Accord de traitement des données (DPA)

conformément à l'art. 28 du règlement général sur la protection des données (RGPD)

Version 1.0, en date du 22 septembre 2026

Parties

Client (responsable du traitement au sens de l'art. 4, point 7), du RGPD) :

Société / Nom : _____

Adresse : _____

E-mail du compte scryp : _____

scryp (sous-traitant au sens de l'art. 4, point 8), du RGPD) :

Gökhan Sagir, entrepreneur individuel, agissant sous la marque scryp
Erdbergstraße 121/9, 1030 Vienne, Autriche
UID : ATU83108129
Contact protection des données : datenschutz@scryp.at

Ci-après le « Client » et « scryp », ensemble les « Parties ».

De quoi il s'agit

Le Client utilise scryp pour faire transcrire et analyser des enregistrements audio et vidéo. Dans ces enregistrements s'expriment des personnes dont les données à caractère personnel relèvent de la responsabilité du Client. scryp traite ces données uniquement pour le compte du Client. Le présent accord détermine ce que scryp est autorisé à faire avec les données, comment scryp les protège et ce qu'il en advient au terme du traitement.

1. Objet et champ d'application

1.1 Le présent accord s'applique à toutes les données à caractère personnel que scryp traite pour le compte du Client dans le cadre de la fourniture du service scryp conformément aux Conditions générales d'utilisation (CGU, disponibles sur www.scryp.at/agb). Le contrat relatif à l'utilisation du service est ci-après dénommé « contrat principal ». La version en vigueur du présent accord est disponible sur www.scryp.at/avv.

1.2 Ne relèvent pas du présent accord les données de la relation contractuelle elle-même, c'est-à-dire les données de compte, de contrat, de facturation et d'assistance du Client. scryp traite ces données en qualité de responsable du traitement à part entière, conformément à sa Politique de confidentialité (www.scryp.at/datenschutz).

1.3 Les annexes 1 à 3 font partie intégrante du présent accord. En cas de contradiction entre le présent accord et le contrat principal, le présent accord prévaut pour les questions de protection des données.

1.4 Le présent accord est destiné aux clients qui utilisent scryp dans le cadre d'une activité professionnelle, commerciale ou administrative. En cas d'utilisation strictement privée, le RGPD n'est pas applicable en vertu de son art. 2, par. 2, point c), et aucun accord de traitement des données n'est requis.

2. Nature, finalité et étendue du traitement

2.1 La nature et la finalité du traitement, les types de données et les catégories de personnes concernées sont décrits à l'annexe 1.

2.2 scryp traite les données exclusivement dans des États membres de l'Union européenne. Les lieux de traitement sont indiqués à l'annexe 1 et à l'annexe 3.

2.3 La durée du traitement correspond à la durée du contrat principal, augmentée des délais de suppression prévus au point 12.

3. Instructions

3.1 scryp ne traite les données que sur instruction documentée du Client. Les instructions du Client sont le contrat principal, le présent accord et l'utilisation des fonctionnalités du service par le Client (notamment le téléversement, la transcription, l'analyse, la modification, le partage, l'exportation et la suppression). Chaque utilisation d'une fonctionnalité constitue une instruction individuelle documentée d'exécuter le traitement correspondant.

3.2 Le Client donne toute autre instruction par écrit ; un e-mail à datenschutz@scryp.at suffit. Sont habilités à donner des instructions le titulaire du compte et les personnes que le Client affecte à son compte scryp. Les instructions qui dépassent l'étendue des prestations du service sont considérées comme une demande de modification des prestations.

3.3 Si scryp estime qu'une instruction est contraire au RGPD ou à d'autres dispositions relatives à la protection des données, scryp en informe le Client sans délai. scryp peut suspendre l'exécution jusqu'à ce que le Client confirme ou modifie l'instruction.

3.4 scryp n'utilise pas les données à ses propres fins. En particulier, les enregistrements, transcriptions et analyses du Client ne sont pas utilisés pour l'entraînement ou l'amélioration de modèles d'IA et ne sont pas communiqués à des tiers, sauf disposition contraire du présent accord.

