

Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

- Verantwortlicher, nachfolgend „**Auftraggeber**“ genannt -

und

ReadSpeaker GmbH, Am Sommerfeld 7, 86825 Bad Wörishofen, Deutschland

- Auftragsverarbeiter, nachfolgend „**Auftragnehmer**“ genannt

§ 1 Gegenstand und Dauer des Auftrags

- (1) Der Gegenstand des Auftrags liegt in der Bereitstellung von ReadSpeaker TextAid und ergibt sich im Übrigen aus der Leistungsvereinbarung der Vertragspartner über die Zurverfügungstellung des Dienstes, auf das hier verwiesen wird (nachfolgend „**Leistungsvereinbarung**“). Gegenstand des Auftrags zum Datenumgang ist das Angebot einer SaaS mit Vorlese-Schreib- und Lernfunktionen. In diesem Zusammenhang werden zwangsläufig auch personenbezogene Daten verarbeitet.
- (2) Dieser Auftrag wird Bestandteil der Leistungsvereinbarung und ergänzt die Leistungsvereinbarung hinsichtlich der erforderlichen Regelungen zur Auftragsverarbeitung zwischen den Vertragspartnern.
- (3) Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung. Das Recht zur außerordentlichen fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Der Vertrag gilt unbeschadet des vorstehenden Absatzes so lange, wie der Auftragnehmer personenbezogene Daten des Auftraggebers verarbeitet.

§ 2 Auftragsinhalt

- (1) Nähere Beschreibung des Auftragsgegenstandes im Hinblick auf Art und Zweck der Aufgaben des Auftragnehmers: ReadSpeaker TextAid ist ein SaaS mit Vorlese- Schreib und Lernfunktionen. Nutzer loggen sich browserbasiert ein.
Die Erbringung der vertragsgegenständlichen Datenverarbeitung findet vorbehaltlich abweichender Vereinbarungen über die Einbindung eines Unterauftragnehmers (siehe unten, § 6) ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.
- (2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:
technische Logdaten: IP-Adresse und URL des Zugriffs auf den Dienst

(3) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- TextAid-User*innen

§ 3 Technische/organisatorische Maßnahmen

- (1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.
- (2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Die Einzelheiten hierzu haben die Vertragspartner in **Anlage 1** zu dieser Regelung zur Auftragsverarbeitung vereinbart.
- (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist der Auftragnehmer berechtigt, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 4 Berichtigung, Einschränkung und Löschung von Daten

- (1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.
- (2) Löschkonzept, Recht auf Vergessenwerden, Berichtigungsmöglichkeiten, Datenportabilität und die Möglichkeit der Auskunftserteilung sind nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

§ 5 Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß der DSGVO zu erfüllen; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Benennung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DSGVO ausübt. Der Auftragnehmer hat die Kontaktdaten des Datenschutzbeauftragten dem Auftraggeber zum Zwecke der Ermöglichung einer direkten Kontaktaufnahme mitzuteilen. Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen
- b) Der Auftragnehmer wahrt die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO. Er setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
- c) Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Anlage 1.
- d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.
- e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.
- f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer insoweit nach besten Kräften zu unterstützen.
- g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.
- h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach § 7 dieses Vertrages.

- i) Der Auftragnehmer unterstützt den Auftraggeber in seinem Verantwortungsbereich und soweit möglich im Rahmen bestehender Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen und stellt ihm die insoweit relevanten Informationen unverzüglich zur Verfügung.
- j) Soweit der Auftraggeber zur Durchführung einer Datenschutzfolgenabschätzung verpflichtet ist, unterstützt ihn der Auftragnehmer unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen. Gleiches gilt für eine etwaig bestehende Pflicht zur Konsultation der zuständigen Datenschutz-Aufsichtsbehörde.

§ 6 Unterauftragsverhältnisse

- (1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post-/ Transportdienstleistungen, zum Zwecke der allgemeinen Wartung und Erbringung von Benutzerservices in Anspruch nimmt sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers bei spezifisch ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.
- (2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) beauftragen. Erfolgt eine solche Beauftragung, ist der Auftragnehmer verpflichtet, dem Unterauftragnehmer dieselben Datenschutzpflichten aufzuerlegen, die im Vertrag zwischen Auftragnehmer und Auftraggeber festgelegt sind. Der Auftragnehmer wird dem Auftraggeber auf Anforderung die dazu geschlossene Vereinbarung – nur im datenschutzrechtlich relevanten Umfang – zugänglich machen. Die Unterauftragnehmer gem. der Anlage 2 zu diesem Vertrag gelten als genehmigt. Die Auslagerung auf weitere Unterauftragnehmer oder der Wechsel eines bestehenden Unterauftragnehmers sind nur zulässig, soweit:
 - der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
 - der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
 - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.
- (3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Der Auftragnehmer stellt ferner sicher, dass der Auftraggeber seine Rechte aus dieser Vereinbarung auch direkt gegenüber einem Unterauftragnehmer wahrnehmen kann.
- (4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen

sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen. Die konkret getroffenen Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus i.S.v. Art. 44 ff DSGVO sind in einer Anlage zu diesem Auftrag gesondert zu spezifizieren.

