Data Processing Agreement (DPA)

pursuant to Art. 28 General Data Protection Regulation (GDPR)

Version 1.0, as of 22 September 2026

Parties

Customer (controller within the meaning of Art. 4(7) GDPR):

Company / name: _____

Address: _____

Email of the scryp account: _____

scryp (processor within the meaning of Art. 4(8) GDPR):

Gökhan Sagir, sole trader, trading under the brand scryp
Erdbergstraße 121/9, 1030 Vienna, Austria
VAT ID: ATU83108129
Data protection contact: datenschutz@scryp.at

Hereinafter "Customer" and "scryp", together the "Parties".

What this is about

The Customer uses scryp to have audio and video recordings transcribed and analysed. People speak in these recordings, and the Customer is responsible for their personal data. scryp processes this data only on behalf of the Customer. This agreement sets out what scryp may do with the data, how scryp protects it and what happens to it in the end.

1. Subject matter and scope

1.1 This agreement applies to all personal data that scryp processes on behalf of the Customer when providing the scryp service under the General Terms and Conditions (Terms, available at www.scryp.at/agb). The contract on the use of the service is referred to below as the "Main Contract". The current version of this agreement is available at www.scryp.at/avv.

1.2 This agreement does not cover the data of the contractual relationship itself, meaning the Customer's account, contract, billing and support data. scryp processes this data as an independent controller in accordance with its privacy policy (www.scryp.at/datenschutz).

1.3 Annexes 1 to 3 form part of this agreement. In the event of a conflict between this agreement and the Main Contract, this agreement prevails in matters of data protection.

1.4 This agreement is intended for customers who use scryp in the course of a professional, commercial or official activity. For purely private use, the GDPR does not apply under Art. 2(2)(c), and no data processing agreement is required.

2. Nature, purpose and scope of the processing

2.1 The nature and purpose of the processing, the types of data and the categories of data subjects are described in Annex 1.

2.2 scryp processes the data exclusively in member states of the European Union. The processing locations are named in Annex 1 and Annex 3.

2.3 The duration of the processing corresponds to the term of the Main Contract plus the deletion periods set out in clause 12.

3. Instructions

3.1 scryp processes the data only on documented instructions from the Customer. The Customer's instructions are the Main Contract, this agreement and the Customer's use of the functions of the service (in particular uploading, transcribing, analysing, editing, sharing, exporting and deleting). Each use of a function is a documented individual instruction to carry out the associated processing.

3.2 The Customer issues further instructions in writing; an email to datenschutz@scryp.at is sufficient. The account holder and the persons whom the Customer assigns to its scryp account are authorised to issue instructions. Instructions that go beyond the scope of the service are deemed a request for a change of service.

3.3 If, in scryp's opinion, an instruction infringes the GDPR or other data protection provisions, scryp informs the Customer without delay. scryp may suspend execution until the Customer confirms or amends the instruction.

3.4 scryp does not use the data for its own purposes. In particular, the Customer's recordings, transcripts and analyses are not used to train or improve AI models and are not passed on to third parties unless this agreement provides otherwise.

3.5 If an authority or a court demands that scryp hand over the Customer's data, scryp informs the Customer without delay where legally permissible, refers the authority to the Customer and hands over only what scryp is legally obliged to provide. In doing so, scryp checks whether a statutory duty of confidentiality of the Customer precludes the handover (Section 6(5) Austrian Data Protection Act, DSG).

4. Obligations of the Customer

4.1 The Customer is responsible for the lawfulness of the recordings and their processing. In particular, the Customer ensures a legal basis (Art. 6, and for special categories Art. 9 GDPR), the information of the data subjects (Art. 13 and 14 GDPR) and that no non-public statements are recorded without the consent of the speakers (for example Section 120 of the Austrian Criminal Code, StGB).

4.2 If recordings contain special categories of personal data (for example health data) or content subject to professional secrecy, the Customer checks in advance whether the processing is permissible and whether a data protection impact assessment (Art. 35 GDPR) is required. scryp provides the information from this agreement and its annexes for this purpose.

