Auftragsverarbeitungsvertrag

Verarbeitung personenbezogener Daten im Auftrag, Art. 28 DSGVO
Processing of personal data on behalf of a controller, Art. 28 GDPR

Produkt	Schwärzwerk, Betrieb durch Respeak (gehostete Betriebsart)
Auftragnehmer	Respeak GmbH, Kaiserstraße 89–93, 76133 Karlsruhe
Ansprechpartner	Dr. Tim Rietz, Geschäftsführer
Dokument	Fassung 1.2
Stand	28.10.2026

Dieser Vertrag wird geschlossen zwischen

.....
.....
.....

vertreten durch .....

Name und Anschrift der Behörde oder des Unternehmens

nachfolgend „Auftraggeber“

und

Respeak GmbH, Kaiserstraße 89–93, 76133 Karlsruhe, Deutschland, eingetragen im Handelsregister des Amtsgerichts Mannheim unter HRB 741830, vertreten durch den Geschäftsführer Dr. Tim Rietz

nachfolgend „Auftragnehmer“

nachfolgend einzeln „Partei“ und gemeinsam „die Parteien“.

This Agreement is concluded between

.....
.....
.....

represented by .....

Name and address of the public authority or company

hereinafter “Controller”

and

Respeak GmbH, Kaiserstraße 89–93, 76133 Karlsruhe, Germany, registered with the commercial register of the local court of Mannheim under HRB 741830, represented by its managing director Dr. Tim Rietz

hereinafter “Processor”

hereinafter individually a “Party” and jointly “the Parties”.

§ 1 Gegenstand und Geltungsbereich

(1) Der Auftragnehmer stellt dem Auftraggeber die Software Schwärzwerk nach Maßgabe eines gesonderten Vertrages bereit (nachfolgend „Hauptvertrag“). Schwärzwerk erkennt personenbezogene Daten in Dokumenten, ersetzt sie durch Platzhalter oder entfernt sie aus der Datei und legt das Ergebnis zur Freigabe vor.

(2) Dieser Vertrag gilt für die gehostete Betriebsart, in der der Auftragnehmer die Software auf von ihm betriebenen Systemen bereitstellt und die Dokumente des Auftraggebers dort verar-

Section 1 Subject matter and scope

(1) The Processor provides the Controller with the software Schwärzwerk under a separate agreement (hereinafter the “Main Agreement”). Schwärzwerk detects personal data in documents, replaces it with placeholders or removes it from the file, and presents the result for approval.

(2) This Agreement applies to the hosted mode of operation, in which the Processor operates the software on systems under its own responsibility and the Controller's documents are

beitet werden. Er konkretisiert die Pflichten der Parteien nach Art. 28 DSGVO.

(3) In den übrigen Betriebsarten von Schwärzwerk findet keine Auftragsverarbeitung statt. Läuft die Software auf einem Arbeitsplatzrechner des Auftraggebers, auf einem Server im Haus des Auftraggebers oder auf einem Gerät ohne Netzanbindung, verlassen weder Dokumente noch die bei der Pseudonymisierung entstehende Zuordnungstabelle die Systeme des Auftraggebers. Der Auftragnehmer erhält von den Inhalten keine Kenntnis und ist insoweit Lieferant der Software und nicht Auftragsverarbeiter. Dieser Vertrag gilt für diese Betriebsarten nicht, soweit sich aus Absatz 4 nichts anderes ergibt.

(4) Eine Ausnahme zu Absatz 3 ist der Glossar-Abgleich. Das Glossar hält Begriffe, die immer oder nie geschwärzt werden; ein Eintrag kann ein Name sein. Schaltet der Auftraggeber den Abgleich ein und teilt eine Liste, überträgt die Anwendung deren Einträge an die Systeme des Auftragnehmers. Für diese Einträge gilt dieser Vertrag auch in den Betriebsarten nach Absatz 3. Der Abgleich ist in der Voreinstellung ausgeschaltet, er lässt sich jederzeit abschalten, und eine Installation mit einer von Hand eingespielten Lizenzdatei kann ihn nicht einschalten.

(5) Die Dauer der Verarbeitung entspricht der Laufzeit des Hauptvertrages.

§ 2 Art, Umfang und Zweck der Verarbeitung

(1) Art, Umfang und Zweck der Verarbeitung, die Arten der verarbeiteten personenbezogenen Daten und die Kategorien betroffener Personen ergeben sich aus Anlage 1. Die dort genannten Daten werden nachfolgend „Auftraggeber-Daten“ genannt.

(2) Die Auftraggeber-Daten gliedern sich in zwei Gruppen, die dieser Vertrag durchgehend unterscheidet. Dokumentdaten sind die vom Auftraggeber hochgeladenen Dokumente und alles, was bei ihrer Verarbeitung entsteht. Kontodaten sind die Angaben zu den Personen, die die Anwendung bedienen.

(3) Der Auftraggeber entscheidet, welche Dokumente er hochlädt. Die Parteien gehen davon aus, dass die Dokumente besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO und Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO enthalten

processed there. It sets out the Parties' obligations under Art. 28 GDPR.

(3) The other modes of operation of Schwärzwerk do not involve processing on behalf of the Controller. Where the software runs on a workstation of the Controller, on a server within the Controller's own premises, or on a device without network access, neither the documents nor the re-identification table created during pseudonymisation leave the Controller's systems. The Processor obtains no knowledge of the content and acts as a software supplier rather than as a processor. This Agreement does not apply to those modes of operation, unless paragraph 4 provides otherwise.

(4) An exception to paragraph 3 is the glossary synchronisation. The glossary holds terms that are always or never redacted; an entry may be a name. If the Controller enables synchronisation and shares a list, the application transmits its entries to the Processor's systems. This Agreement applies to those entries in the modes of operation covered by paragraph 3 as well. Synchronisation is off by default, can be switched off at any time, and an installation running on a manually installed licence file cannot enable it.

(5) The duration of the processing corresponds to the term of the Main Agreement.

Section 2 Nature, scope and purpose of the processing

(1) The nature, scope and purpose of the processing, the types of personal data processed and the categories of data subjects are set out in Appendix 1. The data specified there is hereinafter referred to as “Controller Data”.

(2) Controller Data falls into two groups, which this Agreement distinguishes throughout. Document data is the documents uploaded by the Controller together with everything created during their processing. Account data is the information about the persons who operate the application.

(3) The Controller decides which documents it uploads. The Parties assume that the documents may contain special categories of personal data under Art. 9 GDPR and data relating to criminal convictions and offences under Art. 10 GDPR, because administrative files regularly do. The

können, weil Verwaltungsvorgänge sie regelmäßig enthalten. Der Schutzbedarf der Verarbeitung ist entsprechend hoch.

(4) Bei der Verarbeitung entsteht neben dem geschwärzten Ergebnis eine Analysedatei, die den vollständigen Originaltext des Dokuments im Klartext und die Fundstellen enthält. Sie ist für die erneute Anzeige eines Dokuments im Prüfeditor erforderlich. Sie ist so sensibel wie das Original und unterliegt denselben Regeln zur Aufbewahrung und Löschung nach § 10.

