Acuerdo de encargo del tratamiento (DPA)

conforme al art. 28 del Reglamento General de Protección de Datos (RGPD)

Version 1.0, a fecha de 22 de septiembre de 2026

Partes

Cliente (responsable del tratamiento en el sentido del art. 4.7 del RGPD):

Empresa / Nombre: _____

Dirección: _____

Correo electrónico de la cuenta de scryp: _____

scryp (encargado del tratamiento en el sentido del art. 4.8 del RGPD):

Gökhan Sagir, empresario individual, que actúa bajo la marca scryp
Erdbergstraße 121/9, 1030 Wien, Österreich
UID: ATU83108129
Contacto de protección de datos: datenschutz@scryp.at

En lo sucesivo, el «Cliente» y «scryp», conjuntamente las «Partes».

De qué se trata

El Cliente utiliza scryp para que sus grabaciones de audio y vídeo sean transcritas y analizadas. En esas grabaciones hablan personas de cuyos datos personales es responsable el Cliente. scryp trata esos datos únicamente por encargo del Cliente. El presente acuerdo establece qué puede hacer scryp con los datos, cómo los protege scryp y qué ocurre con ellos al final.

1. Objeto y ámbito de aplicación

1.1 El presente acuerdo se aplica a todos los datos personales que scryp trata por encargo del Cliente al prestar el servicio scryp conforme a los Términos del servicio (AGB, disponibles en www.scryp.at/agb). El contrato sobre el uso del servicio se denomina en lo sucesivo «Contrato principal». La versión vigente del presente acuerdo puede consultarse en www.scryp.at/avv.

1.2 No son objeto del presente acuerdo los datos de la propia relación contractual, es decir, los datos de cuenta, contrato, facturación y asistencia del Cliente. scryp trata estos datos como responsable del tratamiento por derecho propio, conforme a su Política de privacidad (www.scryp.at/datenschutz).

1.3 Los Anexos 1 a 3 forman parte integrante del presente acuerdo. En caso de contradicción entre el presente acuerdo y el Contrato principal, prevalecerá el presente acuerdo en materia de protección de datos.

1.4 El presente acuerdo está destinado a los Clientes que utilizan scryp en el marco de una actividad profesional, empresarial o de autoridad pública. En caso de uso puramente privado, el RGPD no es aplicable conforme a su art. 2.2.c), y no se requiere un contrato de encargo del tratamiento.

2. Naturaleza, finalidad y alcance del tratamiento

2.1 La naturaleza y la finalidad del tratamiento, los tipos de datos y las categorías de interesados se describen en el Anexo 1.

2.2 scryp trata los datos exclusivamente en Estados miembros de la Unión Europea. Los lugares de tratamiento se indican en el Anexo 1 y en el Anexo 3.

2.3 La duración del tratamiento corresponde a la vigencia del Contrato principal más los plazos de supresión regulados en la cláusula 12.

3. Instrucciones

3.1 scryp trata los datos únicamente siguiendo instrucciones documentadas del Cliente. Las instrucciones del Cliente son el Contrato principal, el presente acuerdo y el uso de las funciones del servicio por parte del Cliente (en particular, cargar, transcribir, analizar, editar, compartir, exportar y eliminar). Cada uso de una función constituye una instrucción individual documentada de ejecutar el tratamiento correspondiente.

3.2 El Cliente impartirá otras instrucciones por escrito; basta un correo electrónico a datenschutz@scryp.at. Están facultados para impartir instrucciones el titular de la cuenta y las personas que el Cliente emplee para su cuenta de scryp. Las instrucciones que excedan el alcance de las prestaciones del servicio se considerarán una solicitud de modificación de las prestaciones.

3.3 Si, a juicio de scryp, una instrucción infringe el RGPD u otras disposiciones en materia de protección de datos, scryp informará de ello al Cliente sin dilación. scryp podrá suspender su ejecución hasta que el Cliente confirme o modifique la instrucción.

3.4 scryp no utiliza los datos para fines propios. En particular, las grabaciones, transcripciones y análisis del Cliente no se utilizan para entrenar ni mejorar modelos de IA ni se comunican a terceros, salvo que el presente acuerdo disponga otra cosa.

