Accordo sul trattamento dei dati (DPA)

ai sensi dell'art. 28 del Regolamento generale sulla protezione dei dati (GDPR)

Version 1.0, aggiornata al 22 settembre 2026

Parti

Cliente (titolare del trattamento ai sensi dell'art. 4, punto 7, GDPR):

Ragione sociale / Nome: _____

Indirizzo: _____

E-mail dell'account scryp: _____

scryp (responsabile del trattamento ai sensi dell'art. 4, punto 8, GDPR):

Gökhan Sagir, imprenditore individuale, operante con il marchio scryp
Erdbergstraße 121/9, 1030 Wien, Österreich
UID: ATU83108129
Contatto per la protezione dei dati: datenschutz@scryp.at

Di seguito il «Cliente» e «scryp», congiuntamente le «Parti».

Di cosa si tratta

Il Cliente utilizza scryp per far trascrivere e analizzare registrazioni audio e video. In tali registrazioni parlano persone dei cui dati personali il Cliente è responsabile. scryp tratta tali dati esclusivamente per conto del Cliente. Il presente Accordo stabilisce che cosa scryp può fare con i dati, come scryp li protegge e che cosa ne avviene al termine.

1. Oggetto e ambito di applicazione

1.1 Il presente Accordo si applica a tutti i dati personali che scryp tratta per conto del Cliente nell'erogazione del Servizio scryp in base ai Termini di servizio (disponibili all'indirizzo www.scryp.at/agb). Il contratto relativo all'utilizzo del Servizio è di seguito denominato «Contratto principale». La versione di volta in volta aggiornata del presente Accordo è disponibile all'indirizzo www.scryp.at/avv.

1.2 Non rientrano nell'oggetto del presente Accordo i dati del rapporto contrattuale stesso, ossia i dati relativi all'account, al contratto, alla fatturazione e all'assistenza del Cliente. scryp tratta tali dati in qualità di titolare autonomo del trattamento secondo la propria Informativa sulla privacy (www.scryp.at/datenschutz).

1.3 Gli Allegati da 1 a 3 costituiscono parte integrante del presente Accordo. In caso di contrasto tra il presente Accordo e il Contratto principale, nelle questioni relative alla protezione dei dati prevale il presente Accordo.

1.4 Il presente Accordo è destinato ai clienti che utilizzano scryp nell'ambito di un'attività professionale, commerciale o di un'autorità pubblica. In caso di utilizzo esclusivamente privato, il GDPR non si applica ai sensi dell'art. 2, par. 2, lett. c) e non è necessario alcun accordo sul trattamento dei dati.

2. Natura, finalità e portata del trattamento

2.1 La natura e la finalità del trattamento, i tipi di dati e le categorie di interessati sono descritti nell'Allegato 1.

2.2 scryp tratta i dati esclusivamente negli Stati membri dell'Unione europea. I luoghi del trattamento sono indicati nell'Allegato 1 e nell'Allegato 3.

2.3 La durata del trattamento corrisponde alla durata del Contratto principale, maggiorata dei termini di cancellazione disciplinati al punto 12.

3. Istruzioni

3.1 scryp tratta i dati soltanto su istruzione documentata del Cliente. Le istruzioni del Cliente sono costituite dal Contratto principale, dal presente Accordo e dall'utilizzo delle funzionalità del Servizio da parte del Cliente (in particolare caricamento, trascrizione, analisi, modifica, condivisione, esportazione e cancellazione). Ogni utilizzo di una funzionalità costituisce un'istruzione singola documentata di eseguire il relativo trattamento.

3.2 Il Cliente impartisce ulteriori istruzioni in forma scritta; è sufficiente un'e-mail a datenschutz@scryp.at. Sono autorizzati a impartire istruzioni l'intestatario dell'account e le persone che il Cliente impiega per il proprio account scryp. Le istruzioni che eccedono l'ambito delle prestazioni del Servizio si considerano una richiesta di modifica delle prestazioni.

3.3 Se, a giudizio di scryp, un'istruzione viola il GDPR o altre disposizioni in materia di protezione dei dati, scryp ne informa immediatamente il Cliente. scryp può sospenderne l'esecuzione finché il Cliente non confermi o modifichi l'istruzione.