3.5 Si une autorité ou un tribunal exige de scryp la remise de données du Client, scryp en informe le Client sans délai, dans la mesure où la loi le permet, renvoie l'organisme demandeur au Client et ne remet que ce à quoi scryp est légalement tenu. scryp vérifie à cette occasion si une obligation légale de secret du Client s'oppose à la remise (§ 6, al. 5, DSG).

4. Obligations du Client

4.1 Le Client est responsable de la licéité des enregistrements et de leur traitement. Il veille en particulier à disposer d'une base juridique (art. 6 et, pour les catégories particulières de données, art. 9 du RGPD), à informer les personnes concernées (art. 13 et 14 du RGPD) et à ce qu'aucun propos non public ne soit enregistré sans l'accord des personnes qui s'expriment (par exemple § 120 StGB en Autriche).

4.2 Si des enregistrements contiennent des catégories particulières de données à caractère personnel (par exemple des données de santé) ou des contenus couverts par le secret professionnel, le Client vérifie au préalable si le traitement est licite et si une analyse d'impact relative à la protection des données (art. 35 du RGPD) est nécessaire. scryp met à disposition à cette fin les informations contenues dans le présent accord et ses annexes.

4.3 Le Client maintient à jour l'adresse e-mail de son compte scryp. scryp adresse à cette adresse toutes les communications prévues par le présent accord, en particulier les notifications visées au point 10.

4.4 Le Client a le droit de donner des instructions à scryp, d'exiger des justificatifs et de procéder à des audits conformément au point 11.

5. Confidentialité et secret professionnel

5.1 scryp n'autorise l'accès aux données qu'aux personnes qui sont tenues au secret des données (§ 6 DSG) et à la confidentialité et qui ont été informées des conséquences d'une violation (art. 28, par. 3, point b), et art. 29 du RGPD). Cette obligation subsiste après la fin de l'activité.

5.2 scryp est conçu de telle sorte que les contenus du Client (enregistrements, transcriptions, analyses, noms de fichiers et de dossiers) ne sont stockés que sous forme chiffrée et n'existent en clair, pendant la durée du traitement concerné, que dans la mémoire vive des serveurs de traitement. En fonctionnement courant, les personnes travaillant chez scryp n'ont pas accès aux contenus en clair. Les détails figurent à l'annexe 2.

5.3 Si le Client est soumis à une obligation légale de secret (par exemple § 9 RAO, § 54 ÄrzteG, § 121 StGB), scryp s'engage, en qualité d'auxiliaire du Client, à garder secrets de la même manière tous les contenus auxquels scryp a accès dans le cadre de la prestation. Pour les clients soumis au droit allemand, cet engagement vaut également obligation de confidentialité au sens du § 203, al. 4, StGB (Allemagne). Sur demande, scryp confirme cet engagement dans une déclaration distincte.

6. Sécurité du traitement

6.1 scryp met en œuvre les mesures techniques et organisationnelles prévues à l'art. 32 du RGPD qui sont décrites à l'annexe 2.

6.2 scryp peut faire évoluer ces mesures et les remplacer par des mesures équivalentes ou meilleures. Le niveau de protection ne doit pas en être diminué. scryp documente les modifications substantielles et les communique au Client. La version en vigueur de l'annexe 2 est disponible sur www.scryp.at/avv.

6.3 scryp vérifie l'efficacité des mesures au moins une fois par an et communique le résultat au Client sur demande.

7. Sous-traitants ultérieurs

7.1 Le Client autorise les sous-traitants ultérieurs mentionnés à l'annexe 3 (autorisation générale au sens de l'art. 28, par. 2, du RGPD).

7.2 Si scryp souhaite ajouter ou remplacer un sous-traitant ultérieur, scryp en informe le Client au moins 30 jours avant son intervention par e-mail à l'adresse du compte scryp. Le Client peut s'y opposer par écrit, pour un motif sérieux tenant à la protection des données, dans les 14 jours suivant la réception de cette communication ; un e-mail suffit. Si le Client ne s'oppose pas, la modification est réputée autorisée.