4.3 The Customer keeps the email address of its scryp account up to date. scryp sends all notices under this agreement to this address, in particular notifications under clause 10.

4.4 The Customer has the right to issue instructions to scryp, to request evidence and to carry out audits under clause 11.

5. Confidentiality and professional secrecy

5.1 scryp grants access to the data only to persons who are bound to data secrecy (Section 6 DSG) and confidentiality and who have been instructed about the consequences of a breach (Art. 28(3)(b), Art. 29 GDPR). The obligation continues after the end of their engagement.

5.2 scryp is built so that the Customer's content (recordings, transcripts, analyses, file and folder names) is stored only in encrypted form and exists in plain text only for the duration of the respective processing in the working memory of the processing servers. Persons at scryp have no access to content in plain text during normal operation. Details are set out in Annex 2.

5.3 If the Customer is subject to a statutory duty of confidentiality (for example Section 9 of the Austrian Lawyers' Code, RAO; Section 54 of the Austrian Physicians' Act, ÄrzteG; Section 121 StGB), scryp undertakes, as an auxiliary of the Customer, to keep all content that becomes accessible to scryp in the course of the service confidential in the same way. For customers subject to German law, this also constitutes an obligation of secrecy under Section 203(4) of the German Criminal Code (StGB, Germany). On request, scryp confirms this obligation in a separate declaration.

6. Security of processing

6.1 scryp implements the technical and organisational measures under Art. 32 GDPR described in Annex 2.

6.2 scryp may further develop these measures and replace them with equivalent or better ones. The level of protection must not fall below the current level. scryp documents material changes and informs the Customer. The current version of Annex 2 is available at www.scryp.at/avv.

6.3 scryp reviews the effectiveness of the measures at least once a year and informs the Customer of the result on request.

7. Sub-processors

7.1 The Customer authorises the sub-processors named in Annex 3 (general authorisation under Art. 28(2) GDPR).

7.2 If scryp intends to add or replace a sub-processor, scryp informs the Customer at least 30 days before the engagement by email to the address of the scryp account. The Customer may object in writing within 14 days of receipt of this notice on important data protection grounds; an email is sufficient. If the Customer does not object, the change is deemed approved.

7.3 If the Parties cannot find a solution after an objection, the Customer may terminate the Main Contract with effect from the planned engagement date. scryp refunds pro rata any fees the Customer has prepaid for the period after termination.

7.4 scryp imposes on each sub-processor, by contract, the same data protection obligations that apply to scryp under this agreement, in particular sufficient guarantees of appropriate technical and organisational measures (Art. 28(4) GDPR). If a sub-processor fails to fulfil its obligations, scryp is liable to the Customer for that sub-processor's obligations as for its own conduct.

7.5 Ancillary services without access to customer data, for example telecommunications, cleaning or maintenance without data access, do not constitute sub-processing.

8. Processing location and third countries

8.1 scryp processes and stores the data in Austria and Germany. scryp does not transfer data to countries outside the European Union or the European Economic Area.

8.2 Should a sub-processor process data in a third country, this happens only to the extent described in Annex 3 and only with an appropriate safeguard under Chapter V GDPR (for example an adequacy decision of the European Commission or EU standard contractual clauses).

9. Assistance to the Customer

9.1 Rights of data subjects: In most cases the Customer can fulfil access, rectification, erasure and data portability itself using the functions of the service (view, edit, export, delete). Because scryp holds content only in encrypted form, scryp cannot determine which persons appear in a recording. If a data subject contacts scryp, scryp forwards the request to the Customer without delay and does not answer it itself unless the Customer instructs scryp to do so.

9.2 Security, personal data breaches, data protection impact assessment and consultation of the supervisory authority (Art. 32 to 36 GDPR): scryp assists the Customer with the information available to scryp, in particular this agreement, Annex 2 and the details of an incident under clause 10.

9.3 scryp may, after prior notice, charge reasonable remuneration on a time and material basis for assistance that goes beyond providing the information and functions described in this agreement. This does not apply where the assistance becomes necessary because of an error on scryp's part.

10. Notification of personal data breaches

10.1 If scryp becomes aware of a personal data breach affecting the Customer's data, scryp notifies the Customer without undue delay and at the latest within 48 hours of becoming aware, by email to the address of the scryp account.