- (5) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Auftragnehmers in Textform. Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

§ 7 Kontrollrechte des Auftraggebers

- (1) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennendem Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- (2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.
- (3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:
 - den Beleg der Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;
 - die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;
 - aktuelle Testate unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzauditorien);
 - eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 8 Mitteilung bei Datenschutzverletzungen des Auftragnehmers

Der Auftragnehmer meldet dem Auftraggeber unverzüglich etwaige Verletzungen des Schutzes personenbezogener Daten in der Weise, dass der Auftraggeber seine gesetzlichen Pflichten, insbesondere nach Art. 33 und 34 DSGVO fristgerecht erfüllen kann. Der Auftragnehmer fertigt über den gesamten Vorgang einer Verletzung im vorgenannten Sinne eine Dokumentation an, die er dem Auftraggeber für weitere Maßnahmen zur Verfügung stellt.

§ 9 Weisungsbefugnis des Auftraggebers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten nur auf Basis dokumentierter Weisungen des Auftraggebers, es sei denn er ist nach dem Recht des Mitgliedstaats oder nach

Unionsrecht zu einer Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 S. 2 lit. a DSGVO). Mündliche Weisungen bestätigt der Auftraggeber unverzüglich in Textform. Die anfänglichen Weisungen und dauerhafte Weisungen des Auftraggebers werden durch die Leistungsvereinbarung und diesen Vertrag festgelegt.

- (2) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

§ 10 Löschung und Rückgabe personenbezogener Daten

- (1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherungskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- (2) Mit Beendigung der vertragsgegenständlichen Datenverarbeitungen, oder ggf. früher auf Weisung des Auftraggebers, hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit der Leistungsvereinbarung und/oder der Datenverarbeitung stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist dem Auftraggeber auf Anforderung vorzulegen. Ein Zurückbehaltungsrecht wird hinsichtlich der im Auftrag verarbeiteten Daten bzw. der dazu genutzten Datenträger ausgeschlossen.
- (3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

Ort, Datum, Unterschrift
Auftraggeber

Ort, Datum, Unterschrift
Auftragnehmer

Anlage 1: Technische/organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen: Alarmanlage, Absicherung von Gebäudeschächten, automatisches Zutrittskontrollsystem, Chipkarten-/RFID-Schließsystem, Schließanlage mit Codeschloss, manuelles Schließsystem, biometrische Zutrittsschranken, Videoüberwachung, Bewegungsmelder / Lichtschranken, Sicherheitsschlüssel, Schlüsselregelung, Personenkontrolle/Identitätskontrolle durch Pförtner/Rezeption, Protokollierung der Besucher, sorgfältige Auswahl des Reinigungspersonals, Pflicht zum Tragen von Berechtigungskarten und Besucherausweisen
- Zugangskontrolle
Berechtigungskonzept, Rechteverwaltung durch Systemadministrator, Reduzierung der Anzahl der Administratoren auf das erforderliche Minimum, Passwortkonzept inkl. Passwortlänge und Passwortwechsel, Physische Löschung von Datenspeichern vor der Wiederverwendung, Einsatz von Aktenvernichtern oder Dienstleistern zur sicheren Aktenvernichtung, Sichere Aufbewahrung von Mediengeräten
- Zugriffskontrolle
Zuweisung von Benutzerrechten, individuelle Benutzerprofile für jeden Benutzer, Passwortkonzept, Authentifizierung mit Benutzername / Passwort, 2-Faktor Authentifizierung, Zuteilung von Benutzerprofilen zu IT-Systemen, Einsatz von System zur Erkennung von Einbrüchen, Einsatz von Antivirensoftware, Einsatz einer Hardware-Firewall, VPN-Zugang zu internen Systemen von außen, Einsatz einer Software-Firewall
- Trennungskontrolle
Rechtevergabe für Datenbankbenutzer, Logische Mandantentrennung (software-seitig), Trennung von Produktiv- und Testsystemen
- Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen;

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

- Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport: Installation von dedizierten Einwahlen oder VPN-Tunneln, Weitergabe von Daten in anonymisierter oder pseudonymisierter Form, Dokumentation der Empfänger von Daten und die Zeiträume der geplanten Übermittlung oder vereinbarte Löschfristen, Beim physischen Transport: sichere Transportbehälter / Verpackung, Bei physischem Transport: sorgfältige Auswahl des Transportmittels, Personal und -Fahrzeuge
- Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Übersicht der Anwendungen, mit denen Datensätze eingegeben, geändert und gelöscht werden können

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust:
Unterbrechungsfreie Stromversorgung (USV) X Klimatisierung der Serverräume,
Geräte zur Überwachung von Temperatur und Luftfeuchtigkeit in Serverräumen,
Geschützte Steckdosen in Serverräumen,
Brand- und Rauchmeldeanlagen,
Feuerlöscher in Serverräumen,
Alarmmeldung bei unbefugtem Zutritt zu Serverräumen,
Backup & Recovery Konzept vorhanden,
Lagerung der Datensicherung an einem sicheren, ausgelagerten Ort,
Serverräume nicht unter Sanitäranlagen,
In hochwassergefährdeten Gebieten: Serverräume oberhalb der Wasserlinie
- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO):
Notfallmanagement inkl. Notfallpläne
Regelmäßige Tests der Wiederherstellbarkeit von Daten (mind. 1-2-mal pro Jahr)
Konzept zur Meldung von Vorfällen vorhanden, angekündigt und zugänglich für Arbeitgeber (Meldekette, Eskalationsstufen, ...)