§ 3 Weisungen des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder der Mitgliedstaaten zu einer anderen Verarbeitung verpflichtet. In diesem Fall teilt er dem Auftraggeber die rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Gesetz eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Auftraggebers sind in diesem Vertrag und seinen Anlagen abschließend festgelegt. Die Bedienung der Anwendung durch Beschäftigte des Auftraggebers gilt als Weisung im Rahmen dieses Vertrages, ebenso die Einstellungen, die der Auftraggeber für seine Organisation wählt. Einzelweisungen, die über diesen Rahmen hinausgehen, ergehen in Textform an die in Anlage 1 genannte Kontaktstelle und werden dort dokumentiert.

(3) Verursacht eine Einzelweisung beim Auftragnehmer einen Aufwand, der über das übliche Maß hinausgeht, hat er Anspruch auf eine angemessene Vergütung. Er weist den Auftraggeber darauf hin, bevor er die Weisung ausführt.

(4) Ist der Auftragnehmer der Auffassung, dass eine Weisung gegen die Datenschutz-Grundverordnung oder gegen andere Datenschutzbestimmungen verstößt, teilt er dies dem Auftraggeber unverzüglich mit. Er ist berechtigt, die Ausführung der Weisung bis zu ihrer Bestätigung durch den Auftraggeber auszusetzen.

§ 4 Verantwortlichkeit des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Er ist im Verhältnis der Parteien zueinander allein verantwortlich für

protection requirement of the processing is correspondingly high.

(4) In addition to the redacted result, the processing creates an analysis file containing the full original text of the document in clear text together with the locations of the findings. It is required in order to re-open a document in the review editor. It is as sensitive as the original and is subject to the same retention and deletion rules under Section 10.

Section 3 Instructions of the Controller

(1) The Processor processes Controller Data solely on documented instructions from the Controller, unless required to process it otherwise by Union or Member State law. In that case, the Processor informs the Controller of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

(2) The Controller's instructions are conclusively set out in this Agreement and its appendices. Use of the application by the Controller's staff constitutes an instruction within the scope of this Agreement, as do the settings the Controller chooses for its organisation. Individual instructions going beyond that scope are issued in text form to the contact point named in Appendix 1 and are documented there.

(3) Where an individual instruction causes the Processor effort exceeding the ordinary extent, the Processor is entitled to reasonable remuneration. The Processor informs the Controller before carrying out the instruction.

(4) If the Processor is of the opinion that an instruction infringes the General Data Protection Regulation or other data protection provisions, it informs the Controller without delay. The Processor is entitled to suspend execution of the instruction until the Controller confirms it.

Section 4 Responsibility of the Controller

(1) The Controller is the controller within the meaning of Art. 4 (7) GDPR. As between the Parties, the Controller is solely responsible for

die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen.

(2) Der Auftraggeber ist für die Qualität der Auftraggeber-Daten verantwortlich. Stellt er bei der Prüfung der Verarbeitungsergebnisse Fehler oder Unregelmäßigkeiten in Bezug auf datenschutzrechtliche Bestimmungen oder seine Weisungen fest, informiert er den Auftragnehmer unverzüglich und vollständig.

(3) Der Auftraggeber stellt dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung, soweit sie dem Auftragnehmer nicht selbst vorliegen.

(4) Machen Dritte gegen den Auftragnehmer Ansprüche geltend, die auf einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen seine Pflichten als Verantwortlicher beruhen, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen frei.

§ 5 Keine Nutzung zu eigenen Zwecken

(1) Der Auftragnehmer nutzt die Auftraggeber-Daten ausschließlich zur Erbringung der Leistungen nach dem Hauptvertrag. Eine Nutzung zu eigenen Zwecken findet nicht statt.

(2) Der Auftragnehmer verwendet die Auftraggeber-Daten insbesondere nicht zum Training, zur Bewertung oder zur Weiterentwicklung von Modellen künstlicher Intelligenz und führt sie nicht mit Daten anderer Auftraggeber oder mit eigenen Beständen zusammen. Die eingesetzten Erkennungsmodelle lernen im Betrieb nicht weiter.

(3) Für Betrieb und Abrechnung wertet der Auftragnehmer Kennzahlen ohne Personenbezug aus, namentlich die Zahl verarbeiteter Dokumente und Seiten, Laufzeiten und Fehlerzustände. Dateinamen, Dokumentinhalte und Fundstellen gehören nicht dazu; Dateinamen werden vor der Auswertung an der Quelle entfernt.

§ 6 Ort der Verarbeitung

(1) Dokumentdaten werden ausschließlich in Rechenzentren in der Bundesrepublik Deutschland verarbeitet und gespeichert. Eine Übermittlung in ein Drittland findet nicht statt.

(2) Kontodaten werden in der Europäischen Union verarbeitet. Für den Versand der System-E-Mails, namentlich Bestätigungscodes, Einla-

the lawfulness of the processing and for safeguarding the rights of data subjects.

(2) The Controller is responsible for the quality of the Controller Data. If, when reviewing the results of the processing, it discovers errors or irregularities with regard to data protection provisions or to its instructions, it informs the Processor without delay and in full.

(3) Upon request, the Controller provides the Processor with the information referred to in Art. 30 (2) GDPR, unless that information is already available to the Processor.

(4) Where third parties assert claims against the Processor which are based on a culpable breach by the Controller of this Agreement or of its obligations as controller, the Controller indemnifies the Processor against those claims.

Section 5 No use for the Processor's own purposes

(1) The Processor uses Controller Data solely to provide the services under the Main Agreement. It does not use the data for its own purposes.

(2) In particular, the Processor does not use Controller Data to train, evaluate or further develop artificial intelligence models, and does not combine it with data of other controllers or with its own data. The detection models in use do not learn further during operation.

(3) For operational and billing purposes the Processor evaluates metrics without any personal reference, namely the number of documents and pages processed, run times and error states. File names, document content and findings are not included; file names are removed at source before any evaluation.

Section 6 Place of processing

(1) Document data is processed and stored exclusively in data centres in the Federal Republic of Germany. It is not transferred to any third country.

(2) Account data is processed within the European Union. For sending system e-mails, namely confirmation codes, invitations and sign-in no-

dungen und Hinweise zur Anmeldung, setzt der Auftragnehmer den in Anlage 2 genannten Dienstleister ein. Dabei werden Name und E-Mail-Adresse der betroffenen Person übermittelt; Dokumentinhalte werden nicht übermittelt.

(3) Eine Verlagerung des Verarbeitungsortes teilt der Auftragnehmer dem Auftraggeber vor ihrem Wirksamwerden mit. Eine Verarbeitung außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums setzt voraus, dass die Voraussetzungen der Art. 44 bis 49 DSGVO erfüllt sind, und bedarf für Dokumentdaten der vorherigen Zustimmung des Auftraggebers in Textform.

tices, the Processor uses the service provider named in Appendix 2. Name and e-mail address of the data subject are transmitted in the process; document content is not.

(3) The Processor notifies the Controller of any relocation of the place of processing before it takes effect. Processing outside the European Union and the European Economic Area requires that the conditions of Art. 44 to 49 GDPR are met and, for document data, the Controller's prior consent in text form.