10.2 As far as known, the notification contains: the nature of the breach, the categories of data and the approximate number of data subjects concerned, the likely consequences, the measures taken and proposed, and a point of contact at scryp. Information that is not yet available is provided by scryp without undue delay.

10.3 scryp documents the breach and assists the Customer with the notification to the supervisory authority and the communication to the data subjects. scryp makes notifications to authorities or data subjects on behalf of the Customer only on the Customer's instruction. The notification to the Customer is not an admission of fault.

11. Evidence and audits

11.1 scryp makes available to the Customer all information necessary to demonstrate compliance with the obligations under Art. 28 GDPR. This includes this agreement, the description of the measures in Annex 2, the record under Art. 30(2) GDPR, the certifications of the sub-processors and written answers to reasoned questions from the Customer.

11.2 If this evidence is insufficient in an individual case, the Customer may carry out an audit, including an inspection, itself or through an auditor bound to confidentiality who is not a competitor of scryp. Audits take place at most once per calendar year, with at least 30 days' notice, during normal business hours and without disrupting operations. Where there are concrete indications of a breach or at the request of a supervisory authority, an audit is also possible at short notice and more frequently.

11.3 The audit does not extend to data of other customers or to data centres of sub-processors. Their certifications and audit reports apply to them. Each Party bears its own costs of the audit.

12. Deletion and return of data

12.1 During the term, the Customer can delete and export its data itself at any time in common formats. Deleted content is removed immediately from the active data set.

12.2 scryp automatically deletes uploaded original files after the processing is complete, normally within a few minutes and at the latest 72 hours after the upload. Only the encrypted playback version, the encrypted transcript and the encrypted analyses remain stored.

12.3 After the end of the Main Contract, the content remains available to the Customer for export for up to 90 days. After that, scryp deletes it automatically, including all copies. If the Customer deletes its account, all data is deleted immediately.

12.4 Backups serve only to restore the overall system. They contain the Customer's content exclusively in encrypted form and are overwritten after 30 days at the latest. Individual deleted customer data is not restored from backups.

12.5 Data that scryp must continue to store due to statutory retention obligations (for example invoice data under Section 132 of the Austrian Federal Fiscal Code, BAO) is exempt from deletion. It is blocked and deleted after the retention period expires.

12.6 On request, scryp confirms the deletion in writing; an email is sufficient.

13. Liability

13.1 Towards data subjects, the Parties are liable in accordance with Art. 82 GDPR.

13.2 Between the Parties, the liability provisions of the Main Contract apply to the extent permitted by law. scryp is liable for sub-processors as for its own conduct (clause 7.4).

13.3 If a Party has paid compensation to data subjects, it may claim back from the other Party the part that corresponds to that Party's share of responsibility for the damage (Art. 82(5) GDPR).

13.4 If the Customer maintains an instruction although scryp has pointed out its unlawfulness under clause 3.3, the Customer indemnifies scryp against all third-party claims and fines based on that instruction.

14. Term, suspension and termination

14.1 This agreement applies for as long as scryp processes data for the Customer, meaning for the term of the Main Contract and until the deletion under clause 12 is complete.

14.2 Use of the service without this agreement is not intended for customers under clause 1.4. Termination of this agreement therefore also constitutes termination of the Main Contract.

14.3 If scryp breaches this agreement, the Customer may require scryp to suspend the affected processing until the breach has been remedied. If scryp fails to remedy a material breach within one month of being requested to do so, the Customer may terminate the Main Contract without notice.

15. Final provisions

15.1 This agreement is concluded in electronic form (Art. 28(9) GDPR). For customers under clause 1.4, it becomes part of the contract through its incorporation into the Terms upon conclusion of the Main Contract; the contracting party is then the holder of the scryp account with the details stored there. In addition, it may be concluded by both Parties signing this document, also as an electronic copy.

15.2 Amendments to this agreement must be made in writing; an email is sufficient. scryp may adapt Annex 2 under clause 6.2 and Annex 3 under clause 7.2. scryp announces other amendments by email at least 30 days before they take effect; the Customer may object until then and terminate the Main Contract as of that date. scryp keeps every version of this agreement with version number and date.