3.5 Si una autoridad o un tribunal exige a scryp la entrega de datos del Cliente, scryp informará al Cliente sin dilación, en la medida en que ello sea legalmente admisible, remitirá a dicho organismo al Cliente y entregará únicamente aquello a lo que scryp esté legalmente obligado. Al hacerlo, scryp comprobará si una obligación legal de secreto del Cliente se opone a la entrega (§ 6, apartado 5, de la DSG).

4. Obligaciones del Cliente

4.1 El Cliente es responsable de la licitud de las grabaciones y de su tratamiento. En particular, se asegura de que exista una base jurídica (art. 6 y, en el caso de categorías especiales, art. 9 del RGPD), de que se informe a los interesados (arts. 13 y 14 del RGPD) y de que no se graben manifestaciones no públicas sin el consentimiento de las personas que hablan (por ejemplo, § 120 del StGB en Austria).

4.2 Si las grabaciones contienen categorías especiales de datos personales (por ejemplo, datos relativos a la salud) o contenidos sujetos al secreto profesional, el Cliente comprobará previamente si el tratamiento es admisible y si se requiere una evaluación de impacto relativa a la protección de datos (art. 35 del RGPD). scryp facilita para ello la información contenida en el presente acuerdo y en sus Anexos.

4.3 El Cliente mantendrá actualizada la dirección de correo electrónico de su cuenta de scryp. scryp dirigirá a esa dirección todas las comunicaciones previstas en el presente acuerdo, en particular las notificaciones conforme a la cláusula 10.

4.4 El Cliente tiene derecho a impartir instrucciones a scryp, a exigir pruebas y a realizar auditorías conforme a la cláusula 11.

5. Confidencialidad y secreto profesional

5.1 scryp permite el acceso a los datos únicamente a personas que se hayan comprometido a respetar el secreto de los datos (§ 6 de la DSG) y la confidencialidad y que hayan sido instruidas sobre las consecuencias de una infracción (art. 28.3.b) y art. 29 del RGPD). Esta obligación subsiste tras la finalización de la actividad.

5.2 scryp está diseñado de modo que los contenidos del Cliente (grabaciones, transcripciones, análisis, nombres de archivos y de carpetas) se almacenan únicamente cifrados y solo existen en texto plano en la memoria RAM de los servidores de procesamiento durante el tiempo que dura el tratamiento correspondiente. Las personas de scryp no tienen acceso a los contenidos en texto plano durante el funcionamiento ordinario. Los detalles figuran en el Anexo 2.

5.3 Si el Cliente está sujeto a una obligación legal de secreto (por ejemplo, § 9 de la RAO, § 54 de la ÄrzteG, § 121 del StGB), scryp se compromete, en calidad de auxiliar del Cliente, a mantener en secreto del mismo modo todos los contenidos a los que scryp tenga acceso en el marco de la prestación. Para los Clientes sujetos al Derecho alemán, esto constituye asimismo una obligación de secreto conforme al § 203, apartado 4, del StGB (Alemania). A petición, scryp confirmará esta obligación en una declaración separada.

6. Seguridad del tratamiento

6.1 scryp aplica las medidas técnicas y organizativas conforme al art. 32 del RGPD que se describen en el Anexo 2.

6.2 scryp podrá seguir desarrollando estas medidas y sustituirlas por otras equivalentes o mejores. El nivel de protección no podrá verse reducido. scryp documentará las modificaciones sustanciales y las comunicará al Cliente. La versión vigente del Anexo 2 puede consultarse en www.scryp.at/avv.

6.3 scryp verifica la eficacia de las medidas al menos una vez al año y comunica el resultado al Cliente a petición de este.

7. Subencargados del tratamiento

7.1 El Cliente autoriza a los subencargados del tratamiento indicados en el Anexo 3 (autorización general conforme al art. 28.2 del RGPD).

7.2 Si scryp desea añadir o sustituir un subencargado del tratamiento, informará al Cliente al menos 30 días antes de su intervención por correo electrónico a la dirección de la cuenta de scryp. El Cliente podrá oponerse por escrito, por motivos importantes relacionados con la protección de datos, dentro de los 14 días siguientes a la recepción de dicha comunicación; basta un correo electrónico. Si el Cliente no se opone, la modificación se considerará autorizada.