3.4 scryp non utilizza i dati per finalità proprie. In particolare, le registrazioni, le trascrizioni e le analisi del Cliente non vengono utilizzate per l'addestramento o il miglioramento di modelli di IA e non vengono comunicate a terzi, salvo quanto diversamente previsto dal presente Accordo.

3.5 Se un'autorità o un tribunale richiede a scryp la consegna di dati del Cliente, scryp ne informa immediatamente il Cliente, nella misura in cui ciò sia giuridicamente ammissibile, rinvia l'autorità richiedente al Cliente e consegna soltanto ciò a cui scryp è tenuto per legge. scryp verifica in tale sede se un obbligo di riservatezza previsto dalla legge a carico del Cliente osti alla consegna (§ 6, comma 5, DSG).

4. Obblighi del Cliente

4.1 Il Cliente è responsabile della liceità delle registrazioni e del loro trattamento. In particolare, provvede a una base giuridica (art. 6 e, per le categorie particolari, art. 9 GDPR), all'informazione degli interessati (artt. 13 e 14 GDPR) e a che nessuna dichiarazione non pubblica venga registrata senza il consenso di chi parla (ad esempio § 120 StGB in Austria).

4.2 Se le registrazioni contengono categorie particolari di dati personali (ad esempio dati relativi alla salute) o contenuti soggetti al segreto professionale, il Cliente verifica preventivamente se il trattamento è ammissibile e se è necessaria una valutazione d'impatto sulla protezione dei dati (art. 35 GDPR). A tal fine scryp mette a disposizione le informazioni contenute nel presente Accordo e nei suoi Allegati.

4.3 Il Cliente mantiene aggiornato l'indirizzo e-mail del proprio account scryp. A tale indirizzo scryp invia tutte le comunicazioni previste dal presente Accordo, in particolare le notifiche di cui al punto 10.

4.4 Il Cliente ha il diritto di impartire istruzioni a scryp, di richiedere prove di conformità e di effettuare audit ai sensi del punto 11.

5. Riservatezza e segreto professionale

5.1 scryp consente l'accesso ai dati soltanto a persone vincolate al segreto dei dati (§ 6 DSG) e alla riservatezza e istruite sulle conseguenze di una violazione (art. 28, par. 3, lett. b), e art. 29 GDPR). L'obbligo permane anche dopo la cessazione dell'attività.

5.2 scryp è progettato in modo tale che i contenuti del Cliente (registrazioni, trascrizioni, analisi, nomi di file e di cartelle) vengano archiviati soltanto in forma crittografata e siano presenti in chiaro soltanto per la durata del rispettivo trattamento nella RAM dei server di elaborazione. Nel normale esercizio, le persone che operano presso scryp non hanno accesso ai contenuti in chiaro. I dettagli sono riportati nell'Allegato 2.

5.3 Se il Cliente è soggetto a un obbligo di riservatezza previsto dalla legge (ad esempio § 9 RAO, § 54 ÄrzteG, § 121 StGB), scryp si impegna, in qualità di ausiliario del Cliente, a mantenere segreti allo stesso modo tutti i contenuti a cui scryp ha accesso nell'ambito della prestazione. Per i clienti soggetti al diritto tedesco, ciò vale al contempo come obbligo di segretezza ai sensi del § 203, comma 4, StGB (Germania). Su richiesta, scryp conferma tale obbligo in una dichiarazione separata.

6. Sicurezza del trattamento

6.1 scryp adotta le misure tecniche e organizzative ai sensi dell'art. 32 GDPR descritte nell'Allegato 2.

6.2 scryp può sviluppare ulteriormente tali misure e sostituirle con misure equivalenti o migliori. Il livello di protezione non può essere ridotto. scryp documenta le modifiche sostanziali e le comunica al Cliente. La versione di volta in volta aggiornata dell'Allegato 2 è disponibile all'indirizzo www.scryp.at/avv.

6.3 scryp verifica l'efficacia delle misure almeno una volta all'anno e comunica il risultato al Cliente su richiesta.

7. Sub-responsabili del trattamento

7.1 Il Cliente autorizza i sub-responsabili del trattamento indicati nell'Allegato 3 (autorizzazione generale ai sensi dell'art. 28, par. 2, GDPR).