15.3 Austrian law applies; the GDPR remains unaffected. If the Customer is an entrepreneur, the court with subject-matter jurisdiction in Vienna has exclusive jurisdiction for all disputes arising from this agreement. Mandatory statutory places of jurisdiction remain unaffected.

15.4 Should a provision be invalid, the remainder of the agreement remains valid. The invalid provision is replaced by the statutory rule that comes closest to its purpose.

15.5 The point of contact for all questions concerning this agreement is datenschutz@scryp.at at scryp. On the Customer's side, it is the email address of the scryp account unless the Customer notifies otherwise.

15.6 scryp provides this agreement in several languages. The German version is binding; translations serve understanding only. In the event of discrepancies, the German wording prevails.

Signatures

For the Customer	**For scryp**
Place, date	Place, date
Name, position	Gökhan Sagir, sole trader
Signature	Signature

Annex 1: Description of the processing

Item	Description
Subject matter	Provision of the scryp service: transcription of audio and video recordings with speech recognition and speaker recognition, on the Ultra plan additionally AI features (AI-based analysis: summary, minutes, task list, social media text), as well as storage, editing, export and sharing of the results.
Purpose	The Customer has its own recordings converted into text and analysed, for example meetings, interviews, dictations, consultations, lectures or podcasts.
Nature of the processing	Receipt of encrypted files, brief decryption in the working memory of the processing servers, automatic transcription and analysis, encryption of the results, encrypted storage, provision in the Customer's account, deletion.
Types of data	Voice recordings and videos (voice, spoken content), transcripts and analyses generated from them, speaker assignments, file and folder names assigned by the Customer, technical metadata (duration, file size, timestamps, detected language, processing status), and for shared transcripts the sharing link. All content is stored in encrypted form; only the technical metadata exists in plain text.
Special categories (Art. 9 GDPR)	Possible, depending on the content of the Customer's recordings (for example health data in medical dictations, details in consultations or client meetings). scryp does not know the content. The Customer checks permissibility under clause 4.2.
Safeguards for special categories	Encryption in the Customer's browser, plain text only in the working memory of scryp's own servers in Vienna, no transfer of content to sub-processors in plain text, no access by persons to content during normal operation, duty of confidentiality under clause 5, no training of AI models with customer data.
Data subjects	Persons who speak or are mentioned in the recordings (for example employees, customers, patients, clients, interview partners, participants in meetings and events), and the users of the Customer's account.
Processing locations	Transcription and AI analysis: scryp's own GPU servers in Vienna, Austria. Web application, interfaces, database, encrypted file storage and backups: data centre of Hetzner Online GmbH in Nuremberg, Germany.
Duration	Term of the Main Contract plus deletion periods under clause 12.

Annex 2: Technical and organisational measures (Art. 32 GDPR)

As of 22 September 2026. The measures describe scryp's normal operation.

1. Encryption and zero-knowledge architecture

- Recordings are encrypted with AES-256-GCM in the Customer's browser before they are transmitted to scryp. A separate file key (FEK) is generated for each file.
- File keys are encrypted with a master key of the account (MEK). The master key is accessible only with the Customer's password (derived with PBKDF2-SHA256, 600,000 iterations). scryp knows neither the password nor the master key in plain text.
- For transcription, the browser transmits the file key to scryp encrypted with a server key (RSA-4096, OAEP). The processing server decrypts the recording exclusively in working memory. Temporary files reside in a RAM file system and are discarded after the job; unencrypted content is never written to disk.
- Transcripts and analyses are encrypted with the file key immediately after creation and stored only in encrypted form. File and folder names are encrypted in the browser.
- When a transcript is shared, the file key is encrypted with a key derived from the sharing password. Recipients decrypt exclusively in their own browser.
- Exception for URL upload: If the Customer retrieves a recording via an internet address, the processing server downloads the file directly, processes it in working memory and deletes it afterwards; the transcript and playback version are stored in encrypted form as usual.
- All connections are encrypted with TLS 1.2 or 1.3.