7.3 Si las Partes no encuentran una solución tras una oposición, el Cliente podrá resolver el Contrato principal con efectos a la fecha prevista de la intervención. scryp reembolsará proporcionalmente las cuotas que el Cliente haya pagado por adelantado para el periodo posterior a la terminación.

7.4 scryp impone contractualmente a cada subencargado del tratamiento las mismas obligaciones en materia de protección de datos que incumben a scryp en virtud del presente acuerdo, en particular garantías suficientes de aplicar medidas técnicas y organizativas apropiadas (art. 28.4 del RGPD). Si un subencargado del tratamiento incumple sus obligaciones, scryp responderá ante el Cliente de las obligaciones de dicho subencargado como de su propia conducta.

7.5 Las prestaciones accesorias sin acceso a los datos del Cliente, por ejemplo telecomunicaciones, limpieza o mantenimiento sin acceso a los datos, no constituyen un subencargo del tratamiento.

8. Lugar del tratamiento y terceros países

8.1 scryp trata y almacena los datos en Austria y Alemania. scryp no realiza transferencias a países situados fuera de la Unión Europea o del Espacio Económico Europeo.

8.2 Si un subencargado del tratamiento tratara datos en un tercer país, ello se producirá únicamente en el alcance descrito en el Anexo 3 y solo con una garantía adecuada conforme al capítulo V del RGPD (por ejemplo, una decisión de adecuación de la Comisión Europea o las cláusulas contractuales tipo de la UE).

9. Asistencia al Cliente

9.1 Derechos de los interesados: el Cliente puede atender por sí mismo, en la mayoría de los casos, las solicitudes de acceso, rectificación, supresión y portabilidad de los datos mediante las funciones del servicio (visualizar, editar, exportar, eliminar). Dado que scryp conserva los contenidos únicamente cifrados, scryp no puede determinar qué personas aparecen en una grabación. Si un interesado se dirige a scryp, scryp remitirá la solicitud al Cliente sin dilación y no la responderá por sí mismo, salvo que el Cliente le dé instrucciones en tal sentido.

9.2 Seguridad, violaciones de la seguridad de los datos, evaluación de impacto relativa a la protección de datos y consulta a la autoridad de control (arts. 32 a 36 del RGPD): scryp asiste al Cliente con la información de que scryp dispone, en particular con el presente acuerdo, el Anexo 2 y los datos sobre un incidente conforme a la cláusula 10.

9.3 scryp podrá, previo aviso, exigir una remuneración razonable en función del esfuerzo por la asistencia que exceda de la puesta a disposición de la información y de las funciones descritas en el presente acuerdo. Esto no se aplica cuando la asistencia sea necesaria a causa de un error de scryp.

10. Notificación de violaciones de la seguridad de los datos personales

10.1 Si scryp tiene conocimiento de una violación de la seguridad de los datos personales que afecte a datos del Cliente, scryp la notificará al Cliente sin dilación indebida y, a más tardar, en el plazo de 48 horas desde que tenga conocimiento de ella, por correo electrónico a la dirección de la cuenta de scryp.

10.2 La notificación incluirá, en la medida en que se conozcan: la naturaleza de la violación, los tipos de datos afectados y el número aproximado de interesados, las consecuencias probables, las medidas adoptadas y propuestas y un punto de contacto en scryp. scryp facilitará sin dilación indebida la información de la que aún no disponga.

10.3 scryp documentará la violación y asistirá al Cliente en la notificación a la autoridad de control y en la comunicación a los interesados. scryp solo efectuará notificaciones a autoridades o comunicaciones a interesados en nombre del Cliente siguiendo instrucciones de este. La notificación al Cliente no constituye un reconocimiento de culpa.

11. Pruebas y auditorías

11.1 scryp pone a disposición del Cliente toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el art. 28 del RGPD. Ello incluye el presente acuerdo, la descripción de las medidas del Anexo 2, el registro conforme al art. 30.2 del RGPD, las certificaciones de los subencargados del tratamiento y respuestas escritas a las preguntas fundadas del Cliente.