7.2 Se scryp intende aggiungere o sostituire un sub-responsabile del trattamento, ne informa il Cliente almeno 30 giorni prima dell'impiego tramite e-mail all'indirizzo dell'account scryp. Il Cliente può opporsi per iscritto entro 14 giorni dal ricevimento di tale comunicazione per un motivo grave attinente alla protezione dei dati; è sufficiente un'e-mail. Se il Cliente non si oppone, la modifica si considera autorizzata.

7.3 Se, a seguito di un'opposizione, le Parti non trovano una soluzione, il Cliente può disdire il Contratto principale con effetto alla data dell'impiego previsto. scryp rimborsa proporzionalmente i corrispettivi che il Cliente ha pagato in anticipo per il periodo successivo alla cessazione.

7.4 scryp impone contrattualmente a ciascun sub-responsabile del trattamento gli stessi obblighi in materia di protezione dei dati che incombono a scryp in base al presente Accordo, in particolare garanzie sufficienti per misure tecniche e organizzative adeguate (art. 28, par. 4, GDPR). Se un sub-responsabile del trattamento non adempie ai propri obblighi, scryp risponde nei confronti del Cliente dell'adempimento di tali obblighi come per il proprio operato.

7.5 Le prestazioni accessorie senza accesso ai dati del Cliente, ad esempio telecomunicazioni, pulizia o manutenzione senza accesso ai dati, non costituiscono un ricorso a sub-responsabili del trattamento.

8. Luogo del trattamento e paesi terzi

8.1 scryp tratta e archivia i dati in Austria e in Germania. scryp non effettua alcun trasferimento verso paesi al di fuori dell'Unione europea o dello Spazio economico europeo.

8.2 Qualora un sub-responsabile del trattamento tratti dati in un paese terzo, ciò avviene soltanto nella misura descritta nell'Allegato 3 e soltanto in presenza di una garanzia adeguata ai sensi del capo V del GDPR (ad esempio una decisione di adeguatezza della Commissione europea o le clausole contrattuali standard dell'UE).

9. Assistenza al Cliente

9.1 Diritti degli interessati: nella maggior parte dei casi il Cliente può soddisfare autonomamente le richieste di accesso, rettifica, cancellazione e portabilità dei dati tramite le funzionalità del Servizio (visualizzazione, modifica, esportazione, cancellazione). Poiché scryp conserva i contenuti soltanto in forma crittografata, scryp non è in grado di stabilire quali persone compaiano in una registrazione. Se un interessato si rivolge a scryp, scryp inoltra immediatamente la richiesta al Cliente e non vi risponde direttamente, salvo che il Cliente non gli impartisca un'istruzione in tal senso.

9.2 Sicurezza, violazioni dei dati personali, valutazione d'impatto sulla protezione dei dati e consultazione dell'autorità di controllo (artt. da 32 a 36 GDPR): scryp assiste il Cliente con le informazioni di cui dispone, in particolare con il presente Accordo, l'Allegato 2 e le indicazioni relative a un incidente ai sensi del punto 10.

9.3 Per l'assistenza che vada oltre la messa a disposizione delle informazioni e delle funzionalità descritte nel presente Accordo, scryp può richiedere, previa comunicazione, un compenso adeguato in base all'impegno richiesto. Ciò non vale se l'assistenza si rende necessaria a causa di un errore di scryp.

10. Notifica delle violazioni dei dati personali

10.1 Se scryp viene a conoscenza di una violazione dei dati personali che riguarda dati del Cliente, scryp la notifica al Cliente senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne è venuto a conoscenza, tramite e-mail all'indirizzo dell'account scryp.

10.2 La notifica contiene, per quanto noto: la natura della violazione, i tipi di dati interessati e il numero approssimativo di interessati, le probabili conseguenze, le misure adottate e proposte e un punto di contatto presso scryp. Le informazioni non ancora disponibili vengono fornite da scryp successivamente senza ingiustificato ritardo.

10.3 scryp documenta la violazione e assiste il Cliente nella notifica all'autorità di controllo e nella comunicazione agli interessati. scryp effettua notifiche ad autorità o comunicazioni agli interessati per conto del Cliente soltanto su istruzione di quest'ultimo. La notifica al Cliente non costituisce ammissione di responsabilità.

11. Prove di conformità e audit

11.1 scryp mette a disposizione del Cliente tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR. Ne fanno parte il presente Accordo, la descrizione delle misure nell'Allegato 2, il registro di cui all'art. 30, par. 2, GDPR, le certificazioni dei sub-responsabili del trattamento e le risposte scritte a domande motivate del Cliente.