2. Physical access control

- Web application, database, file storage and backups run in the data centre of Hetzner Online GmbH in Nuremberg (ISO/IEC 27001 certified, BSI C5 Type 2 attestation) with access control, video surveillance and security staff of the operator.
- The GPU servers for transcription and AI analysis are located in scryp's own locked premises in Vienna. Only authorised persons have access; the entrance is mechanically locked and additionally secured biometrically.
- All storage media of these servers are fully encrypted. If a storage medium is stolen or removed, the data remains unreadable without the key. Unencrypted content exists on these servers only in working memory during a running job and is never written to a storage medium.

3. System and data access control

- Server access only for scryp administrators via encrypted SSH connections with personal keys or randomly generated strong passwords; access follows the principle of least privilege.
- Separate administration interface with its own login, restricted to approved IP addresses. The administration interface shows only account and job metadata, no content.
- User accounts: passwords are hashed with Argon2id; protection against login attempts through rate limiting and temporary lockout; sessions run without cookies using short-lived tokens.
- Protection of the interfaces against abuse and overload through rate limiting and automatic blocking.
- Automated services (processing servers) authenticate with their own rotatable credentials and receive only the keys required for the respective job.

4. Separation control and pseudonymisation

- Cryptographic separation: each customer has its own master key, each file its own file key. One customer's content cannot be read with another customer's keys.
- Logical separation of production, database, cache and monitoring systems in separate network zones.
- Processing jobs sent to the GPU servers contain no names and no email addresses, only the technical data required for the job.

5. Integrity and traceability

- All changes to the application and infrastructure are made through versioned source code and automated, traceable deployment; software images are pinned by their checksum.
- Account events (for example login, deletion, subscription changes) are logged with a timestamp, without IP addresses.
- System logs contain no content and are deleted after 14 days. IP addresses are neither stored nor logged. To prevent abuse, requests are counted only via a short-lived, keyed and non-reversible pseudonym that expires after one hour at the latest.

6. Availability and resilience

- Highly available cluster of three servers with load balancing; database with synchronous replication across three nodes; cache with automatic failover.
- Daily encrypted backup of the database with restore to any point in time within the last 30 days; cluster configuration backed up every six hours. Backups are located in the data centre in Nuremberg.
- Deployment of new versions without service interruption; protection against overload attacks at network and application level.
- Continuous monitoring with automatic alerting in the event of faults.

7. Deletion and data minimisation

- Uploaded original files are deleted after processing, normally within a few minutes; an automatic rule removes leftover uploads after 72 hours at the latest.
- The Customer deletes content and account itself at any time; deletion takes effect immediately in the active data set. After a subscription ends, content is deleted automatically after 90 days.
- No cookies, no third-party tracking or analytics tools, no storage of IP addresses.

8. Organisation

- All persons working for scryp are bound to data secrecy and confidentiality and have been briefed on the security architecture.
- scryp keeps a record of processing activities (Art. 30 GDPR). The data protection impact assessment, the record and these measures are reviewed at least once a year and whenever material changes occur.
- Incident process: detection through monitoring, assessment, containment, notification of affected customers under clause 10 of the agreement, follow-up.
- Sub-processors are checked for their guarantees before engagement and bound by contract under Art. 28(4) GDPR.

Annex 3: Sub-processors

As of 22 September 2026.

Sub-processor	Service	Data	Processing location	Safeguard
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Germany	Operation of the servers for web application, interfaces and database; encrypted object storage; backups	All data named in Annex 1, content exclusively encrypted	Nuremberg, Germany (EU)	Data processing agreement; ISO/IEC 27001; BSI C5
Mailjet GmbH (Sinch group), Alt Moabit 2, 10557 Berlin, Germany	Sending of system emails (for example the "transcript ready" notification)	Email address of the account, date of the job, link to the account; no content, no file names	France (EU)	Data processing agreement; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, Ireland	Receipt and handling of support requests by email (Microsoft 365)	Only data that the Customer itself submits in a support request	EU; remote access from third countries possible	Data processing agreement; EU standard contractual clauses; EU-US Data Privacy Framework