: hasła są hashowane algorytmem Argon2id; ochrona przed próbami logowania przez ograniczanie liczby żądań i czasową blokadę; sesje działają bez plików cookie, z krótkotrwałymi tokenami.
- Ochrona interfejsów przed nadużyciami i przeciążeniem przez ograniczanie liczby żądań i automatyczne blokady.
- Usługi zautomatyzowane (serwery przetwarzające) uwierzytelniają się własnymi, rotowanymi danymi dostępowymi i otrzymują wyłącznie klucze niezbędne do danego zlecenia.

4. Kontrola rozdzielności i pseudonimizacja

- Rozdzielność kryptograficzna: każdy Klient ma własny klucz główny, każdy plik własny klucz pliku. Treści jednego Klienta nie są czytelne przy użyciu cudzych kluczy.
- Logiczne oddzielenie systemów produkcyjnych, bazodanowych, pamięci podręcznej i monitoringu w odrębnych strefach sieciowych.
- Zlecenia przetwarzania kierowane do serwerów GPU nie zawierają nazwisk ani adresów e-mail, a jedynie dane techniczne niezbędne do zlecenia.

5. Integralność i rozliczalność

- Wszystkie zmiany w aplikacji i infrastrukturze są dokonywane za pośrednictwem wersjonowanego kodu źródłowego i zautomatyzowanego, możliwego do prześledzenia wdrażania; obrazy oprogramowania są identyfikowane przez ich sumę kontrolną.
- Zdarzenia dotyczące konta (na przykład logowanie, usunięcie, zmiany subskrypcji) są rejestrowane ze znacznikiem czasu, bez adresów IP.
- Dzienniki systemowe nie zawierają treści i są usuwane po 14 dniach. Adresy IP nie są przechowywane ani rejestrowane. W celu ochrony przed nadużyciami dostępy są zliczane wyłącznie na podstawie krótkotrwałego, utworzonego przy użyciu tajnego klucza i nieodwracalnego pseudonimu, który wygasa najpóźniej po upływie godziny.

6. Dostępność i odporność

- Klaster wysokiej dostępności złożony z trzech serwerów z równoważeniem obciążenia; baza danych z replikacją synchroniczną na trzech węzłach; pamięć podręczna z automatycznym przełączaniem awaryjnym.
- Codzienna zaszyfrowana kopia zapasowa bazy danych z możliwością odtworzenia stanu z dowolnego momentu ostatnich 30 dni; konfiguracja klastra zabezpieczana co sześć godzin. Kopie zapasowe znajdują się w centrum danych w Norymberdze.
- Wdrażanie nowych wersji bez przerw w działaniu; ochrona przed atakami przeciążeniowymi na poziomie sieci i aplikacji.
- Ciągły monitoring z automatycznym alarmowaniem w przypadku zakłóceń.

7. Usuwanie i minimalizacja danych

- Przesłane pliki oryginalne są usuwane po przetworzeniu, z reguły w ciągu kilku minut; automatyczna reguła usuwa pozostałe przesłane pliki najpóźniej po 72 godzinach.
- Klient w każdej chwili samodzielnie usuwa treści i konto; usunięcie działa natychmiast w aktywnym zbiorze danych. Po zakończeniu subskrypcji treści są automatycznie usuwane po 90 dniach.
- Brak plików cookie, brak narzędzi śledzących lub analitycznych podmiotów trzecich, brak przechowywania adresów IP.

8. Organizacja

- Wszystkie osoby pracujące w scryp są zobowiązane do zachowania tajemnicy danych i poufności oraz przeszkolone w zakresie architektury bezpieczeństwa.
- scryp prowadzi rejestr czynności przetwarzania (art. 30 RODO). Ocena skutków dla ochrony danych, rejestr i niniejsze środki są weryfikowane co najmniej raz w roku oraz przy istotnych zmianach.
- Proces reagowania na incydenty: wykrywanie przez monitoring, ocena, ograniczanie skutków, zgłoszenie dotkniętym Klientom zgodnie z pkt 10 umowy, działania następcze.

- Dalsze podmioty przetwarzające są przed rozpoczęciem korzystania z ich usług weryfikowane pod kątem gwarancji i zobowiązywane umownie zgodnie z art. 28 ust. 4 RODO.

Załącznik 3: Dalsze podmioty przetwarzające

Stan na dzień 22 września 2026 r.

Dalszy podmiot przetwarzający	Usługa	Dane	Miejsce przetwarzania	Gwarancja
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Niemcy	Eksploatacja serwerów aplikacji internetowej, interfejsów i bazy danych; zaszyfrowana pamięć obiektowa; kopie zapasowe	Wszystkie dane wymienione w Załączniku 1, treści wyłącznie w postaci zaszyfrowanej	Norymberga, Niemcy (UE)	Umowa powierzenia przetwarzania danych; ISO/IEC 27001; BSI C5
Mailjet GmbH (Sinch-Konzern), Alt Moabit 2, 10557 Berlin, Niemcy	Wysyłka systemowych wiadomości e-mail (na przykład powiadomienie „Transkrypcja gotowa”)	Adres e-mail konta, data zlecenia, link do konta; bez treści, bez nazw plików	Francja (UE)	Umowa powierzenia przetwarzania danych; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, Irlandia	Przyjmowanie i obsługa zgłoszeń do pomocy technicznej przesyłanych pocztą elektroniczną (Microsoft 365)	Wyłącznie dane, które Klient sam przekazuje w zgłoszeniu	UE; możliwy zdalny dostęp z państw trzecich	Umowa powierzenia przetwarzania danych; standardowe klauzule umowne UE; Ramy Ochrony Danych UE-USA (DPF)