7.3 Si, après une opposition, les Parties ne parviennent pas à une solution, le Client peut résilier le contrat principal avec effet à la date prévue pour l'intervention. scryp rembourse au prorata les montants que le Client a payés d'avance pour la période postérieure à la fin du contrat.

7.4 scryp impose par contrat à chaque sous-traitant ultérieur les mêmes obligations en matière de protection des données que celles qui incombent à scryp en vertu du présent accord, en particulier des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées (art. 28, par. 4, du RGPD). Si un sous-traitant ultérieur ne remplit pas ses obligations, scryp répond envers le Client des obligations de ce sous-traitant ultérieur comme de son propre fait.

7.5 Les prestations accessoires sans accès aux données du Client, par exemple les télécommunications, le nettoyage ou la maintenance sans accès aux données, ne constituent pas une sous-traitance ultérieure.

8. Lieu du traitement et pays tiers

8.1 scryp traite et stocke les données en Autriche et en Allemagne. scryp ne procède à aucun transfert vers des pays situés en dehors de l'Union européenne ou de l'Espace économique européen.

8.2 Si un sous-traitant ultérieur devait traiter des données dans un pays tiers, cela n'a lieu que dans la mesure décrite à l'annexe 3 et uniquement sur la base d'une garantie appropriée au sens du chapitre V du RGPD (par exemple une décision d'adéquation de la Commission européenne ou les clauses contractuelles types de l'UE).

9. Assistance au Client

9.1 Droits des personnes concernées : le Client peut, dans la plupart des cas, donner suite lui-même aux demandes d'accès, de rectification, d'effacement et de portabilité des données au moyen des fonctionnalités du service (affichage, modification, exportation, suppression). Comme scryp ne conserve les contenus que sous forme chiffrée, scryp ne peut pas déterminer quelles personnes apparaissent dans un enregistrement. Si une personne concernée s'adresse à scryp, scryp transmet la demande sans délai au Client et n'y répond pas directement, sauf si le Client lui en donne l'instruction.

9.2 Sécurité, violations de données à caractère personnel, analyse d'impact relative à la protection des données et consultation de l'autorité de contrôle (art. 32 à 36 du RGPD) : scryp assiste le Client au moyen des informations dont scryp dispose, en particulier le présent accord, l'annexe 2 et les informations relatives à un incident conformément au point 10.

9.3 Pour toute assistance allant au-delà de la mise à disposition des informations et fonctionnalités décrites dans le présent accord, scryp peut, après notification préalable, facturer une rémunération raisonnable en fonction du temps consacré. Cela ne s'applique pas lorsque l'assistance est rendue nécessaire par une faute de scryp.

10. Notification des violations de données à caractère personnel

10.1 Si scryp a connaissance d'une violation de données à caractère personnel concernant des données du Client, scryp la notifie au Client dans les meilleurs délais, et au plus tard dans les 48 heures après en avoir pris connaissance, par e-mail à l'adresse du compte scryp.

10.2 La notification contient, dans la mesure où ces éléments sont connus : la nature de la violation, les types de données concernés et le nombre approximatif de personnes concernées, les conséquences probables, les mesures prises et proposées ainsi qu'un point de contact chez scryp. scryp communique dans les meilleurs délais les informations qui ne sont pas encore disponibles.

10.3 scryp documente la violation et assiste le Client pour la notification à l'autorité de contrôle et la communication aux personnes concernées. scryp n'effectue de notifications aux autorités ou aux personnes concernées pour le compte du Client que sur instruction de celui-ci. La notification au Client ne constitue pas une reconnaissance de responsabilité.

11. Justificatifs et audits

11.1 scryp met à la disposition du Client toutes les informations nécessaires pour démontrer le respect des obligations prévues à l'art. 28 du RGPD. En font partie le présent accord, la description des mesures à l'annexe 2, le registre visé à l'art. 30, par. 2, du RGPD, les certifications des sous-traitants ultérieurs et des réponses écrites aux questions motivées du Client.