§ 7 Vertraulichkeit und Zugriff durch den Auftragnehmer

(1) Der Auftragnehmer verpflichtet alle Personen, die Auftraggeber-Daten verarbeiten, vor Aufnahme ihrer Tätigkeit zur Vertraulichkeit. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus. Sie erfolgt in Textform, und der Auftragnehmer weist sie auf Anforderung nach.

(2) Die Personen, die Auftraggeber-Daten verarbeiten, werden mit den für sie geltenden Datenschutzbestimmungen vertraut gemacht und regelmäßig geschult.

(3) Der Auftragnehmer hat administrativen Zugang zu den Systemen, auf denen die Verarbeitung stattfindet. Ein Zugriff auf Auftraggeber-Daten erfolgt nur, soweit er für Betrieb, Fehlerbehebung, Sicherung oder Wiederherstellung erforderlich ist. Der Auftragnehmer hält die Zahl der zugangsberechtigten Personen so klein wie möglich und führt darüber ein Verzeichnis.

(4) Ein Zugriff auf Dokumentinhalte zur Fehlerbehebung erfolgt nach vorheriger Abstimmung mit dem Auftraggeber, sofern die Störung dies zulässt, und wird protokolliert.

Section 7 Confidentiality and access by the Processor

(1) The Processor obliges all persons processing Controller Data to maintain confidentiality before they take up their work. The obligation continues after the end of their engagement. It is made in text form, and the Processor demonstrates it upon request.

(2) The persons processing Controller Data are familiarised with the data protection provisions applicable to them and are trained regularly.

(3) The Processor has administrative access to the systems on which the processing takes place. Access to Controller Data only occurs where required for operation, troubleshooting, backup or restoration. The Processor keeps the number of persons with such access as small as possible and maintains a record of them.

(4) Access to document content for troubleshooting takes place after prior coordination with the Controller, where the incident permits, and is logged.

§ 8 Sicherheit der Verarbeitung

(1) Der Auftragnehmer trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in Anlage 3 zusammengefasst.

(2) Anlage 3 ist eine Zusammenfassung. Die vollständige Beschreibung steht in den Dokumenten „Kurzübersicht Datenschutz und IT-Sicherheit“, „IT-Sicherheitskonzept Schwärzwerk“

Section 8 Security of the processing

(1) The Processor implements the technical and organisational measures required under Art. 32 GDPR. The measures in place at the time this Agreement is concluded are summarised in Appendix 3.

(2) Appendix 3 is a summary. The full description is set out in the documents „Kurzübersicht Datenschutz und IT-Sicherheit“, „IT-Sicherheitskonzept Schwärzwerk“ and „Technische und

und „Technische und organisatorische Maßnahmen nach Art. 32 DSGVO“ in ihrer jeweils dem Auftraggeber übergebenen Fassung. Diese Dokumente sind Bestandteil dieses Vertrages. Bei Widersprüchen zwischen Anlage 3 und diesen Dokumenten gilt die für die betroffenen Personen günstigere Regelung.

(3) Der Auftragnehmer darf die Maßnahmen während der Laufzeit ändern. Das Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen teilt er dem Auftraggeber mit.

(4) Eine Zertifizierung des Auftragnehmers nach ISO/IEC 27001 oder ein Testat nach BSI C5 liegt nicht vor. Die Zertifikate und Prüfberichte des in Anlage 2 genannten Hosters reicht der Auftragnehmer auf Anforderung weiter; sie betreffen die Rechenzentren und den Betrieb der Infrastruktur und nicht die Anwendung des Auftragnehmers.

§ 9 Zuordnungstabelle der Pseudonymisierung

(1) Im Platzhaltermodus ersetzt die Software Namen und andere Angaben durch Platzhalter und legt eine Tabelle an, die jeden Platzhalter auf die ursprüngliche Angabe zurückführt. Diese Tabelle ist die zusätzliche Information im Sinne von Art. 4 Nr. 5 DSGVO.

(2) Die Tabelle wird über einen eigenen Weg herausgegeben. Sie wird nie zusammen mit den pseudonymisierten Dokumenten in dasselbe Archiv gepackt und nicht in derselben Anfrage ausgeliefert.

(3) Der Auftraggeber legt in den Einstellungen seiner Organisation fest, wie mit der Tabelle verfahren wird. Zur Wahl stehen drei Regeln: die Aufbewahrung bis zum Ablauf der Aufbewahrungsfrist nach § 10, die Vernichtung beim ersten Abruf und der eigene Schlüssel nach Absatz 4. Die Voreinstellung für neue Organisationen ist die Aufbewahrung. Jede Änderung der Einstellung, jeder Abruf und jede Vernichtung erzeugt einen Protokolleintrag.

(4) Bei der Regel „eigener Schlüssel“ erzeugt das Team des Auftraggebers ein Schlüsselpaar im Browser. Der private Teil erreicht die Systeme des Auftragnehmers nie. Die Tabelle wird beim Entstehen auf den öffentlichen Teil versiegelt und versiegelt herausgegeben; der Auftragnehmer kann sie nicht lesen. Diese Regel gilt für die Zuordnungstabelle und nicht für die Dokumente: um ein Dokument zu schwärzen, muss der Arbeitsprozess es lesen. Die Einstellung setzt

organisatorische Maßnahmen nach Art. 32 DSGVO“ in the version handed over to the Controller. Those documents form part of this Agreement. In the event of a conflict between Appendix 3 and those documents, the provision more favourable to the data subjects prevails.

(3) The Processor may change the measures during the term. The level of protection must not fall below the agreed level. The Processor notifies the Controller of material changes.

(4) The Processor holds neither an ISO/IEC 27001 certification nor a BSI C5 attestation. The Processor passes on the certificates and audit reports of the hosting provider named in Appendix 2 upon request; they concern the data centres and the operation of the infrastructure, not the Processor's application.

Section 9 Re-identification table

(1) In placeholder mode the software replaces names and other details with placeholders and creates a table mapping each placeholder back to the original detail. That table is the additional information within the meaning of Art. 4 (5) GDPR.

(2) The table is handed over through a separate route. It is never packaged into the same archive as the pseudonymised documents and is not delivered in the same request.

(3) The Controller determines in its organisation settings how the table is handled. There are three options: retention until the retention period under Section 10 expires, destruction upon first retrieval, and the Controller's own key under paragraph 4. The default for new organisations is retention. Every change to the setting, every retrieval and every destruction creates an audit log entry.

(4) Under the “own key” option the Controller's team generates a key pair in the browser. The private half never reaches the Processor's systems. The table is sealed to the public half when it is created and is handed over sealed; the Processor cannot read it. This option covers the re-identification table and not the documents: in order to redact a document, the processing job has to read it. The setting requires the team to

voraus, dass das Team vorher einen Schlüssel angelegt hat, und wird ohne Schlüssel abgewiesen.

(5) Im Blackbox-Modus entsteht keine Tabelle. Dort wird nichts pseudonymisiert; die erkannten Angaben werden aus der Datei entfernt. Es gibt in diesem Modus nichts, was der Auftragnehmer zurückübersetzen könnte.

(6) Die Rückübersetzung eines bearbeiteten Dokuments läuft im Browser des Auftraggebers. Der zurückübersetzte Text erreicht die Systeme des Auftragnehmers zu keinem Zeitpunkt.