11.2 Se nel singolo caso tali prove non sono sufficienti, il Cliente può effettuare un audit, comprese le ispezioni, direttamente o tramite un auditor vincolato alla riservatezza che non sia un concorrente di scryp. Gli audit hanno luogo al massimo una volta per anno civile, con un preavviso di almeno 30 giorni, durante il normale orario di

lavoro e senza arrecare disturbo all'esercizio. In presenza di indizi concreti di una violazione o su richiesta di un'autorità di controllo, l'audit è possibile anche con breve preavviso e con maggiore frequenza.

11.3 L'audit non si estende ai dati di altri clienti né ai centri dati dei sub-responsabili del trattamento. Per questi ultimi valgono le rispettive certificazioni e i rispettivi rapporti di audit. Ciascuna Parte sostiene i propri costi dell'audit.

12. Cancellazione e restituzione dei dati

12.1 Durante la durata del contratto, il Cliente può cancellare autonomamente i propri dati in qualsiasi momento ed esportarli in formati di uso comune. I contenuti cancellati vengono rimossi immediatamente dall'archivio dati attivo.

12.2 scryp cancella automaticamente i file originali caricati al termine del trattamento, di norma entro pochi minuti e comunque al più tardi 72 ore dopo il caricamento. Rimangono archiviati soltanto la versione crittografata per la riproduzione, la trascrizione crittografata e le analisi crittografate.

12.3 Dopo la cessazione del Contratto principale, i contenuti restano a disposizione del Cliente per l'esportazione per un massimo di ulteriori 90 giorni. Successivamente scryp li cancella automaticamente, comprese tutte le copie. Se il Cliente cancella il proprio account, tutti i dati vengono cancellati immediatamente.

12.4 Le copie di backup servono esclusivamente al ripristino dell'intero sistema. Esse contengono i contenuti del Cliente esclusivamente in forma crittografata e vengono sovrascritte al più tardi dopo 30 giorni. Non viene effettuato alcun ripristino di singoli dati del Cliente cancellati a partire dalle copie di backup.

12.5 I dati che scryp deve continuare a conservare in forza di obblighi legali di conservazione (ad esempio i dati di fatturazione ai sensi del § 132 BAO) sono esclusi dalla cancellazione. Essi vengono bloccati e cancellati alla scadenza del termine.

12.6 Su richiesta, scryp conferma la cancellazione per iscritto; è sufficiente un'e-mail.

13. Responsabilità

13.1 Nei confronti degli interessati, le Parti rispondono ai sensi dell'art. 82 GDPR.

13.2 Nei rapporti tra le Parti si applicano le disposizioni sulla responsabilità del Contratto principale, nella misura consentita dalla legge. Per i sub-responsabili del trattamento scryp risponde come per il proprio operato (punto 7.4).

13.3 Se una Parte ha risarcito il danno agli interessati, può rivalersi sull'altra Parte per la quota corrispondente alla parte di responsabilità di quest'ultima per il danno (art. 82, par. 5, GDPR).

13.4 Se il Cliente mantiene un'istruzione nonostante scryp lo abbia avvertito della sua illiceità ai sensi del punto 3.3, il Cliente manleva scryp da tutte le pretese di terzi e da tutte le sanzioni amministrative pecuniarie fondate su tale istruzione.

14. Durata, sospensione e cessazione

14.1 Il presente Accordo si applica finché scryp tratta dati per il Cliente, ossia per la durata del Contratto principale e fino al completamento della cancellazione ai sensi del punto 12.

14.2 Per i clienti di cui al punto 1.4 non è previsto un utilizzo del Servizio senza il presente Accordo. La disdetta del presente Accordo vale pertanto al contempo come disdetta del Contratto principale.

14.3 Se scryp viola il presente Accordo, il Cliente può esigere che scryp sospenda il trattamento interessato finché la violazione non sia stata eliminata. Se scryp non pone fine a una violazione grave entro un mese dalla diffida, il Cliente può risolvere il Contratto principale senza preavviso.