11.2 Si ces justificatifs ne suffisent pas dans un cas particulier, le Client peut procéder à un audit, y compris une inspection, lui-même ou par l'intermédiaire d'un auditeur tenu à la confidentialité et qui n'est pas un concurrent de

scryp. Les audits ont lieu au maximum une fois par année civile, moyennant un préavis d'au moins 30 jours, pendant les heures de bureau habituelles et sans perturbation de l'exploitation. En présence d'indices concrets d'une violation ou à la demande d'une autorité de contrôle, l'audit est également possible à bref délai et plus fréquemment.

11.3 L'audit ne s'étend ni aux données d'autres clients ni aux centres de données des sous-traitants ultérieurs. Pour ces derniers, leurs certifications et rapports d'audit font foi. Chaque Partie supporte ses propres frais d'audit.

12. Suppression et restitution des données

12.1 Pendant la durée du contrat, le Client peut à tout moment supprimer lui-même ses données et les exporter dans des formats courants. Les contenus supprimés sont immédiatement retirés des données actives.

12.2 scryp supprime automatiquement les fichiers originaux téléversés une fois le traitement terminé, en règle générale en quelques minutes et au plus tard 72 heures après le téléversement. Seuls sont conservés la version de lecture chiffrée, la transcription chiffrée et les analyses chiffrées.

12.3 Après la fin du contrat principal, les contenus restent à la disposition du Client pour exportation pendant 90 jours au maximum. Passé ce délai, scryp les supprime automatiquement, y compris toutes les copies. Si le Client supprime son compte, toutes les données sont supprimées immédiatement.

12.4 Les sauvegardes servent uniquement à la restauration de l'ensemble du système. Elles ne contiennent les contenus du Client que sous forme chiffrée et sont écrasées au plus tard après 30 jours. Aucune restauration de données individuelles du Client supprimées n'est effectuée à partir des sauvegardes.

12.5 Les données que scryp doit continuer à conserver en raison d'obligations légales de conservation (par exemple les données de facturation en vertu du § 132 BAO) sont exclues de la suppression. Elles sont bloquées et supprimées à l'expiration du délai.

12.6 Sur demande, scryp confirme la suppression par écrit ; un e-mail suffit.

13. Responsabilité

13.1 À l'égard des personnes concernées, les Parties sont responsables conformément à l'art. 82 du RGPD.

13.2 Dans les rapports entre les Parties, les dispositions du contrat principal relatives à la responsabilité s'appliquent dans la mesure permise par la loi. scryp répond des sous-traitants ultérieurs comme de son propre fait (point 7.4).

13.3 Si une Partie a versé une réparation à des personnes concernées, elle peut réclamer à l'autre Partie la part correspondant à la responsabilité de celle-ci dans le dommage (art. 82, par. 5, du RGPD).

13.4 Si le Client maintient une instruction bien que scryp l'ait informé de son illicéité conformément au point 3.3, le Client garantit scryp contre toutes les réclamations de tiers et amendes fondées sur cette instruction.

14. Durée, suspension et résiliation

14.1 Le présent accord s'applique aussi longtemps que scryp traite des données pour le Client, c'est-à-dire pendant la durée du contrat principal et jusqu'à l'achèvement de la suppression conformément au point 12.

14.2 L'utilisation du service sans le présent accord n'est pas prévue pour les clients visés au point 1.4. La résiliation du présent accord vaut donc également résiliation du contrat principal.

14.3 Si scryp enfreint le présent accord, le Client peut exiger que scryp suspende le traitement concerné jusqu'à ce qu'il soit remédié à la violation. Si scryp ne met pas fin à une violation grave dans un délai d'un mois à compter de la mise en demeure, le Client peut résilier le contrat principal sans préavis.

15. Dispositions finales

15.1 Le présent accord est conclu sous forme électronique (art. 28, par. 9, du RGPD). Pour les clients visés au point 1.4, il devient partie intégrante du contrat par son intégration dans les CGU lors de la conclusion du contrat principal ; la partie contractante est alors le titulaire du compte scryp, avec les informations qui y sont enregistrées. Il peut en outre être conclu par la signature du présent document par les deux Parties, y compris sous forme de copie électronique.