§ 10 Aufbewahrung und Löschung im laufenden Betrieb

(1) Der Auftraggeber legt die Aufbewahrungsfrist für Vorgänge selbst in den Einstellungen seiner Organisation fest und kann sie jederzeit ändern. Nach Ablauf der Frist löscht ein täglicher Lauf den Vorgang.

(2) Ist keine Frist gesetzt, findet keine automatische Löschung statt. Der Auftragnehmer weist den Auftraggeber hierauf hin; die Festlegung der Frist bleibt eine Entscheidung des Verantwortlichen.

(3) Die Frist wird beim Anlegen eines Vorgangs als festes Datum gesetzt. Eine spätere Verkürzung wirkt für bereits angelegte Vorgänge nicht zurück. Der Auftraggeber kann jeden Vorgang jederzeit sofort löschen.

(4) Die Löschung erfasst das hochgeladene Original, das geschwärzte Ergebnis, die Analysedatei mit dem Originaltext, die gespeicherten Korrekturen, die Zuordnungstabelle und die zugehörigen Datenbankeinträge. Mit dem Vorgang wird auch sein Schlüssel vernichtet, so dass verbliebene Kopien der Objekte im Speicher nicht mehr entschlüsselt werden können. Der Protokolleintrag über die Verarbeitung bleibt bestehen; er enthält keine Dokumentinhalte.

(5) Nummeriert der Auftraggeber Platzhalter über einen Vorgang hinaus, organisationsweit oder in einem benannten Nummernkreis, hält die Anwendung für diesen Kreis die vergebenen Nummern zu Prüfwerten der erkannten Angaben, die mit einem geheimen Schlüssel gebildet werden. Die Angaben selbst stehen dort nicht. Ein solcher Kreis wird von der Löschung einzelner Vorgänge nicht erfasst; benannte Kreise löscht der Auftraggeber selbst in der Anwendung, im Übrigen gelten § 12 Abs. 3 und § 15.

have created a key beforehand and is refused without one.

(5) In blackbox mode no table is created. Nothing is pseudonymised there; the detected data is removed from the file. In that mode there is nothing the Processor could translate back.

(6) The restoration of an edited document runs in the Controller's browser. The restored text never reaches the Processor's systems.

Section 10 Retention and deletion during the term

(1) The Controller itself sets the retention period for cases in its organisation settings and may change it at any time. Once the period expires, a daily run deletes the case.

(2) If no period is set, no automatic deletion takes place. The Processor points this out to the Controller; setting the period remains a decision of the controller.

(3) The period is stamped as a fixed date when a case is created. Shortening it later has no retroactive effect on cases already created. The Controller may delete any case immediately at any time.

(4) Deletion covers the uploaded original, the redacted result, the analysis file containing the original text, the stored corrections, the re-identification table and the associated database records. The key of the case is destroyed together with it, so that any remaining copies of the objects in storage can no longer be decrypted. The audit log entry about the processing remains; it contains no document content.

(5) Where the Controller numbers placeholders beyond a single case, organisation-wide or in a named numbering series, the application keeps, for that series, the numbers assigned to check values of the detected details, formed with a secret key. The details themselves are not stored there. Such a series is not covered by the deletion of individual cases; the Controller deletes named series itself in the application, and otherwise Section 12 (3) and Section 15 apply.

§ 11 Weitere Auftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter hinzuzuziehen. Die bei Vertragsschluss hinzugezogenen weiteren Auftragsverarbeiter ergeben sich aus Anlage 2.

(2) Der Auftragnehmer teilt dem Auftraggeber die Hinzuziehung oder Ersetzung eines weiteren Auftragsverarbeiters spätestens 30 Tage vor dem Wirksamwerden in Textform mit. Der Auftraggeber kann innerhalb von 14 Tagen nach Zugang der Mitteilung aus datenschutzrechtlichen Gründen widersprechen. Kommt eine Einigung nicht zustande, kann der Auftraggeber den Hauptvertrag und diesen Vertrag zum vorgesehenen Wirksamwerden der Änderung kündigen, ohne dass ihm daraus Kosten entstehen.

(3) Der Auftragnehmer erlegt jedem weiteren Auftragsverarbeiter dieselben Pflichten auf, die ihm nach diesem Vertrag obliegen, und prüft vor der Beauftragung dessen technische und organisatorische Maßnahmen. Für das Verhalten des weiteren Auftragsverarbeiters haftet der Auftragnehmer wie für eigenes Verhalten.

(4) Nicht genehmigungspflichtig sind Nebenleistungen, die der Auftragnehmer in Anspruch nimmt und bei denen ein Zugriff auf Auftraggeber-Daten nicht der Zweck der Leistung ist, namentlich Telekommunikation, Postdienste und Wartung von Endgeräten. Der Auftragnehmer trifft auch hier die erforderlichen Vereinbarungen zur Vertraulichkeit.

Section 11 Sub-processors

(1) The Controller grants the Processor general authorisation to engage sub-processors. The sub-processors engaged at the time this Agreement is concluded are set out in Appendix 2.

(2) The Processor notifies the Controller in text form of the engagement or replacement of a sub-processor at least 30 days before it takes effect. The Controller may object within 14 days of receipt of the notification on data protection grounds. If no agreement is reached, the Controller may terminate the Main Agreement and this Agreement with effect from the intended date of the change, at no cost to the Controller.

(3) The Processor imposes on every sub-processor the same obligations it is subject to under this Agreement and reviews the sub-processor's technical and organisational measures before engaging it. The Processor is liable for the conduct of the sub-processor as for its own.

(4) Ancillary services used by the Processor where access to Controller Data is not the purpose of the service, namely telecommunications, postal services and the maintenance of end user devices, do not require authorisation. Here too the Processor puts the necessary confidentiality arrangements in place.

§ 12 Rechte der betroffenen Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen zu beantworten.

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet er den Antrag unverzüglich an den Auftraggeber weiter und beantwortet ihn nicht selbst.

(3) Der Auftragnehmer berichtigt, löscht oder schränkt die Verarbeitung von Auftraggeber-Daten auf Weisung des Auftraggebers ein, soweit dieser es nicht selbst über die Anwendung tun kann.

(4) Entsteht dem Auftragnehmer durch die Unterstützung ein Aufwand, der über das übliche Maß hinausgeht, hat er Anspruch auf eine ange-

Section 12 Rights of data subjects

(1) The Processor assists the Controller by appropriate technical and organisational measures in responding to requests from data subjects.

(2) If a data subject approaches the Processor directly, the Processor forwards the request to the Controller without delay and does not answer it itself.

(3) The Processor rectifies, erases or restricts the processing of Controller Data on the Controller's instruction, to the extent the Controller cannot do so itself through the application.

(4) Where the assistance causes the Processor effort exceeding the ordinary extent, the Processor is entitled to reasonable remuneration. It informs the Controller beforehand.

messene Vergütung. Er weist den Auftraggeber vorher darauf hin.

§ 13 Meldung von Verletzungen und weitere Unterstützung

(1) Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem sie ihm bekannt geworden ist. Eine eigene Prüfung, ob die Verletzung meldepflichtig ist, nimmt er nicht vor; diese Bewertung trifft der Auftraggeber.

