

Auftrag gemäß Art. 28 DS-GVO

Vereinbarung

Vertragsparteien

Auftraggeber:

Auftragnehmer / Auftragsverarbeiter:

LexLogik UG

Mahlgasse 4 , 88339 Bad Waldsee

Deutschland

(vertreten d. d. Geschäftsführer Jonas Maximilian Regul)

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand und Dauer des Auftrags bestimmen sich vorrangig nach dem jeweiligen Hauptvertragsverhältnis zwischen den Parteien über die Nutzung der von der Auftragnehmerin bereitgestellten Software- und Cloud-Dienstleistungen („Hauptvertrag“), soweit dort nicht ausdrücklich Abweichendes vereinbart ist.

(2) Die Auftragnehmerin erbringt Dienstleistungen zur technischen Verarbeitung von Dokumenten und zugehörigen Inhalten, die der Auftraggeber über die Plattform einstellt oder anderweitig im vertraglich vereinbarten Umfang übersendet. Die Verarbeitung erfolgt

ausschließlich im Auftrag und nach Weisung des Auftraggebers im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Auftrags.

(3) Die Auftragnehmerin verfolgt ein Zero-Retention-Paradigma. Inhaltsdaten des Auftraggebers werden ausschliesslich im flüchtigen Arbeitsspeicher (RAM) für die Dauer der technischen Analyse verarbeitet. Eine persistente Speicherung auf physischen Datenträgern erfolgt nicht. Nach Abschluss des Analysevorgangs werden sämtliche Inhaltsdaten im Arbeitsspeicher unwiderruflich gelöscht..

(4) Soweit im Rahmen des Betriebs der Plattform technische Metadaten (z. B. Protokolle zu Zugriffen, Fehlern, Performance) unvermeidlich anfallen, werden diese nur in dem Umfang verarbeitet, der für Betrieb, Sicherheit und Nachweisbarkeit erforderlich ist, und unter Beachtung der gesetzlichen Vorgaben sowie der Anlage 2 (TOM).

2. Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung von Daten

(1) Der Umfang, die Art und der Zweck der Verarbeitung personenbezogener Daten sowie die Kategorien personenbezogener Daten und der Kreis der Betroffenen ergeben sich aus dem Hauptvertrag und der vom Auftraggeber ggf. ausgefüllten Anlage 1, soweit sich nichts Abweichendes bereits aus dem Hauptvertrag ergibt.

(2) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt, soweit nicht ausdrücklich etwas anderes vereinbart ist.

(3) Jede beabsichtigte Verlagerung der Verarbeitung personenbezogener Daten in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (einschließlich geeigneter Garantien und dokumentierter Risikobewertung, soweit erforderlich).

3. Technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

(1) Die Auftragnehmerin hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn bzw. vor Fortsetzung der Verarbeitung zu dokumentieren und dem Auftraggeber auf Anforderung zur Prüfung zur Verfügung zu stellen (Anlage 2). Mit vertraglicher Verweisung auf die aktuelle

Anlage 2 oder deren Anerkennung durch den Auftraggeber werden diese Maßnahmen Bestandteil des Auftrags.

(2) Die Auftragnehmerin gewährleistet ein dem Risiko angemessenes Schutzniveau gemäß Art. 28 Abs. 3 Satz 2 lit. c, Art. 32 DS-GVO i. V. m. Art. 5 Abs. 1 und 2 DS-GVO. Zu berücksichtigen sind insbesondere der Stand der Technik, die Implementierungskosten sowie Art, Umfang und Zwecke der Verarbeitung sowie unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Die Auftragnehmerin darf gleichwertige oder verbesserte Maßnahmen umsetzen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen der Maßnahmen sind zu dokumentieren und dem Auftraggeber mitzuteilen, soweit dies für die Rechte des Auftraggebers von Bedeutung ist.

4. Berichtigung, Sperrung und Löschung von Daten

(1) Nach Abschluss der jeweiligen Verarbeitung oder auf Weisung des Auftraggebers hat die Auftragnehmerin die im Auftrag verarbeiteten Inhaltsdaten unverzüglich zu löschen oder zurückzugeben, soweit keine gesetzliche Aufbewahrungspflicht der Auftragnehmerin entgegensteht.