11.2 Si en un caso concreto estas pruebas no fueran suficientes, el Cliente podrá realizar una auditoría, incluidas inspecciones, por sí mismo o a través de un auditor sujeto a confidencialidad que no sea competidor de scryp. Las auditorías se realizarán como máximo una vez por año natural, con un preaviso de al menos 30 días, durante el horario comercial habitual y sin perturbar el funcionamiento. En caso de indicios concretos de una infracción o a

requerimiento de una autoridad de control, la auditoría también podrá realizarse a corto plazo y con mayor frecuencia.

11.3 La auditoría no se extiende a los datos de otros clientes ni a los centros de datos de los subencargados del tratamiento. Para estos rigen sus certificaciones e informes de auditoría. Cada Parte asumirá sus propios costes de la auditoría.

12. Supresión y devolución de los datos

12.1 Durante la vigencia del contrato, el Cliente puede eliminar por sí mismo sus datos en cualquier momento y exportarlos en formatos habituales. Los contenidos eliminados se retiran de inmediato del conjunto de datos activo.

12.2 scryp elimina automáticamente los archivos originales cargados una vez concluido el tratamiento, por regla general en pocos minutos y, a más tardar, 72 horas después de la carga. Solo se conservan la versión de reproducción cifrada, la transcripción cifrada y los análisis cifrados.

12.3 Tras la finalización del Contrato principal, los contenidos permanecen a disposición del Cliente para su exportación durante un máximo de 90 días. Transcurrido ese plazo, scryp los elimina automáticamente, incluidas todas las copias. Si el Cliente elimina su cuenta, todos los datos se eliminan de inmediato.

12.4 Las copias de seguridad sirven únicamente para restaurar el sistema en su conjunto. Contienen los contenidos del Cliente exclusivamente cifrados y se sobrescriben a más tardar a los 30 días. No se realiza ninguna restauración de datos individuales de clientes eliminados a partir de copias de seguridad.

12.5 Quedan excluidos de la supresión los datos que scryp deba seguir conservando en virtud de obligaciones legales de conservación (por ejemplo, los datos de facturación conforme al § 132 de la BAO). Dichos datos se bloquean y se eliminan una vez transcurrido el plazo.

12.6 A petición, scryp confirmará la supresión por escrito; basta un correo electrónico.

13. Responsabilidad

13.1 Frente a los interesados, las Partes responden conforme al art. 82 del RGPD.

13.2 En la relación entre las Partes se aplican las disposiciones sobre responsabilidad del Contrato principal, en la medida en que la ley lo permita. scryp responde de los subencargados del tratamiento como de su propia conducta (cláusula 7.4).

13.3 Si una Parte ha abonado una indemnización a los interesados, podrá reclamar a la otra Parte la parte que corresponda a la cuota de responsabilidad de esta en el daño (art. 82.5 del RGPD).

13.4 Si el Cliente mantiene una instrucción a pesar de que scryp le ha advertido de su ilicitud conforme a la cláusula 3.3, el Cliente mantendrá indemne a scryp frente a todas las reclamaciones de terceros y multas que se basen en dicha instrucción.

14. Duración, suspensión y terminación

14.1 El presente acuerdo rige mientras scryp trate datos para el Cliente, es decir, durante la vigencia del Contrato principal y hasta que concluya la supresión conforme a la cláusula 12.

14.2 No está previsto que los Clientes a que se refiere la cláusula 1.4 utilicen el servicio sin el presente acuerdo. Por ello, la resolución del presente acuerdo se considera al mismo tiempo resolución del Contrato principal.

14.3 Si scryp infringe el presente acuerdo, el Cliente podrá exigir que scryp suspenda el tratamiento afectado hasta que se subsane la infracción. Si scryp no pone fin a una infracción grave en el plazo de un mes desde el requerimiento, el Cliente podrá resolver el Contrato principal sin preaviso.

15. Disposiciones finales

15.1 El presente acuerdo se celebra en forma electrónica (art. 28.9 del RGPD). Para los Clientes a que se refiere la cláusula 1.4, pasa a formar parte del contrato mediante su incorporación a los Términos del servicio con la celebración del Contrato principal; en ese caso, la parte contratante es el titular de la cuenta de scryp con los datos allí registrados. Además, puede celebrarse mediante la firma del presente documento por ambas Partes, también en forma de copia electrónica.