(2) Die Meldung enthält, soweit die Angaben vorliegen, die in Art. 33 Abs. 3 DSGVO genannten Punkte. Fehlende Angaben reicht der Auftragnehmer nach, ohne die Meldung dadurch zu verzögern.

(3) Die Meldung geht an die in Anlage 1 genannte Kontaktstelle des Auftraggebers. Der Auftragnehmer dokumentiert jede Verletzung mit Sachverhalt, Wirkung und ergriffenen Maßnahmen und übergibt dem Auftraggeber nach Abschluss eine schriftliche Darstellung.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO und bei einer vorherigen Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO, indem er die technischen Angaben, eine Beschreibung der Datenflüsse und die Maßnahmendokumentation zuliefert.

§ 14 Nachweise und Überprüfungen

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anforderung alle Informationen zur Verfügung, die zum Nachweis der Einhaltung seiner Pflichten aus diesem Vertrag erforderlich sind. Er legt dazu regelmäßig die Kurzübersicht, das IT-Sicherheitskonzept und die Maßnahmendokumentation in aktueller Fassung vor.

(2) Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrages zu überprüfen, einschließlich einer Überprüfung vor Ort. Eine Überprüfung vor Ort erfolgt einmal im Kalenderjahr, zu den üblichen Geschäftszeiten, nach Ankündigung mit einer Frist von zwei Wochen und ohne Störung des Betriebsablaufs. Bei einer Verletzung des Schutzes personenbezogener Daten und bei einem begründeten Verdacht darauf ist eine weitere Überprüfung ohne Rücksicht auf diese Beschränkungen zulässig.

Section 13 Personal data breaches and further assistance

(1) The Processor notifies the Controller of any personal data breach without undue delay after becoming aware of it. The Processor does not itself assess whether the breach is notifiable; that assessment is made by the Controller.

(2) The notification contains the points listed in Art. 33 (3) GDPR to the extent the information is available. The Processor provides missing information subsequently and does not delay the notification for it.

(3) The notification is sent to the Controller's contact point named in Appendix 1. The Processor documents every breach with the facts, the effect and the measures taken, and provides the Controller with a written account once the matter is closed.

(4) The Processor assists the Controller with the data protection impact assessment under Art. 35 GDPR and with any prior consultation of the supervisory authority under Art. 36 GDPR by supplying the technical information, a description of the data flows and the documentation of the measures.

Section 14 Evidence and audits

(1) Upon request, the Processor makes available to the Controller all information necessary to demonstrate compliance with its obligations under this Agreement. For that purpose it regularly provides the Kurzübersicht, the IT security concept and the documentation of the measures in their current version.

(2) The Controller is entitled to verify compliance with this Agreement, including by an on-site audit. An on-site audit takes place once per calendar year, during normal business hours, upon two weeks' notice and without disrupting operations. In the event of a personal data breach, and where there is a reasonable suspicion of one, a further audit is permitted without regard to those restrictions.

(3) Der Auftraggeber kann einen Dritten mit der Überprüfung beauftragen. Er verpflichtet den Dritten in Textform zur Verschwiegenheit, soweit dieser nicht ohnehin einer berufsrechtlichen Verschwiegenheitspflicht unterliegt. Ein Wettbewerber des Auftragnehmers ist als Prüfer ausgeschlossen.

(4) Der Auftragnehmer ist nicht verpflichtet, Daten und Informationen anderer Auftraggeber offenzulegen. Die Befugnisse der Aufsichtsbehörde gegenüber dem Auftragnehmer bleiben von diesem Paragrafen unberührt.

(3) The Controller may instruct a third party to carry out the audit. It obliges that third party to confidentiality in text form, unless the third party is already subject to a professional duty of confidentiality. A competitor of the Processor is excluded as an auditor.

(4) The Processor is not obliged to disclose data or information relating to other controllers. The powers of the supervisory authority vis-à-vis the Processor remain unaffected by this Section.

§ 15 Rückgabe und Löschung nach Beendigung

(1) Nach Beendigung des Hauptvertrages gibt der Auftragnehmer die Auftraggeber-Daten nach Wahl des Auftraggebers zurück oder löscht sie. Der Auftraggeber teilt seine Wahl innerhalb von 30 Tagen nach Beendigung mit. Trifft er keine Wahl, löscht der Auftragnehmer die Daten.

(2) Die Rückgabe erfolgt in einem gängigen, maschinenlesbaren Format über die vorhandenen Ausgabewege. Die Löschung erfolgt innerhalb von 30 Tagen nach der Mitteilung oder nach Ablauf der Frist nach Absatz 1.

(3) In den verschlüsselten Sicherungsarchiven bleiben gelöschte Daten bis zum turnusmäßigen Ablauf des jeweiligen Standes erhalten. Der längste vorgehaltene Stand ist zwölf Monate alt. Eine gezielte Löschung einzelner Daten aus einem Sicherungsarchiv ist nicht möglich. Wird ein Stand eingespielt, stellt der Auftragnehmer sicher, dass die gelöschten Daten erneut gelöscht werden.

(4) Der Auftragnehmer weist die Löschung auf Anforderung in Textform nach. Dokumentation, die dem Nachweis der ordnungsgemäßen Verarbeitung dient, darf er über das Vertragsende hinaus aufbewahren, ebenso Daten, für die eine gesetzliche Aufbewahrungspflicht besteht.

Section 15 Return and deletion after termination

(1) After termination of the Main Agreement the Processor, at the Controller's choice, returns the Controller Data or deletes it. The Controller communicates its choice within 30 days of termination. If it makes no choice, the Processor deletes the data.

(2) The return is made in a common, machine-readable format through the existing export routes. The deletion is carried out within 30 days of the notification or of the expiry of the period under paragraph 1.

(3) Deleted data remains in the encrypted backup archives until the respective snapshot expires in the ordinary rotation. The oldest snapshot retained is twelve months old. Selective deletion of individual data from a backup archive is not possible. If a snapshot is restored, the Processor ensures that the deleted data is deleted again.

(4) Upon request, the Processor confirms the deletion in text form. It may retain documentation serving as evidence of proper processing beyond the end of the Agreement, as well as data subject to a statutory retention obligation.

§ 16 Berufsgeheimnisse

(1) Ist der Auftraggeber Berufsgeheimnisträger im Sinne von § 203 StGB, insbesondere Rechtsanwältin oder Rechtsanwalt, Steuerberaterin oder Steuerberater, Ärztin oder Arzt, so können die Auftraggeber-Daten fremde Geheimnisse enthalten, die dem Berufsgeheimnis unterliegen.

Section 16 Professional secrets

(1) Where the Controller is subject to a professional duty of secrecy within the meaning of Section 203 of the German Criminal Code, in particular as an attorney, a tax adviser or a physician, the Controller Data may contain third-party secrets covered by that duty.

(2) In diesem Fall schließen die Parteien zusätzlich zu diesem Vertrag die „Vereinbarung über die Inanspruchnahme von Dienstleistungen und die Verpflichtung zur Verschwiegenheit (§ 43e BRAO, § 203 StGB)“ des Auftragnehmers. Sie regelt die Verpflichtung des Auftragnehmers und der von ihm herangezogenen Personen zur Verschwiegenheit unter Hinweis auf die strafrechtlichen Folgen einer Verletzung.

