

Auftragsverarbeitungsvertrag

zwischen Kunde (»Auftraggeber«) und Anbieter (»Auftragnehmer«)

1. Vertragsgegenstand:

Gegenstand des Vertrages ist die Verarbeitung personenbezogener Daten im Auftrag (im Folgenden: »Auftragsverarbeitung«) gemäß Art. 28 DSGVO. Dieser Vertrag ergänzt den zwischen den Parteien geschlossenen Vertrags über die Nutzung von Beck-Noxtua (im Folgenden: »Hauptvertrag«).

2. Laufzeit:

Die Laufzeit der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages und endet gleichzeitig mit dieser, ohne dass eine gesonderte Kündigung erforderlich ist.

3. Art und Zweck der Verarbeitung:

Die Verarbeitung personenbezogener Daten erfolgt, um dem Auftraggeber die Funktionalität der KI-Anwendung »Beck-Noxtua« bereitzustellen.

4. Art der personenbezogenen Daten und Kategorien betroffener Personen

Gegenstand der Auftragsverarbeitung sind folgende Arten personenbezogener Daten:

- von einem berechtigten Nutzer für die Verarbeitung durch „Beck-Noxtua“ bereitgestellte Informationen, z.B. Inhalte von elektronischen Dokumenten und Eingaben („Prompts“);
- der von "Beck-Noxtua" zurückgelieferte KI-Output (Prompts und KI-Output zusammen: „Chat“);

Nicht Gegenstand der Auftragsverarbeitung sind folgende Arten personenbezogener Daten:

- Name, Kontaktdaten der berechtigten Nutzer
- Log-in-Daten der berechtigten Nutzer, IP-Adressen
- Protokolldaten und Daten über die Inanspruchnahme von „Beck-Noxtua“ (Nutzungszeiten)

Diese Daten werden zur Erfüllung des zwischen den Parteien geschlossenen Hauptvertrags in eigener Verantwortung des Anbieters verarbeitet. Dies umfasst auch Vertriebsdienstleistungen und den Kundendienst.

4.2 **Betroffene Personen** im Rahmen der Auftragsverarbeitung sind **berechtigte Nutzer und weitere natürliche Personen**, auf die sich Informationen beziehen, die als Inhalte von elektronischen Dokumenten und Eingaben (»Prompts«) für die Verarbeitung durch »Beck-Noxtua« bereitgestellt werden.

4.3 Temporäre Speicherung der Chats

Chats werden temporär für einen Zeitraum von bis zu 8 Stunden auf dem Server gespeichert. Der Kunde hat die Optionen, diesen Zeitraum zu verlängern.

5. Technische und organisatorische Maßnahmen

- 5.1 Der Auftragnehmer dokumentiert die von ihm getroffenen technischen und organisatorischen Maßnahmen (»TOM«). Die TOM des Auftragnehmers sind in der aktuellen Fassung in der »Übersicht TOM Verlag C.H.Beck« dargestellt. Sie werden Grundlage des Vertrages.
- 5.2 Der Auftragnehmer ergreift die erforderlichen TOM zur Gewährleistung der Datensicherheit und eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sowie der raschen Wiederherstellbarkeit der Verfügbarkeit und des Zugangs zu personenbezogenen Daten. Er berücksichtigt dabei den Stand der Technik und die Implementierungskosten sowie Art,

Umfang und Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen gemäß Art. 32 DSGVO.

- 5.3 Die TOM unterliegen dem technischen Fortschritt und der Weiterentwicklung. Daher ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der nach Ziffer 5.1 festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

6. Pflichten des Auftragnehmers

6.1 Ansprechpartner der Parteien

- Ansprechpartner beim Auftragnehmer ist:
Dr. Dr. Oliver Hofmann; E-Mail: oliver.hofmann@beck-noxtua.de
- Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers: E-Mail: datenschutzbeauftragter@beck.de
- Zur Erteilung von Weisungen im Namen des Auftraggebers ist der vom Auftraggeber zu benennende Ansprechpartner beim Auftraggeber befugt. Der Auftraggeber teilt dem Auftragnehmer Namen und Kontaktdaten dieses Ansprechpartners unverzüglich nach Vertragsschluss schriftlich mit.

Der Auftraggeber hat Weisungen im Sinne von Art. 28 Abs. 1 Satz 2 Buchst. a DSGVO stets an den Ansprechpartner beim Auftragnehmer zu richten.