15. Disposizioni finali

15.1 Il presente Accordo è concluso in forma elettronica (art. 28, par. 9, GDPR). Per i clienti di cui al punto 1.4, esso diventa parte integrante del contratto mediante il richiamo nei Termini di servizio al momento della conclusione del Contratto principale; in tal caso la parte contraente è l'intestatario dell'account scryp con i dati ivi registrati. Inoltre, esso può essere concluso mediante la sottoscrizione del presente documento da parte di entrambe le Parti, anche in copia elettronica.

15.2 Le modifiche del presente Accordo richiedono la forma scritta; è sufficiente un'e-mail. scryp può adeguare l'Allegato 2 ai sensi del punto 6.2 e l'Allegato 3 ai sensi del punto 7.2. scryp comunica le altre modifiche tramite e-mail almeno 30 giorni prima della loro entrata in vigore; fino a tale momento il Cliente può opporsi e disdire il Contratto principale con effetto a tale data. scryp conserva ogni versione del presente Accordo con numero di versione e data.

15.3 Si applica il diritto austriaco; il GDPR resta impregiudicato. Se il Cliente è un imprenditore, per tutte le controversie derivanti dal presente Accordo è esclusivamente competente il tribunale di Vienna competente per materia. Restano impregiudicati i fori inderogabili previsti dalla legge.

15.4 Qualora una disposizione sia invalida, il resto dell'Accordo rimane valido. La disposizione invalida è sostituita dalla norma di legge che più si avvicina alla sua finalità.

15.5 Il punto di contatto per tutte le questioni relative al presente Accordo è, per scryp, datenschutz@scryp.at. Per il Cliente è l'indirizzo e-mail dell'account scryp, salvo diversa comunicazione del Cliente.

15.6 scryp mette a disposizione il presente Accordo in più lingue. Fa fede la versione tedesca; le traduzioni hanno finalità di comprensione. In caso di divergenze prevale il testo tedesco.

Firme

Per il Cliente	**Per scryp**
Luogo, data	Luogo, data
Nome, funzione	Gökhan Sagir, imprenditore individuale
Firma	Firma

Allegato 1: Descrizione del trattamento

Voce	Descrizione
Oggetto	Erogazione del Servizio scryp: trascrizione di registrazioni audio e video con riconoscimento vocale e riconoscimento dei parlanti, nel piano Ultra inoltre funzioni di IA (analisi assistita dall'IA: riassunto, verbale, elenco di attività, testo per i social media), nonché archiviazione, modifica, esportazione e condivisione dei risultati.
Finalità	Il Cliente fa convertire in testo e analizzare le proprie registrazioni, ad esempio riunioni, interviste, dettati, colloqui di consulenza, conferenze o podcast.
Natura del trattamento	Ricezione di file crittografati, breve decrittografia nella RAM dei server di elaborazione, trascrizione e analisi automatiche, crittografia dei risultati, archiviazione crittografata, messa a disposizione nell'account del Cliente, cancellazione.
Tipi di dati	Registrazioni vocali e video (voce, contenuti parlati), trascrizioni e analisi da esse generate, attribuzioni dei parlanti, nomi di file e di cartelle assegnati dal Cliente, metadati tecnici (durata, dimensione del file, data e ora, lingua rilevata, stato del trattamento), in caso di trascrizioni condivise il link di condivisione. Tutti i contenuti vengono archiviati in forma crittografata; soltanto i metadati tecnici sono presenti in chiaro.
Categorie particolari (art. 9 GDPR)	Possibili, a seconda del contenuto delle registrazioni del Cliente (ad esempio dati relativi alla salute nei dettati medici, informazioni in colloqui di consulenza o con assistiti). scryp non conosce il contenuto. Il Cliente ne verifica l'ammissibilità ai sensi del punto 4.2.
Garanzie per le categorie particolari	Crittografia nel browser del Cliente, contenuti in chiaro soltanto nella RAM dei server propri di scryp a Vienna, nessuna comunicazione di contenuti in chiaro a sub-responsabili del trattamento, nessun accesso di persone ai contenuti nel normale esercizio, obbligo di riservatezza ai sensi del punto 5, nessun addestramento di modelli di IA con i dati del Cliente.
Interessati	Persone che parlano o vengono menzionate nelle registrazioni (ad esempio dipendenti, clienti, pazienti, assistiti, intervistati, partecipanti a riunioni ed eventi), nonché gli utenti dell'account del Cliente.
Luoghi del trattamento	Trascrizione e analisi tramite IA: server GPU propri di scryp a Vienna, Austria. Applicazione web, interfacce, banca dati, archivio file crittografato e copie di backup: centro dati di Hetzner Online GmbH a Norimberga, Germania.
Durata	Durata del Contratto principale, maggiorata dei termini di cancellazione ai sensi del punto 12.