(3) Die Verpflichtungen aus jener Vereinbarung bestehen neben den Pflichten aus diesem Vertrag und werden durch ihn nicht eingeschränkt.

(2) In that case the Parties additionally conclude the Processor's “Agreement on the use of services and undertaking of confidentiality (Section 43e BRAO, Section 203 StGB)”. It governs the confidentiality obligations of the Processor and of the persons it engages, with reference to the criminal consequences of a breach.

(3) The obligations under that agreement exist alongside the obligations under this Agreement and are not limited by it.

§ 17 Laufzeit und Kündigung

(1) Laufzeit und Kündigung dieses Vertrages richten sich nach dem Hauptvertrag. Die Beendigung des Hauptvertrages beendet auch diesen Vertrag.

(2) Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen. § 11 Abs. 2 bleibt unberührt.

(3) Verstößt der Auftragnehmer schwerwiegend gegen diesen Vertrag oder gegen datenschutzrechtliche Bestimmungen und behebt er den Verstoß nicht innerhalb einer angemessenen Frist, kann der Auftraggeber den Hauptvertrag aus wichtigem Grund kündigen.

Section 17 Term and termination

(1) The term and termination of this Agreement follow the Main Agreement. Termination of the Main Agreement also terminates this Agreement.

(2) Separate termination of this Agreement is excluded. Section 11 (2) remains unaffected.

(3) If the Processor seriously breaches this Agreement or data protection law and does not remedy the breach within a reasonable period, the Controller may terminate the Main Agreement for cause.

§ 18 Haftung

(1) Für die Haftung der Parteien gelten die Regelungen des Hauptvertrages.

(2) Art. 82 DSGVO bleibt unberührt. Die Haftung gegenüber betroffenen Personen wird durch diesen Vertrag weder ausgeschlossen noch beschränkt.

Section 18 Liability

(1) The liability of the Parties is governed by the provisions of the Main Agreement.

(2) Art. 82 GDPR remains unaffected. Liability towards data subjects is neither excluded nor limited by this Agreement.

§ 19 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses Vertrages bedürfen der Textform. Das gilt auch für die Aufhebung dieses Formerfordernisses.

(2) Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag oder sonstigen Vereinbarungen der Parteien gehen in datenschutzrechtlichen Fragen die Regelungen dieses Vertrages vor.

(3) Ist eine Bestimmung dieses Vertrages unwirksam oder enthält der Vertrag eine Lücke, bleiben die übrigen Bestimmungen wirksam. Die Parteien ersetzen die unwirksame Bestimmung durch eine zulässige Regelung, die ihrem Zweck

Section 19 Final provisions

(1) Amendments and supplements to this Agreement require text form. This also applies to any waiver of this form requirement.

(2) In the event of a conflict between this Agreement and the Main Agreement or other agreements between the Parties, the provisions of this Agreement prevail in matters of data protection law.

(3) If a provision of this Agreement is invalid or the Agreement contains a gap, the remaining provisions remain effective. The Parties replace the invalid provision with a permissible provision

am nächsten kommt und den Anforderungen des Art. 28 DSGVO genügt.

(4) Es gilt deutsches Recht. Gerichtsstand ist der im Hauptvertrag vereinbarte Gerichtsstand.

(5) Verbindlich ist die deutsche Fassung dieses Vertrages. Die englische Fassung dient der Information.

Ort, Datum / Place, date .....

Auftraggeber, Name und Funktion
Controller, name and function

that comes closest to its purpose and meets the requirements of Art. 28 GDPR.

(4) German law applies. The place of jurisdiction is the one agreed in the Main Agreement.

(5) The German version of this Agreement is binding. The English version is provided for information.

Ort, Datum / Place, date .....

Auftragnehmer, Respeak GmbH
Processor, Respeak GmbH

Anlage 1: Gegenstand der Verarbeitung

Zweck der Verarbeitung

Bereitstellung der Software Schwärzwerk nach dem Hauptvertrag: Erkennung personenbezogener Daten in den vom Auftraggeber hochgeladenen Dokumenten, Ersetzung durch Platzhalter oder Entfernung aus der Datei, Bereitstellung des Ergebnisses zur Prüfung und zum Abruf.

Art der Verarbeitung

Erheben, Speichern, Auslesen, Verändern, Verwenden, Bereitstellen und Löschen im Rahmen der Leistungserbringung. Die Verarbeitung erfolgt automatisiert. Eine automatisierte Entscheidung mit rechtlicher Wirkung gegenüber betroffenen Personen findet nicht statt; das Ergebnis wird der Sachbearbeitung zur Freigabe vorgelegt.

Arten personenbezogener Daten: Dokumentdaten

Die vom Auftraggeber hochgeladenen Dokumente und eingefügten Texte und alles, was bei ihrer Verarbeitung entsteht, namentlich das geschwärzte Ergebnis, die Analysedatei mit dem Originaltext, die gespeicherten Korrekturen, die Zuordnungstabelle, die Nummernkreise nach § 10 Abs. 5 und das Vorgangsprotokoll. Dateinamen gehören dazu.

Erkannt und verarbeitet werden insbesondere: Namen, Anschriften, E-Mail-Adressen, Telefonnummern, Datumsangaben, Organisationen und Ortsangaben; Aktenzeichen, Ausweis- und Vorgangsnummern, IBAN, Kontonummern und Bankleitzahlen, Kreditkartennummern; Gesichter auf Fotos und Scans.

Besondere Kategorien nach Art. 9 DSGVO: Gesundheitsdaten, Religionszugehörigkeit, politische Meinung, Gewerkschaftszugehörigkeit, sexuelle Orientierung. Daten nach Art. 10 DSGVO: Angaben zu Straftaten und strafrechtlichen Verurteilungen.

Arten personenbezogener Daten: Kontodaten

Name, E-Mail-Adresse und Organisationszugehörigkeit der Nutzerinnen und Nutzer, Anmeldedaten und Sitzungsdaten, Rolle und Berechtigungen, Protokolleinträge über Anmeldungen und über Handlungen in der Anwendung.

Appendix 1: Subject matter of the processing

Purpose of the processing

Provision of the software Schwärzwerk under the Main Agreement: detection of personal data in the documents uploaded by the Controller, replacement with placeholders or removal from the file, and provision of the result for review and retrieval.

Nature of the processing

Collection, storage, retrieval, alteration, use, disclosure and erasure in the course of providing the services. The processing is automated. There is no automated decision producing legal effects concerning data subjects; the result is presented to a case handler for approval.

Types of personal data: document data

The documents uploaded and texts pasted by the Controller and everything created during their processing, namely the redacted result, the analysis file containing the original text, the stored corrections, the re-identification table, the numbering series under Section 10 (5) and the case log. File names are included.

Detected and processed in particular: names, addresses, e-mail addresses, telephone numbers, dates, organisations and locations; file references, identity and case numbers, IBANs, account and bank codes, credit card numbers; faces in photographs and scans.