15.2 Toute modification du présent accord doit être faite par écrit ; un e-mail suffit. scryp peut adapter l'annexe 2 conformément au point 6.2 et l'annexe 3 conformément au point 7.2. scryp annonce les autres modifications par e-mail au moins 30 jours avant leur entrée en vigueur ; jusqu'à cette date, le Client peut s'y opposer et résilier le contrat principal avec effet à cette date. scryp conserve chaque version du présent accord avec son numéro de version et sa date.

15.3 Le droit autrichien s'applique, sans préjudice du RGPD. Si le Client est un professionnel, le tribunal matériellement compétent de Vienne est exclusivement compétent pour tous les litiges découlant du présent accord. Les compétences juridictionnelles impératives prévues par la loi demeurent réservées.

15.4 Si une disposition est invalide, le reste de l'accord demeure valable. La disposition invalide est remplacée par la règle légale qui se rapproche le plus de sa finalité.

15.5 Pour toutes les questions relatives au présent accord, le point de contact chez scryp est datenschutz@scryp.at. Du côté du Client, il s'agit de l'adresse e-mail du compte scryp, sauf indication contraire du Client.

15.6 scryp met le présent accord à disposition en plusieurs langues. La version allemande fait foi ; les traductions sont fournies à titre d'information. En cas de divergence, le texte allemand prévaut.

Signatures

Pour le Client	**Pour scryp**
Lieu, date	Lieu, date
Nom, fonction	Gökhan Sagir, entrepreneur individuel
Signature	Signature

Annexe 1 : Description du traitement

Point	Description
Objet	Fourniture du service scryp : transcription d'enregistrements audio et vidéo avec reconnaissance vocale et identification des locuteurs, dans la formule Ultra en outre les fonctionnalités d'IA (analyse assistée par IA : résumé, compte rendu, liste de tâches, texte pour les réseaux sociaux), ainsi que stockage, modification, exportation et partage des résultats.
Finalité	Le Client fait convertir en texte et analyser ses propres enregistrements, par exemple des réunions, des interviews, des dictées, des entretiens de conseil, des exposés ou des podcasts.
Nature du traitement	Réception de fichiers chiffrés, déchiffrement de courte durée dans la mémoire vive des serveurs de traitement, transcription et analyse automatiques, chiffrement des résultats, stockage chiffré, mise à disposition dans le compte du Client, suppression.
Types de données	Enregistrements vocaux et vidéos (voix, contenus parlés), transcriptions et analyses qui en sont issues, attributions des locuteurs, noms de fichiers et de dossiers attribués par le Client, métadonnées techniques (durée, taille du fichier, horodatages, langue détectée, état du traitement), pour les transcriptions partagées le lien de partage. Tous les contenus sont stockés sous forme chiffrée ; seules les métadonnées techniques existent en clair.
Catégories particulières (art. 9 du RGPD)	Possibles, selon le contenu des enregistrements du Client (par exemple des données de santé dans des dictées médicales, des informations échangées lors d'entretiens de conseil ou d'entretiens avec des mandants). scryp ne connaît pas le contenu. Le Client vérifie la licéité conformément au point 4.2.
Garanties pour les catégories particulières	Chiffrement dans le navigateur du Client, texte en clair uniquement dans la mémoire vive des serveurs propres de scryp à Vienne, aucune transmission de contenus en clair aux sous-traitants ultérieurs, aucun accès de personnes aux contenus en fonctionnement courant, obligation de secret conformément au point 5, aucun entraînement de modèles d'IA avec les données des clients.
Personnes concernées	Personnes qui s'expriment ou sont mentionnées dans les enregistrements (par exemple collaborateurs, clients, patients, mandants, personnes interviewées, participants à des réunions et à des événements), ainsi que les utilisateurs du compte du Client.
Lieux de traitement	Transcription et analyse par IA : serveurs GPU propres de scryp à Vienne, Autriche. Application web, interfaces, base de données, stockage de fichiers chiffré et sauvegardes : centre de données de Hetzner Online GmbH à Nuremberg, Allemagne.
Durée	Durée du contrat principal, augmentée des délais de suppression prévus au point 12.