(2) Soweit vom Leistungsumfang des Hauptvertrags umfasst, unterstützt die Auftragnehmerin den Auftraggeber bei der Erfüllung von Rechten der Betroffenen (z. B. Auskunft, Berichtigung, Löschung, Datenübertragbarkeit), soweit dies technisch möglich und mit angemessenem Aufwand verbunden ist und der Auftraggeber die erforderlichen Weisungen erteilt hat.

5. Qualitätssicherung und sonstige Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin erfüllt die Pflichten aus Art. 28 bis 33 DS-GVO, soweit diese auf Auftragsverarbeiter anwendbar sind, und insbesondere:

- Vertraulichkeit gemäß Art. 28 Abs. 3 Satz 2 lit. b, Art. 29, Art. 32 Abs. 4 DS-GVO;
- Einsatz von Personen, die auf die Vertraulichkeit verpflichtet und mit den für sie relevanten datenschutzrechtlichen Vorgaben vertraut gemacht wurden;
- Verarbeitung personenbezogener Daten ausschließlich gemäß Weisung des Auftraggebers und diesem Vertrag, es sei denn, die Auftragnehmerin ist gesetzlich zur Verarbeitung verpflichtet;

- Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 Satz 2 lit. c, Art. 32 DS-GVO und Anlage 2.

(2) Die Auftragnehmerin informiert den Auftraggeber unverzüglich, wenn ihr eine Weisung des Auftraggebers rechtswidrig oder aus Sicht der Auftragnehmerin mit Datenschutzrecht unvereinbar erscheint.

(3) Die Auftragnehmerin arbeitet auf Anfrage des Auftraggebers mit der Aufsichtsbehörde zusammen, soweit dies im Rahmen des Auftrags erforderlich und zumutbar ist.

(4) Die Auftragnehmerin informiert den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt entsprechend, soweit Behörden im Zusammenhang mit der Auftragsverarbeitung bei der Auftragnehmerin ermitteln, soweit eine Mitteilung rechtlich zulässig ist.

(5) Soweit der Auftraggeber aufgrund der Auftragsverarbeitung Ansprüchen Dritter oder Betroffener ausgesetzt ist, unterstützt die Auftragnehmerin den Auftraggeber nach den gesetzlichen Vorgaben und im zumutbaren Umfang, insbesondere durch Bereitstellung erforderlicher Informationen, soweit diese bei der Auftragnehmerin vorliegen.

(6) Die Auftragnehmerin überprüft regelmäßig ihre internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um eine Verarbeitung im Einklang mit den Anforderungen des anwendbaren Datenschutzrechts zu gewährleisten.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Vereinbarung sind solche Leistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen (insbesondere Hosting, Betrieb von Rechenzentrumskapazität, infrastrukturelle Dienstleistungen, soweit sie der Verarbeitung im Auftrag dienen).

(2) Nicht hierzu zählen insbesondere allgemeine Hilfs- und Nebenleistungen, die die Auftragnehmerin ohne besondere Einbindung in die Auftragsverarbeitung in Anspruch nimmt (z. B. Telekommunikation, Post-/Transportdienstleistungen, allgemeine Büroorganisation), sofern keine Zugriffe auf personenbezogene Daten des Auftraggebers erfolgen oder diese nur im unvermeidbaren technischen Rahmen erfolgen. Für solche Nebenleistungen wählt die Auftragnehmerin zuverlässige Anbieter und trifft angemessene Datenschutzvorkehrungen.

(3) Die Auftragnehmerin darf Unterauftragsverarbeiter nur im Rahmen der gesetzlichen Vorgaben einsetzen. Soweit erforderlich, wird der Auftraggeber über beabsichtigte

Änderungen bei der Zulassung oder dem Ersatz weiterer Unterauftragsverarbeiter informiert oder erhält ein Widerspruchsrecht gemäß den Regelungen des Hauptvertrags.

(4) Die Auftragnehmerin stellt sicher, dass die Unterauftragsverarbeiter dieselben datenschutzrechtlichen Schutzpflichten einhalten, wie sie in diesem Vertrag vereinbart sind, insbesondere durch Verträge gemäß Art. 28 Abs. 4 DS-GVO.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, nach vorheriger Ankündigung in angemessenem Umfang und zu angemessenen Zeiten Überprüfungen der Einhaltung der Vorgaben aus Art. 28 DS-GVO sowie dieser Vereinbarung durchzuführen oder durch einen von ihm benannten, von der Auftragnehmerin nicht unbillig abzulehnenden Dritten durchführen zu lassen.