15.2 Las modificaciones del presente acuerdo requieren la forma escrita; basta un correo electrónico. scryp podrá adaptar el Anexo 2 conforme a la cláusula 6.2 y el Anexo 3 conforme a la cláusula 7.2. scryp anunciará otras modificaciones por correo electrónico al menos 30 días antes de su entrada en vigor; hasta entonces, el Cliente podrá oponerse y resolver el Contrato principal con efectos a esa fecha. scryp conserva cada versión del presente acuerdo con número de versión y fecha.

15.3 Se aplica el Derecho austriaco; el RGPD no se ve afectado. Si el Cliente es empresario, para todos los litigios derivados del presente acuerdo será exclusivamente competente el tribunal de Viena competente por razón de la materia. Los fueros legales imperativos no se ven afectados.

15.4 Si alguna disposición fuera inválida, el resto del acuerdo conservará su validez. La disposición inválida será sustituida por la regulación legal que más se aproxime a su finalidad.

15.5 La persona de contacto para todas las cuestiones relativas al presente acuerdo es, por parte de scryp, datenschutz@scryp.at. Por parte del Cliente, lo es la dirección de correo electrónico de la cuenta de scryp, salvo que el Cliente comunique otra cosa.

15.6 scryp pone a disposición el presente acuerdo en varios idiomas. La versión alemana es la vinculante; las traducciones se facilitan únicamente a efectos de comprensión. En caso de discrepancia, prevalecerá el texto alemán.

Firmas

Por el Cliente	**Por scryp**
Lugar, fecha	Lugar, fecha
Nombre, cargo	Gökhan Sagir, empresario individual
Firma	Firma

Anexo 1: Descripción del tratamiento

Punto	Descripción
Objeto	Prestación del servicio scryp: transcripción de grabaciones de audio y vídeo con reconocimiento de voz e identificación de hablantes; en el plan Ultra, además, funciones de IA (análisis asistido por IA: resumen, acta, lista de tareas, texto para redes sociales), así como almacenamiento, edición, exportación y uso compartido de los resultados.
Finalidad	El Cliente hace convertir en texto y analizar sus propias grabaciones, por ejemplo reuniones, entrevistas, dictados, conversaciones de asesoramiento, ponencias o pódcast.
Naturaleza del tratamiento	Recepción de archivos cifrados, descifrado breve en la memoria RAM de los servidores de procesamiento, transcripción y análisis automáticos, cifrado de los resultados, almacenamiento cifrado, puesta a disposición en la cuenta del Cliente, supresión.
Tipos de datos	Grabaciones de voz y vídeos (voz, contenidos hablados), las transcripciones y los análisis generados a partir de ellos, asignaciones de hablantes, nombres de archivos y de carpetas asignados por el Cliente, metadatos técnicos (duración, tamaño del archivo, marcas de tiempo, idioma detectado, estado del tratamiento) y, en el caso de transcripciones compartidas, el enlace para compartir. Todos los contenidos se almacenan cifrados; solo los metadatos técnicos existen en texto plano.
Categorías especiales (art. 9 del RGPD)	Posibles, en función del contenido de las grabaciones del Cliente (por ejemplo, datos relativos a la salud en dictados médicos, información de conversaciones de asesoramiento o con mandantes). scryp desconoce el contenido. El Cliente comprueba la admisibilidad conforme a la cláusula 4.2.
Garantías para las categorías especiales	Cifrado en el navegador del Cliente, texto plano únicamente en la memoria RAM de los servidores propios de scryp en Viena, ninguna comunicación de contenidos en texto plano a subencargados del tratamiento, ningún acceso de personas a los contenidos durante el funcionamiento ordinario, obligación de secreto conforme a la cláusula 5, ningún entrenamiento de modelos de IA con datos de clientes.
Interesados	Personas que hablan o son mencionadas en las grabaciones (por ejemplo, empleados, clientes, pacientes, mandantes, entrevistados, participantes en reuniones y eventos), así como los usuarios de la cuenta del Cliente.
Lugares de tratamiento	Transcripción y análisis de IA: servidores GPU propios de scryp en Viena, Austria. Aplicación web, interfaces, base de datos, almacenamiento cifrado de archivos y copias de seguridad: centro de datos de Hetzner Online GmbH en Núremberg, Alemania.
Duración	Vigencia del Contrato principal más los plazos de supresión conforme a la cláusula 12.