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutz-Management: Die Geschäftsführung übernimmt die Verantwortung für die Einhaltung des Datenschutzes, z.B. durch die Bereitstellung der notwendigen Ressourcen. Ein Datenschutzkonzept ist veröffentlicht und wird regelmäßig gepflegt.
Datenschutzkonzept in schriftlicher Form
Regelmäßige Kontrollen und Überprüfungen / Versionierung / Aktualisierung
- Incident-Response-Management:
Notfallhandbücher sind vorhanden, angekündigt und jederzeit zugänglich.
Regelmäßige Penetrationstests / Code-Reviews / Audits
Meldewege eingerichtet und bekannt gemacht
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO):
Standardmäßig werden nur personenbezogene Daten verarbeitet, die für jeden spezifischen Zweck der Verarbeitung erforderlich sind.
- Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, Nachkontrollen, sorgfältige Auswahl der Auftragsverarbeiter im Hinblick auf Datensicherheitsmaßnahmen und Schutz der Rechte der betroffenen Person, Vorläufige Prüfung und Dokumentation der Sicherheitsmaßnahmen der vom Verarbeiter getroffenen Maßnahmen, Dokumentierte Anweisungen an den Auftragsverarbeiter (z.B. durch Datenverarbeitungsvertrag) im Sinne des Art.28 DS-GVO, Dokumentierte Verpflichtung des

Arbeitgebers des Auftragsverarbeiters zur Wahrung der Vertraulichkeit, die Verarbeiter haben
Datenschutzbeauftragte, Sicherstellung der Vernichtung von Daten nach der
Vertragsbeendigung, wirksame Kontrollrechte für den Auftragsverarbeiter, Laufende
Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

Anlage 2: Unterauftragnehmer:

DeepL

Die DeepL API wird in der Übersetzungsfunktion von TextAid verwendet.

Art der Verarbeitung: Bilder und/oder Sonstiges, Übersetzung von selbst eingegebenem Text (kann möglicherweise personenbezogene Daten im Inhalt enthalten).

Die Funktionalität ist optional durch die Bildungseinrichtung deaktivierbar.

Die Verarbeitung von Aktivierungen aus der Europäischen Union findet innerhalb der Europäischen Union statt.

Weitere Informationen zum Umgang mit Daten finden Sie auf den Seiten von DeepL:

<https://www.deepl.com/pro-data-security/>

ReadSpeaker AB

Art der Verarbeitung:

Kontaktdaten (sowohl von Studenten als auch von Angestellten), Teilnehmernummern in der Ausbildung, Studienverlauf.

Verarbeitung von Vorname, Nachname, E-Mail-Adresse, Passwort und Benutzerstatistiken von Benutzern.

Land der Verarbeitung: Schweden

Niederlassung: Schweden

Amazon AWS

Art der Verarbeitung:

In die TextAid-Bibliothek hochgeladene Dokumente werden auf AWS gespeichert.

Dokumente (können möglicherweise personenbezogene Daten im Inhalt enthalten). (Die Funktionalität kann von der Bildungseinrichtung deaktiviert werden)

Land der Verarbeitung: Irland

Informationen und Dokumente:

<https://aws.amazon.com/de/compliance/eu-data-protection/>

Microsoft Bing-Sprachausgabe

Art der Verarbeitung: Umwandlung von Sprache in Text (kann möglicherweise personenbezogene Daten im Inhalt enthalten).

Die Funktionalität ist optional durch die Bildungseinrichtung deaktivierbar.

Die Verarbeitung von Aktivierungen aus der Europäischen Union findet innerhalb der Europäischen Union statt.

Informationen und Dokumente:

<https://learn.microsoft.com/en-us/legal/cognitive-services/speech-service/speech-to-text/data-privacy-security#what-data-does-speech-to-text-process>

ABBYY Cloud OCR SDK.

Art der Verarbeitung:

Umwandlung von selbst eingegebenen Scans/Fotos/Bildern in Text-PDFs (kann möglicherweise personenbezogene Daten im Inhalt enthalten).

Die Funktionalität kann optional von der Bildungseinrichtung deaktiviert werden.

Die Verarbeitung von Aktivierungen aus der Europäischen Union findet innerhalb der Europäischen Union statt.

Informationen und Dokumente:

<https://www.abbyy.com/legal/cloud-terms-of-service/dpa-universal-data-processing/>