Allegato 2: Misure tecniche e organizzative (art. 32 GDPR)

Aggiornato al 22 settembre 2026. Le misure descrivono il normale esercizio di scryp.

1. Crittografia e architettura zero-knowledge

- Le registrazioni vengono crittografate con AES-256-GCM già nel browser del Cliente prima di essere trasmesse a scryp. Per ogni file viene generata una chiave del file (FEK) dedicata.
- Le chiavi dei file vengono crittografate con una chiave principale dell'account (MEK). La chiave principale è accessibile soltanto con la password del Cliente (derivazione mediante PBKDF2-SHA256, 600.000 iterazioni). scryp non conosce in chiaro né la password né la chiave principale.
- Per la trascrizione, il browser trasmette a scryp la chiave del file crittografata con una chiave del server (RSA-4096, OAEP). Il server di elaborazione decrittografa la registrazione esclusivamente nella RAM. I file temporanei risiedono in un file system in RAM e vengono eliminati al termine dell'incarico; i contenuti non crittografati non vengono mai scritti su supporti di memorizzazione.
- Le trascrizioni e le analisi vengono crittografate con la chiave del file subito dopo la loro creazione e archiviate soltanto in forma crittografata. I nomi di file e di cartelle vengono crittografati nel browser.
- In caso di condivisione di una trascrizione, la chiave del file viene crittografata con una chiave derivata dalla password di condivisione. I destinatari decrittografano esclusivamente nel proprio browser.
- Eccezione caricamento tramite URL: se il Cliente richiama una registrazione tramite un indirizzo internet, il server di elaborazione scarica direttamente il file, lo elabora nella RAM e successivamente lo cancella; la trascrizione e la versione per la riproduzione vengono archiviate in forma crittografata come di consueto.
- Tutte le connessioni sono crittografate con TLS 1.2 o 1.3.

2. Controllo dell'accesso fisico

- L'applicazione web, la banca dati, l'archivio file e le copie di backup sono eseguiti nel centro dati di Hetzner Online GmbH a Norimberga (certificato ISO/IEC 27001, attestazione BSI C5 di tipo 2) con controllo dell'accesso fisico, videosorveglianza e personale di sicurezza del gestore.
- I server GPU per la trascrizione e l'analisi tramite IA si trovano in locali propri e chiusi di scryp a Vienna. L'accesso è consentito soltanto alle persone autorizzate; l'ingresso è chiuso meccanicamente e protetto inoltre da un sistema biometrico.
- Tutti i supporti di memorizzazione di tali server sono completamente crittografati. In caso di furto o rimozione di un supporto, i dati restano illeggibili senza la chiave. Su tali server i contenuti non crittografati sono presenti soltanto nella RAM durante un incarico in corso e non vengono mai scritti su un supporto di memorizzazione.

3. Controllo dell'accesso ai sistemi e ai dati

- Accesso ai server riservato agli amministratori di scryp tramite connessioni SSH crittografate con chiavi personali o password robuste generate casualmente; accesso secondo il principio del privilegio minimo.
- Interfaccia di amministrazione separata con accesso dedicato, limitata a indirizzi IP autorizzati. L'interfaccia di amministrazione mostra soltanto metadati relativi ad account e incarichi, nessun contenuto.
- Account utente: le password vengono sottoposte a hashing con Argon2id; protezione contro i tentativi di accesso mediante limitazione della frequenza e blocco temporaneo; le sessioni funzionano senza cookie con token di breve durata.
- Protezione delle interfacce da abusi e sovraccarico mediante limitazione della frequenza e blocchi automatici.
- I servizi automatizzati (server di elaborazione) si autenticano con credenziali proprie e rotabili e ricevono soltanto le chiavi necessarie per il rispettivo incarico.

4. Controllo della separazione e pseudonimizzazione

- Separazione crittografica: ogni Cliente dispone di una propria chiave principale, ogni file di una propria chiave del file. I contenuti di un Cliente non sono leggibili con chiavi altrui.
- Separazione logica dei sistemi di produzione, banca dati, cache e monitoraggio in zone di rete distinte.
- Gli incarichi di elaborazione inviati ai server GPU non contengono nomi né indirizzi e-mail, ma soltanto i dati tecnici necessari per l'incarico.