Anexo 2: Medidas técnicas y organizativas (art. 32 del RGPD)

A fecha de 22 de septiembre de 2026. Las medidas describen el funcionamiento ordinario de scryp.

1. Cifrado y arquitectura de conocimiento cero (Zero-Knowledge)

- Las grabaciones se cifran ya en el navegador del Cliente con AES-256-GCM antes de transmitirse a scryp. Para cada archivo se genera una clave de archivo propia (FEK).
- Las claves de archivo se cifran con una clave maestra de la cuenta (MEK). La clave maestra solo es accesible con la contraseña del Cliente (derivación con PBKDF2-SHA256, 600.000 iteraciones). scryp no conoce en texto plano ni la contraseña ni la clave maestra.
- Para la transcripción, el navegador transmite a scryp la clave de archivo cifrada con una clave del servidor (RSA-4096, OAEP). El servidor de procesamiento descifra la grabación exclusivamente en la memoria RAM. Los archivos temporales residen en un sistema de archivos en RAM y se descartan una vez finalizado el encargo; los contenidos sin cifrar no se escriben en ningún momento en soportes de datos.
- Las transcripciones y los análisis se cifran con la clave de archivo inmediatamente después de su creación y se almacenan únicamente cifrados. Los nombres de archivos y de carpetas se cifran en el navegador.
- Al compartir una transcripción, la clave de archivo se cifra con una clave derivada de la contraseña para compartir. Los destinatarios descifran exclusivamente en su propio navegador.
- Excepción para la carga mediante URL: si el Cliente obtiene una grabación a través de una dirección de internet, el servidor de procesamiento descarga el archivo directamente, lo procesa en la memoria RAM y lo elimina a continuación; la transcripción y la versión de reproducción se almacenan cifradas como de costumbre.
- Todas las conexiones están cifradas con TLS 1.2 o 1.3.

2. Control de acceso físico

- La aplicación web, la base de datos, el almacenamiento de archivos y las copias de seguridad funcionan en el centro de datos de Hetzner Online GmbH en Núremberg (certificado según ISO/IEC 27001, atestación BSI C5 de tipo 2), con control de acceso físico, videovigilancia y personal de seguridad del operador.
- Los servidores GPU para la transcripción y el análisis de IA se encuentran en salas propias y cerradas de scryp en Viena. Solo tienen acceso las personas autorizadas; el acceso está cerrado mecánicamente y protegido adicionalmente mediante sistemas biométricos.
- Todos los soportes de datos de estos servidores están completamente cifrados. En caso de robo o extracción de un soporte de datos, los datos permanecen ilegibles sin la clave. En estos servidores, los contenidos sin cifrar solo existen en la memoria RAM durante un encargo en curso y nunca se escriben en un soporte de datos.

3. Control de acceso a los sistemas y a los datos

- Acceso a los servidores únicamente para los administradores de scryp mediante conexiones SSH cifradas con claves personales o contraseñas seguras generadas aleatoriamente; acceso conforme al principio de mínimo privilegio.
- Interfaz de administración separada con inicio de sesión propio, restringida a direcciones IP autorizadas. La interfaz de administración muestra únicamente metadatos de cuentas y encargos, no contenidos.
- Cuentas de usuario: las contraseñas se almacenan como hash con Argon2id; protección frente a intentos de inicio de sesión mediante limitación de tasa y bloqueo temporal; las sesiones funcionan sin cookies, con tokens de corta duración.

- Protección de las interfaces frente a abusos y sobrecargas mediante limitación de tasa y bloqueos automáticos.
- Los servicios automatizados (servidores de procesamiento) se autentican con credenciales propias y rotables y reciben únicamente las claves necesarias para el encargo correspondiente.

4. Control de separación y seudonimización

- Separación criptográfica: cada Cliente tiene su propia clave maestra y cada archivo su propia clave de archivo. Los contenidos de un Cliente no pueden leerse con claves ajenas.
- Separación lógica de los sistemas de producción, base de datos, caché y supervisión en zonas de red separadas.
- Los encargos de procesamiento enviados a los servidores GPU no contienen nombres ni direcciones de correo electrónico, solo los datos técnicos necesarios para el encargo.