Annexe 2 : Mesures techniques et organisationnelles (art. 32 du RGPD)

État au 22 septembre 2026. Les mesures décrivent le fonctionnement normal de scryp.

1. Chiffrement et architecture « zero-knowledge »

- Les enregistrements sont chiffrés avec AES-256-GCM dès le navigateur du Client, avant d'être transmis à scryp. Une clé de fichier (FEK) distincte est générée pour chaque fichier.
- Les clés de fichier sont chiffrées avec une clé principale du compte (MEK). La clé principale n'est accessible qu'avec le mot de passe du Client (dérivation par PBKDF2-SHA256, 600 000 itérations). scryp ne connaît ni le mot de passe ni la clé principale en clair.
- Pour la transcription, le navigateur transmet à scryp la clé de fichier chiffrée avec une clé serveur (RSA-4096, OAEP). Le serveur de traitement déchiffre l'enregistrement exclusivement dans la mémoire vive. Les fichiers temporaires se trouvent dans un système de fichiers en mémoire vive et sont rejetés à l'issue de la tâche ; les contenus non chiffrés ne sont à aucun moment écrits sur un support de stockage.
- Les transcriptions et analyses sont chiffrées avec la clé de fichier immédiatement après leur création et ne sont stockées que sous forme chiffrée. Les noms de fichiers et de dossiers sont chiffrés dans le navigateur.
- Lors du partage d'une transcription, la clé de fichier est chiffrée avec une clé dérivée du mot de passe de partage. Les destinataires déchiffrent exclusivement dans leur propre navigateur.
- Exception pour le téléversement par URL : si le Client récupère un enregistrement à partir d'une adresse internet, le serveur de traitement télécharge directement le fichier, le traite dans la mémoire vive, puis le supprime ; la transcription et la version de lecture sont stockées sous forme chiffrée, comme à l'accoutumée.
- Toutes les connexions sont chiffrées avec TLS 1.2 ou 1.3.

2. Contrôle de l'accès physique

- L'application web, la base de données, le stockage de fichiers et les sauvegardes fonctionnent dans le centre de données de Hetzner Online GmbH à Nuremberg (certifié ISO/IEC 27001, attestation BSI C5 de type 2), avec contrôle d'accès physique, vidéosurveillance et personnel de sécurité de l'exploitant.
- Les serveurs GPU destinés à la transcription et à l'analyse par IA se trouvent dans des locaux propres et fermés de scryp à Vienne. Seules les personnes autorisées y ont accès ; l'accès est verrouillé mécaniquement et sécurisé en outre par un contrôle biométrique.
- Tous les supports de stockage de ces serveurs sont intégralement chiffrés. En cas de vol ou de retrait d'un support de stockage, les données restent illisibles sans la clé. Sur ces serveurs, les contenus non chiffrés n'existent que dans la mémoire vive pendant l'exécution d'une tâche et ne sont jamais écrits sur un support de stockage.

3. Contrôle de l'accès aux systèmes et aux données

- Accès aux serveurs réservé aux administrateurs de scryp via des connexions SSH chiffrées avec des clés personnelles ou des mots de passe forts générés aléatoirement ; accès selon le principe du moindre privilège.
- Interface d'administration distincte avec authentification propre, limitée aux adresses IP autorisées. L'interface d'administration n'affiche que les métadonnées de compte et de tâche, jamais de contenus.
- Comptes utilisateurs : les mots de passe sont hachés avec Argon2id ; protection contre les tentatives de connexion par limitation du débit et blocage temporaire ; les sessions fonctionnent sans cookies, avec des jetons à courte durée de vie.
- Protection des interfaces contre les abus et la surcharge par limitation du débit et blocages automatiques.

- Les services automatisés (serveurs de traitement) s'authentifient avec des identifiants propres, pouvant faire l'objet d'une rotation, et ne reçoivent que les clés nécessaires à la tâche concernée.