(2) Die Auftragnehmerin stellt auf Anforderung die erforderlichen Auskünfte zur Verfügung und weist die Umsetzung der technischen und organisatorischen Maßnahmen nach, soweit dem Auftraggeber ein Prüfbedarf im Rahmen des Art. 28 DS-GVO zusteht.

(3) Kosten: Überprüfungen, die auf ein nachweisbares Fehlverhalten der Auftragnehmerin zurückzuführen sind, trägt die Auftragnehmerin. Im Übrigen können die Parteien angemessene Vergütung für die Durchführung von Prüfungen vereinbaren, soweit der Aufwand nicht bereits durch den Hauptvertrag abgedeckt ist.

8. Mitteilung bei Verstößen und Unterstützungspflichten

(1) Die Auftragnehmerin unterstützt den Auftraggeber bei der Erfüllung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten, soweit dies im Rahmen des Auftrags und mit angemessenem Aufwand möglich ist. Hierzu gehören insbesondere:

a) technische und organisatorische Maßnahmen, die ein angemessenes Schutzniveau berücksichtigen und die Feststellung relevanter Vorfälle ermöglichen, soweit vereinbart;

b) die unverzügliche Meldung einer festgestellten Verletzung des Schutzes personenbezogener Daten an den Auftraggeber, sofern die Meldung gegenüber dem Auftraggeber aus Sicht der Auftragnehmerin erforderlich ist;

c) die Bereitstellung relevanter Informationen an den Auftraggeber, soweit der Auftraggeber gegenüber Betroffenen oder Behörden informationspflichtig ist und die Informationen bei der Auftragnehmerin vorliegen;

d) die Unterstützung bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen, soweit vereinbart und zumutbar.

(2) Für Unterstützungsleistungen, die nicht im Leistungsumfang des Hauptvertrags enthalten sind und nicht auf ein schuldhaftes Verhalten der Auftragnehmerin zurückzuführen sind, kann eine gesonderte Vergütung vereinbart werden.

9. Weisungsbefugnis des Auftraggebers

(1) Weisungen des Auftraggebers zur Verarbeitung personenbezogener Daten erteilt der Auftraggeber grundsätzlich in Textform oder in der im Hauptvertrag vereinbarten Form (z. B. über die Plattform-Funktionen).

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich auf Textform, soweit sie erteilt werden.

(3) Die Auftragnehmerin informiert den Auftraggeber unverzüglich, wenn eine Weisung aus Sicht der Auftragnehmerin gegen Datenschutzvorschriften verstößt. Die Auftragnehmerin darf die Durchführung der betreffenden Weisung aussetzen, bis sie vom Auftraggeber bestätigt oder geändert wurde, sofern ein gesetzliches Verbot nicht ohnehin entgegensteht.

10. Löschung und Rückgabe personenbezogener Daten

(1) Kopien oder Duplikate der Inhaltsdaten werden nicht ohne Wissen des Auftraggebers erstellt. Hiervon unberührt bleiben technisch notwendige temporäre Speicherungen im Rahmen der Verarbeitung sowie Daten, deren Aufbewahrung der Auftragnehmerin gesetzlich auferlegt ist.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder auf Aufforderung des Auftraggebers – spätestens mit Beendigung des Hauptvertrags – hat die Auftragnehmerin sämtliche Inhaltsdaten und, soweit vereinbart, Verarbeitungsergebnisse dem Auftraggeber herauszugeben oder nach dokumentierter Weisung datenschutzkonform zu löschen, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Gleiches gilt für Test- und Ausschussmaterial, soweit solches angefallen ist.

(3) Nachweisdokumentationen, die der Nachweis der auftrags- und ordnungsgemäßen Verarbeitung dienen, bewahrt die Auftragnehmerin gemäß gesetzlicher oder nachgewiesener

Aufbewahrungsfristen auf und kann sie zum Nachweis gegenüber Behörden verwenden. Auf Anforderung des Auftraggebers kann eine Übergabe zum Zwecke der Aufbewahrung beim Auftraggeber vereinbart werden.

11. Sonstige Vereinbarungen

11.1 Entgelte

(1) Für diesen Auftragsverarbeitungsvertrag wird kein gesondertes Entgelt verlangt, soweit nicht ausdrücklich anderes vereinbart ist (z. B. im Hauptvertrag).