5. Integridad y trazabilidad

- Todas las modificaciones de la aplicación y de la infraestructura se realizan mediante código fuente versionado y despliegues automatizados y trazables; las imágenes de software se fijan mediante su suma de comprobación.
- Los eventos de la cuenta (por ejemplo, inicio de sesión, eliminación, cambios de suscripción) se registran con marca de tiempo, sin direcciones IP.
- Los registros del sistema no contienen contenidos y se eliminan a los 14 días. Las direcciones IP no se almacenan ni se registran. Para prevenir abusos, los accesos se contabilizan únicamente mediante un seudónimo de corta duración, generado con una clave secreta y no reversible, que caduca como máximo al cabo de una hora.

6. Disponibilidad y resiliencia

- Clúster de alta disponibilidad de tres servidores con balanceo de carga; base de datos con replicación síncrona en tres nodos; caché con conmutación automática por error.
- Copia de seguridad cifrada diaria de la base de datos con restauración a cualquier momento de los últimos 30 días; la configuración del clúster se respalda cada seis horas. Las copias de seguridad se encuentran en el centro de datos de Núremberg.
- Despliegue de nuevas versiones sin interrupción del servicio; protección frente a ataques de sobrecarga a nivel de red y de aplicación.
- Supervisión continua con alertas automáticas en caso de incidencias.

7. Supresión y minimización de datos

- Los archivos originales cargados se eliminan tras el tratamiento, por regla general en pocos minutos; una regla automática elimina las cargas que hayan quedado pendientes a más tardar a las 72 horas.
- El Cliente elimina por sí mismo los contenidos y la cuenta en cualquier momento; la eliminación surte efecto de inmediato en el conjunto de datos activo. Tras la finalización de una suscripción, los contenidos se eliminan automáticamente a los 90 días.
- Sin cookies, sin herramientas de seguimiento o análisis de terceros, sin almacenamiento de direcciones IP.

8. Organización

- Todas las personas que trabajan en scryp están obligadas a respetar el secreto de los datos y la confidencialidad y han sido instruidas en la arquitectura de seguridad.

- scryp lleva un registro de las actividades de tratamiento (art. 30 del RGPD). La evaluación de impacto relativa a la protección de datos, el registro y estas medidas se revisan al menos una vez al año y en caso de modificaciones sustanciales.
- Proceso de gestión de incidentes: detección mediante supervisión, evaluación, contención, notificación a los Clientes afectados conforme a la cláusula 10 del acuerdo, seguimiento posterior.
- Los subencargados del tratamiento se examinan en cuanto a sus garantías antes de su intervención y se obligan contractualmente conforme al art. 28.4 del RGPD.

Anexo 3: Subencargados del tratamiento

A fecha de 22 de septiembre de 2026.

Subencargado del tratamiento	Prestación	Datos	Lugar del tratamiento	Garantía
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland	Explotación de los servidores para la aplicación web, las interfaces y la base de datos; almacenamiento de objetos cifrado; copias de seguridad	Todos los datos indicados en el Anexo 1, contenidos exclusivamente cifrados	Núremberg, Alemania (UE)	Contrato de encargo del tratamiento; ISO/IEC 27001; BSI C5
Mailjet GmbH (Sinch-Konzern), Alt Moabit 2, 10557 Berlin, Deutschland	Envío de correos electrónicos del sistema (por ejemplo, la notificación «Transcripción finalizada»)	Dirección de correo electrónico de la cuenta, fecha del encargo, enlace a la cuenta; sin contenidos, sin nombres de archivos	Francia (UE)	Contrato de encargo del tratamiento; ISO/IEC 27001
Microsoft Ireland Operations Ltd., Dublin, Irland	Recepción y gestión de solicitudes de asistencia por correo electrónico (Microsoft 365)	Únicamente los datos que el propio Cliente transmite en una solicitud de asistencia	UE; posible acceso remoto desde terceros países	Contrato de encargo del tratamiento; cláusulas contractuales tipo de la UE; Marco de Privacidad de Datos UE-EE. UU.