5. Integrità e tracciabilità

- Tutte le modifiche all'applicazione e all'infrastruttura avvengono tramite codice sorgente versionato e distribuzione automatizzata e tracciabile; le immagini software sono vincolate alla propria somma di controllo.
- Gli eventi dell'account (ad esempio accesso, cancellazione, modifiche dell'abbonamento) vengono registrati con data e ora, senza indirizzi IP.
- I log di sistema non contengono contenuti e vengono cancellati dopo 14 giorni. Gli indirizzi IP non vengono memorizzati né registrati nei log. Per contrastare gli abusi, gli accessi vengono conteggiati soltanto tramite uno pseudonimo di breve durata, generato con una chiave segreta e non reversibile, che scade al massimo dopo un'ora.

6. Disponibilità e resilienza

- Cluster ad alta disponibilità composto da tre server con bilanciamento del carico; banca dati con replica sincrona su tre nodi; cache con failover automatico.
- Backup giornaliero crittografato della banca dati con ripristino a qualsiasi momento degli ultimi 30 giorni; configurazione del cluster salvata ogni sei ore. I backup risiedono nel centro dati di Norimberga.
- Distribuzione di nuove versioni senza interruzione del servizio; protezione contro attacchi di sovraccarico a livello di rete e di applicazione.
- Monitoraggio continuo con allarme automatico in caso di anomalie.

7. Cancellazione e minimizzazione dei dati

- I file originali caricati vengono cancellati dopo il trattamento, di norma entro pochi minuti; una regola automatica rimuove i caricamenti rimasti in sospeso al più tardi dopo 72 ore.
- Il Cliente cancella autonomamente contenuti e account in qualsiasi momento; la cancellazione ha effetto immediato nell'archivio dati attivo. Dopo la fine di un abbonamento, i contenuti vengono cancellati automaticamente dopo 90 giorni.
- Nessun cookie, nessuno strumento di tracciamento o di analisi di terzi, nessuna memorizzazione di indirizzi IP.

8. Organizzazione

- Tutte le persone che operano presso scryp sono vincolate al segreto dei dati e alla riservatezza e sono state istruite sull'architettura di sicurezza.
- scryp tiene un registro delle attività di trattamento (art. 30 GDPR). La valutazione d'impatto sulla protezione dei dati, il registro e le presenti misure vengono riesaminati almeno una volta all'anno e in caso di modifiche sostanziali.
- Processo di gestione degli incidenti: rilevamento tramite monitoraggio, valutazione, contenimento, notifica ai clienti interessati ai sensi del punto 10 dell'Accordo, analisi successiva.
- I sub-responsabili del trattamento vengono verificati quanto alle loro garanzie prima dell'impiego e vincolati contrattualmente ai sensi dell'art. 28, par. 4, GDPR.

Allegato 3: Sub-responsabili del trattamento

Aggiornato al 22 settembre 2026.

Sub-responsabile del trattamento	Prestazione	Dati	Luogo del trattamento	Garanzia
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland	Gestione dei server per applicazione web, interfacce e banca dati; archiviazione di oggetti crittografata; copie di backup	Tutti i dati indicati nell'Allegato 1, contenuti esclusivamente in forma crittografata	Norimberga, Germania (UE)	Accordo sul trattamento dei dati; ISO/IEC 27001; BSI C5
Mailjet GmbH (Sinch-Konzern), Alt Moabit 2, 10557 Berlin, Deutschland	Invio di e-mail di sistema (ad esempio la notifica «Trascrizione completata»)	Indirizzo e-mail dell'account, data dell'incarico, link all'account; nessun contenuto, nessun nome di file	Francia (UE)	Accordo sul trattamento dei dati; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, Irland	Ricezione e gestione delle richieste di assistenza tramite e-mail (Microsoft 365)	Soltanto i dati che il Cliente stesso trasmette in una richiesta di assistenza	UE; possibile accesso remoto da paesi terzi	Accordo sul trattamento dei dati; clausole contrattuali standard dell'UE; quadro UE-USA per la protezione dei dati personali (EU-US Data Privacy Framework)