(2) Soweit der Auftraggeber Unterstützungsleistungen gemäß Ziff. 4 oder 8 in einem Umfang anfordert, der über die im Hauptvertrag vereinbarten Leistungen hinausgeht, kann eine angemessene Vergütung vereinbart werden.

(3) Soweit der Auftraggeber Kontrollen gemäß Ziff. 7 in einem Umfang ausübt, der über das übliche Maß hinausgeht, kann eine angemessene Vergütung nach vorheriger Vereinbarung (z. B. nach Zeitaufwand) erfolgen.

11.2 Vertragsdauer

(1) Diese Vereinbarung ist abhängig vom Bestand des Hauptvertrags gemäß Ziff. 1. Die Kündigung oder anderweitige Beendigung des Hauptvertrags beendet diese Vereinbarung gleichzeitig, soweit nicht gesetzlich etwas anderes gilt.

(2) Das Recht zur außerordentlichen Kündigung aus wichtigem Grund sowie gesetzliche Rücktrittsrechte bleiben unberührt.

11.3 Rechtswahl

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des Kollisionsrechts, soweit zulässig.

11.4 Gerichtsstand

Ist der Auftraggeber Kaufmann im Sinne des Handelsgesetzbuchs, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen, ist für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag – soweit gesetzlich zulässig – der Gerichtsstand am Sitz der Auftragnehmerin (88339 Bad Waldsee) ausschließlich zuständig.

11.5 Internationale Anwendbarkeit

Soweit auf die Verarbeitung das Datenschutzrecht der Schweiz oder des Vereinigten Königreichs (UK) anwendbar ist, gelten alle Verweise auf die DS-GVO in diesem Vertrag als Verweise auf die entsprechenden, materiell vergleichbaren Regelungen des Schweizer DSG bzw. der UK GDPR.

Unterschriften

Auftraggeber

Auftragnehmerin

LexLogik UG, vertreten d. d. Geschäftsführer

Jonas Maximilian Regul

Anlagen

Anlage 1 zum Auftrag gemäß Art. 28 DS-GVO

Auflistung der personenbezogenen Daten und Zweck ihrer Verarbeitung

Art der Daten

Gegenstand der Vereinbarung sind folgende Datenarten und -Kategorien:

- Personenstammdaten (z. B. Namen, Anreden)
- Kommunikationsdaten (z. B. E-Mail-Adressen, Telefonnummern, falls eingegeben oder in Dokumenten enthalten)
- Vertrags- und Geschäftsstammdaten (z. B. Aktenzeichen, Referenzen in Dokumenten)
- Inhaltsdaten aus Dokumenten (z. B. Texte, Bilder, Metadaten in Dateien, soweit technisch vorhanden)
- technische Nutzungs- und Protokolldaten im zumutbaren Umfang (z. B. zur Sicherstellung des Betriebs und der Integrität der Dienste)

Kreis der Betroffenen

Der Kreis der durch diese Zusatzvereinbarung Betroffenen umfasst:

- Kunden und Interessenten des Auftraggebers

Anlage 2 zum Auftrag gemäß Art. 28 DS-GVO

Technische und organisatorische Maßnahmen (TOM) nach Art. 32 DS-GVO und Anlage

I. Vertraulichkeit

Die Auftragnehmerin setzt keine eigenen Server sondern von einem deutschen Hostinganbieter gemietete Server ein. Dabei stellt die Auftragnehmerin sicher, dass der Hostinganbieter die

erforderlichen Sicherheitsmaßnahmen umsetzt.

- Zugangskontrollen
- Zugriffskontrollen
- Datenträgerkontrollen
- Trennungskontrolle

II. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DS-GVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang der Leistungsbeschreibung des Hauptauftrages zur Verfügung gestellt.

Eingabekontrolle

bei Verwaltungssystemen der Auftragnehmerin:

- Die Daten werden vom Auftraggeber selbst eingegeben bzw. erfasst.
- Änderungen der Daten werden protokolliert.

für die Dienstleistung der Auftragnehmerin:

- Die Daten werden vom Auftraggeber selbst übertragen.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Die Auftragnehmerin stellt sicher, dass ihre Dienstleistung eine hohe Verfügbarkeit aufweist. Da sie über die einzelnen Cloud-Bearbeitungsvorgänge hinaus keine Auftraggeberdaten verarbeitet oder speichert, unterliegen diese keinen besonderen Verfügbarkeitsanforderungen