Special categories under Art. 9 GDPR: health data, religious beliefs, political opinions, trade union membership, sexual orientation. Data under Art. 10 GDPR: information on criminal offences and convictions.

Types of personal data: account data

Name, e-mail address and organisational affiliation of the users, sign-in and session data, role and permissions, audit log entries on sign-ins and on actions within the application.

Kategorien betroffener Personen

Personen, auf die sich die hochgeladenen Dokumente beziehen, namentlich Einwenderinnen und Einwender, Antragstellende, Beteiligte und deren Angehörige sowie die in den Dokumenten genannten Dritten.

Beschäftigte des Auftraggebers und weitere Personen, die die Anwendung im Auftrag des Auftraggebers bedienen.

Categories of data subjects

Persons to whom the uploaded documents relate, namely objectors, applicants, parties and their relatives, as well as third parties named in the documents.

Employees of the Controller and other persons operating the application on the Controller's behalf.

Dauer der Verarbeitung

Für die Laufzeit des Hauptvertrages, für einzelne Vorgänge begrenzt durch die Aufbewahrungsfrist nach § 10.

Duration of the processing

For the term of the Main Agreement, limited for individual cases by the retention period under Section 10.

Kontaktstellen

Contact points

Partei Party	**Name und Funktion** Name and function	**Erreichbarkeit** Contact details
Auftraggeber Controller	.....	.....
Datenschutzbeauftragte Stelle des Auftraggebers Controller's data protection officer	.....	.....
Auftragnehmer Processor	Dr. Tim Rietz Geschäftsführer	info@respeak.io

Der Auftragnehmer ist nicht verpflichtet, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen; die Voraussetzungen des § 38 Abs. 1 BDSG liegen nicht vor. Zuständig ist die Geschäftsführung.

The Processor has not appointed a data protection officer because the conditions of Section 38 (1) of the German Federal Data Protection Act are not met. Responsibility lies with the management.

Anlage 2: Weitere Auftragsverarbeiter

Zum Zeitpunkt des Vertragsschlusses sind die folgenden weiteren Auftragsverarbeiter hinzugezogen.

Appendix 2: Sub-processors

At the time this Agreement is concluded, the following sub-processors are engaged.

Unternehmen und Anschrift Company and address	**Zweck** Purpose	**Datenarten** Types of data	**Ort der Verarbeitung** Place of processing
Hetzner Online GmbH, Industriestraße 25, 91710 Gunzenhausen, Deutschland	Betrieb der Server, der Datenbanken und des Objektspeichers, auf denen die Anwendung läuft Operation of the servers, databases and object storage on which the application runs	Dokumentdaten und Kontodaten Document data and account data	Deutschland Germany
Cloudflare, Inc., 101 Townsend Street, San Francisco, CA 94107, USA, in Europa vertreten durch die Cloudflare Germany GmbH, Rosental 7, 80331 München	Versand der System-E-Mails: Bestätigungscodes, Einladungen und Hinweise zur Anmeldung Dispatch of system e-mails: confirmation codes, invitations and sign-in notices	Name und E-Mail-Adresse der Nutzerinnen und Nutzer. Keine Dokumentdaten Name and e-mail address of the users. No document data	Europäische Union European Union
Functional Software, Inc. (Sentry), 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Fehlerberichte der Anwendung, vor dem Versand bereinigt um Dateinamen, Pfade und Dokumentinhalte Error reports of the application, scrubbed of file names, paths and document content before sending	Technische Angaben zum Fehler. Keine Dokumentdaten Technical details of the error. No document data	Deutschland (EU-Region) Germany (EU region)

Cloudflare und Sentry haben ihren Sitz in den USA. Soweit dabei Daten in ein Drittland gelangen, gelten die Standardvertragsklauseln der Europäischen Kommission nach Art. 46 Abs. 2 lit. c DSGVO. Dokumentdaten sind davon nicht berührt.

Der Identitätsdienst, die Datenbank, der Objektspeicher und die Überwachung werden vom Auftragnehmer auf der in dieser Anlage genannten Infrastruktur selbst betrieben. Ein weiterer Dienstleister ist daran nicht beteiligt.

Cloudflare and Sentry are based in the USA. Where data reaches a third country in that context, the European Commission's standard contractual clauses under Art. 46 (2) (c) GDPR apply. Document data is not affected.

The identity service, the database, the object storage and the monitoring are operated by the Processor itself on the infrastructure named in this Appendix. No further service provider is involved in them.

Die Abwicklung von Zahlungen berührt keine Dokumentdaten. Sie erfolgt außerhalb dieses Vertrages; der Auftragnehmer ist insoweit selbst Verantwortlicher.

Payment processing does not involve any document data. It takes place outside this Agreement; in that respect the Processor is itself a controller.

Anlage 3: Technische und organisatorische Maßnahmen

Diese Anlage fasst die Maßnahmen nach Art. 32 DSGVO für den Betrieb durch den Auftragnehmer zusammen. Die vollständige Beschreibung mit Begründungen, Messwerten und offenen Punkten steht in den beiden in § 8 Abs. 2 genannten Dokumenten.

Appendix 3: Technical and organisational measures

This Appendix summarises the measures under Art. 32 GDPR for the operation by the Processor. The full description, with reasoning, measurements and open points, is set out in the two documents named in Section 8 (2).

Bereich Area	**Maßnahmen** Measures
Pseudonymisierung Pseudonymisation	Die Pseudonymisierung ist der Zweck des Produkts. Die Zuordnungstabelle wird über einen eigenen Weg herausgegeben und nie mit den pseudonymisierten Dokumenten zusammen ausgeliefert. Jeder Abruf und jede Vernichtung wird protokolliert. Im Blackbox-Modus entsteht keine Tabelle. Pseudonymisation is the purpose of the product. The re-identification table is handed over through a separate route and is never delivered together with the pseudonymised documents. Every retrieval and every destruction is logged. In blackbox mode no table is created.
Verschlüsselung bei der Übertragung Encryption in transit	Der gesamte Verkehr zwischen Browser und Anwendung läuft über TLS, mindestens in der Version 1.2. Zertifikate werden automatisch ausgestellt und erneuert. HTTP Strict Transport Security ist aktiv, Aufrufe über Port 80 werden umgeleitet. Abrufadressen für Dokumente sind signiert und zeitlich befristet. All traffic between browser and application runs over TLS, version 1.2 at the minimum. Certificates are issued and renewed automatically. HTTP Strict Transport Security is enabled and calls over port 80 are redirected. Retrieval URLs for documents are signed and time-limited.
Verschlüsselung im Ruhezustand Encryption at rest	Jedes Objekt wird von der Anwendung vor dem Schreiben verschlüsselt, ohne Schalter, der das abstellen könnte. Die Schlüssel sind dreistufig: ein Hauptschlüssel der Installation umschließt den Schlüssel der Organisation, dieser den Schlüssel je Vorgang, dieser verschlüsselt die Objekte. Der Speicher sieht nur Geheimtext, und das gilt auch für den Speicher des Hosters. Die Sicherungsarchive sind verschlüsselt; ein unverschlüsseltes Archiv lässt sich mit dem eingesetzten Werkzeug nicht herstellen. Die Geheimnisse des Identitätsdienstes liegen unter einem eigenen Hauptschlüssel. Für die Datenträger der Maschine und das Datenbankvolumen wird die Verschlüsselung je Installation festgelegt; sie steht in Kapitel 18 der Kurzübersicht. Every object is encrypted by the application before it is written, with no switch that could turn this off. The keys form three levels: a master key of the installation wraps the organisation's key, which wraps the key of each case, which encrypts the objects. The storage only ever sees ciphertext, including the hosting provider's storage. The backup archives are encrypted; the tool in use cannot produce an unencrypted archive. The identity service's secrets are held under a dedicated master key. For the machine's storage volumes and the database volume, encryption is determined per installation; it is recorded in chapter 18 of the Kurzübersicht.