4. Contrôle de la séparation et pseudonymisation

- Séparation cryptographique : chaque client dispose de sa propre clé principale, chaque fichier de sa propre clé de fichier. Les contenus d'un client ne sont pas lisibles avec les clés d'un autre.
- Séparation logique des systèmes de production, de base de données, de cache et de surveillance dans des zones réseau distinctes.
- Les tâches de traitement transmises aux serveurs GPU ne contiennent ni noms ni adresses e-mail, uniquement les données techniques nécessaires à la tâche.

5. Intégrité et traçabilité

- Toutes les modifications de l'application et de l'infrastructure sont effectuées au moyen d'un code source versionné et d'un déploiement automatisé et traçable ; les images logicielles sont fixées par leur somme de contrôle.
- Les événements de compte (par exemple connexion, suppression, modifications d'abonnement) sont journalisés avec horodatage, sans adresses IP.
- Les journaux système ne contiennent aucun contenu et sont supprimés après 14 jours. Les adresses IP ne sont ni stockées ni journalisées. Pour la prévention des abus, les accès sont uniquement comptabilisés au moyen d'un pseudonyme à courte durée de vie, formé à l'aide d'une clé secrète et non réversible, qui expire après une heure au maximum.

6. Disponibilité et résilience

- Cluster à haute disponibilité composé de trois serveurs avec répartition de charge ; base de données avec réplication synchrone sur trois nœuds ; cache avec basculement automatique.
- Sauvegarde quotidienne chiffrée de la base de données avec restauration possible à tout instant des 30 derniers jours ; configuration du cluster sauvegardée toutes les six heures. Les sauvegardes se trouvent dans le centre de données de Nuremberg.
- Déploiement de nouvelles versions sans interruption de service ; protection contre les attaques par saturation au niveau du réseau et de l'application.
- Surveillance continue avec alerte automatique en cas d'incident.

7. Suppression et minimisation des données

- Les fichiers originaux téléversés sont supprimés après le traitement, en règle générale en quelques minutes ; une règle automatique élimine les téléversements restés en attente au plus tard après 72 heures.
- Le Client supprime lui-même ses contenus et son compte à tout moment ; la suppression prend effet immédiatement dans les données actives. Après la fin d'un abonnement, les contenus sont supprimés automatiquement au bout de 90 jours.
- Aucun cookie, aucun outil de suivi ou d'analyse de tiers, aucun stockage d'adresses IP.

8. Organisation

- Toutes les personnes travaillant chez scryp sont tenues au secret des données et à la confidentialité et ont été formées à l'architecture de sécurité.

- scryp tient un registre des activités de traitement (art. 30 du RGPD). L'analyse d'impact relative à la protection des données, le registre et les présentes mesures sont réexaminés au moins une fois par an et lors de toute modification substantielle.
- Processus de gestion des incidents : détection par la surveillance, évaluation, confinement, notification aux clients concernés conformément au point 10 de l'accord, analyse a posteriori.
- Les sous-traitants ultérieurs sont contrôlés quant à leurs garanties avant leur intervention et engagés contractuellement conformément à l'art. 28, par. 4, du RGPD.

Annexe 3 : Sous-traitants ultérieurs

État au 22 septembre 2026.

Sous-traitant ultérieur	Prestation	Données	Lieu du traitement	Garantie
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Allemagne	Exploitation des serveurs pour l'application web, les interfaces et la base de données ; stockage d'objets chiffré ; sauvegardes	Toutes les données mentionnées à l'annexe 1, contenus exclusivement chiffrés	Nuremberg, Allemagne (UE)	Accord de traitement des données ; ISO/IEC 27001 ; BSI C5
Mailjet GmbH (groupe Sinch), Alt Moabit 2, 10557 Berlin, Allemagne	Envoi d'e-mails système (par exemple la notification « Transcription terminée »)	Adresse e-mail du compte, date de la tâche, lien vers le compte ; aucun contenu, aucun nom de fichier	France (UE)	Accord de traitement des données ; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, Irlande	Réception et traitement des demandes d'assistance par e-mail (Microsoft 365)	Uniquement les données que le Client transmet lui-même dans une demande d'assistance	UE ; accès à distance depuis des pays tiers possible	Accord de traitement des données ; clauses contractuelles types de l'UE ; cadre de protection des données UE-États-Unis (DPF)