Zutritt und Zugang Physical and system access	Die Rechenzentren betreibt der in Anlage 2 genannte Hoster; der Auftragnehmer hat dort keinen physischen Zutritt. Die Anmeldung an der Anwendung läuft über einen Identitätsdienst mit eigenem Konto je Person. Der administrative Zugang zu den Servern erfolgt über SSH mit Schlüsseln; die Zahl der Berechtigten ist auf das Notwendige begrenzt. The data centres are operated by the hosting provider named in Appendix 2; the Processor has no physical access to them. Sign-in to the application runs through an identity service with an individual account per person. Administrative access to the servers uses SSH keys; the number of authorised persons is limited to what is necessary.
Zugriff und Trennung Authorisation and separation	Der Zugriff auf Vorgänge ist an die Organisation und das Team gebunden, und jede Anfrage wird gegen diese Zuordnung geprüft. Die Daten verschiedener Auftraggeber sind logisch getrennt. Produktiv- und Testumgebung sind getrennt. Access to cases is bound to the organisation and the team, and every request is checked against that assignment. The data of different controllers is logically separated. Production and test environments are separated.
Eingabe und Nachvollziehbarkeit Input control and traceability	Ein Protokoll hält fest, wer wann welche Handlung vorgenommen hat, namentlich Hochladen, Freigeben, Abrufen, Löschen und die Änderung von Einstellungen. Betriebsmeldungen und Kennzahlen enthalten keine Dateinamen und keine Dokumentinhalte. An audit log records who performed which action and when, namely uploading, approving, retrieving, deleting and changing settings. Operational messages and metrics contain no file names and no document content.
Verfügbarkeit und Wiederanlauf Availability and recovery	Ein Sicherungslauf umfasst Anwendungsdatenbank, Datenbank des Identitätsdienstes, Objektspeicher und Konfiguration in einem Durchgang. Das verschlüsselte Archiv liegt außerhalb der Maschine und in einem anderen Ausfallbereich. Vorgehalten werden 24 stündliche, 14 tägliche, 8 wöchentliche und 12 monatliche Stände. Eine Wiederherstellung wurde geübt und schriftlich festgehalten. One backup run covers the application database, the identity service database, the object storage and the configuration in a single pass. The encrypted archive is stored off the machine and in a different failure domain. 24 hourly, 14 daily, 8 weekly and 12 monthly snapshots are retained. A restoration has been exercised and documented in writing.
Belastbarkeit Resilience	Web-Schicht und Verarbeitung sind getrennte Prozesse; ein Absturz der Verarbeitung nimmt die Anmeldung nicht mit. Aufträge liegen in einer Warteschlange in der Datenbank und überstehen einen Neustart. Die Zahl gleichzeitiger Verarbeitungen und die Menge je Organisation sind begrenzt. The web tier and the processing tier are separate processes; a crash of the processing tier does not take sign-in down with it. Jobs are held in a database queue and survive a restart. The number of concurrent processing runs and the volume per organisation are capped.
Überprüfung der Wirksamkeit Review of effectiveness	Die Wirksamkeit der Schwärzung ist in automatisierten Prüfungen festgeschrieben, die bei jeder Änderung des Codes laufen: die Geometrie der Schwärzung, die Kanäle außerhalb der Seiten wie Metadaten, Anhänge, Lesezeichen und Formularwerte, die Bildpunkte ge-

	scannter Seiten und die Zusage, dass im lokalen Betrieb nichts das Gerät verlässt. Jede dieser Prüfungen hat eine Gegenprobe, die den historischen Fehler wieder einbaut und verlangt, dass die Prüfung rot wird. The effectiveness of the redaction is pinned by automated checks that run on every code change: the geometry of the redaction, the channels outside the page such as metadata, attachments, bookmarks and form values, the pixels of scanned pages, and the assurance that nothing leaves the device in local operation. Each of these checks has a counter-test that reinstates the historical defect and requires the check to turn red.
Patches und Schwachstellen Patching and vulnerabilities	Abhängigkeiten sind auf feste Fassungen gepinnt und werden regelmäßig angehoben. Sicherheitsrelevante Aktualisierungen des Betriebssystems werden zeitnah eingespielt. Meldungen über Schwachstellen nimmt die in Anlage 1 genannte Kontaktstelle entgegen. Dependencies are pinned to fixed versions and raised regularly. Security-relevant operating system updates are applied promptly. Vulnerability reports are received by the contact point named in Appendix 1.
Vertraulichkeit des Personals Confidentiality of personnel	Alle Personen, die Auftraggeber-Daten verarbeiten, sind in Textform zur Vertraulichkeit verpflichtet und werden regelmäßig geschult. Externe, die mit personenbezogenen Daten in Berührung kommen können, werden vor Aufnahme der Tätigkeit zur Verschwiegenheit verpflichtet. All persons processing Controller Data are bound to confidentiality in text form and are trained regularly. External parties who may come into contact with personal data are bound to secrecy before they begin work.
Auftragskontrolle Control of sub-processing	Weitere Auftragsverarbeiter werden vor der Beauftragung auf ihre Maßnahmen geprüft, vertraglich auf dasselbe Schutzniveau verpflichtet und in Anlage 2 benannt. Eine Verarbeitung von Dokumentdaten außerhalb Deutschlands findet nicht statt. Sub-processors are reviewed for their measures before being engaged, are contractually bound to the same level of protection and are named in Appendix 2. Document data is not processed outside Germany.
Löschung Erasure	Die Löschung eines Vorgangs entfernt dessen gesamten Ablagebereich, also Original, Ergebnis, Analysedatei und Zuordnungstabelle, und anschließend die Datenbankeinträge. Die Reihenfolge ist festgelegt, damit ein Fehler in der Mitte keine Dateien hinterlässt, auf die nichts mehr verweist. Mit den Datenbankeinträgen fällt der Schlüssel des Vorgangs weg; die Objekte sind danach auch dann unlesbar, wenn die Löschung im Speicher fehlgeschlagen ist. Deleting a case removes its entire storage prefix, that is the original, the result, the analysis file and the re-identification table, and afterwards the database records. The order is fixed so that an error in between leaves no files that nothing points to any more. The key of the case goes with the database records; the objects are then unreadable even if the delete against storage failed.

Der Auftragnehmer überprüft die Wirksamkeit dieser Maßnahmen mindestens jährlich und hält das Ergebnis schriftlich fest.

The Processor reviews the effectiveness of these measures at least once a year and records the result in writing.