6.2 Verpflichtung auf die Vertraulichkeit: Alle Mitarbeiter, die im Rahmen der Auftragsverarbeitung auf personenbezogene Daten des Auftraggebers zugreifen können, müssen zuvor auf die Vertraulichkeit verpflichtet worden sein. Der Auftragnehmer und dem Auftragnehmer unterstellt Personen, die im Rahmen der Auftragsverarbeitung Zugang zu personenbezogenen Daten haben, dürfen diese Daten gemäß Art. 29 DSGVO ausschließlich auf Weisung des Auftraggebers verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

6.3 Zusammenarbeit mit Aufsichtsbehörden: Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

6.4 Unverzügliche Information des Auftraggebers über Kontrollen und Maßnahmen der Aufsichtsbehörde: Der Auftragnehmer informiert den Auftraggeber unverzüglich über alle Kontrollen und sonstigen Maßnahmen einer Aufsichtsbehörde, die die Auftragsverarbeitung betreffen.

6.5 Unterstützung des Auftraggebers: Ist der Auftraggeber einer Kontrolle einer 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, unterstützt ihn der Auftragnehmer angemessen. Der Auftragnehmer unterstützt den Auftraggeber ferner im Rahmen seiner Pflichten gemäß Kapitel III DSGVO gegenüber der betroffenen Person zu und stellt alle relevanten Informationen unverzüglich zur Verfügung; er unterstützt den Auftraggeber bei einer Datenschutz-Folgenabschätzung des Auftraggebers und im Rahmen einer Konsultation mit der Aufsichtsbehörde.

- 6.6 Dokumentation der technischen und organisatorischen Maßnahmen: Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zum Nachweis der Einhaltung seiner Pflichten zur Verfügung. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditeure, Qualitätsauditeure) oder eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit vorlegen.
- 6.7 Datenschutzverletzungen: Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn durch ihn oder eine ihm unterstellte Personen gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder Verpflichtungen aus dem vorliegenden Vertrag verstößen wurde.

7. Ort der Verarbeitung personenbezogener Daten

Die Datenverarbeitung findet ausschließlich in der Europäischen Union oder dem EWR statt.

8. Unterauftragsverhältnisse

- 8.1 Sollen Unterauftragnehmer (weitere Auftragsverarbeiter gemäß Art. 28 DSGVO) einbezogen werden sollen, gilt:
- Die Einschaltung von Unterauftragnehmern ist nur mit schriftlicher Zustimmung des Auftraggebers gestattet. Ohne eine solche Zustimmung kann der Auftragnehmer zur Vertragsdurchführung einen Unterauftragnehmer mit der gesetzlich gebotenen Sorgfalt einsetzen, wenn er dies dem Auftraggeber vor Beginn der Verarbeitung schriftlich mitgeteilt hat und der Auftraggeber der Unterbeauftragung nicht innerhalb eines Monats nach Zugang der Mitteilung schriftlich widersprochen hat.
 - Der Auftragnehmer gestaltet die vertraglichen Vereinbarungen mit dem Unterauftragnehmer so, dass sie Art. 28 DSGVO entsprechen.
- 8.2 Die vorstehenden Regelungen gelten entsprechend, wenn der Unterauftragnehmer seinerseits ein Unterauftragsverhältnis begründen will.
- 8.3 Erbringt der Unterauftragnehmer seine Leistungen nicht in der EU oder dem EWR stellt der Auftragnehmer sicher, dass die Verarbeitung personenbezogener Daten gemäß Art. 44 ff. DSGVO zulässig ist.
- 8.4 Abweichend von Ziffer 8.1, erster Spiegelstrich, gestattet der Auftraggeber bereits jetzt die Einschaltung des Unterauftragnehmers Noxtua AG, Große Hamburger Str. 17, 10115 Berlin (technischer Betrieb der KI-Anwendung); sowie als Auftragnehmer von Noxtua AG:
Telekom Deutschland GmbH, Landgrabenweg 151, 53227 Bonn und IONOS SE, Elgendorfer Straße 57, 56410 Montabaur.

9. Weisungsbefugnis des Auftraggebers

- 9.1 Der Auftraggeber hat ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung, das er durch Einzelweisungen konkretisieren kann. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich schriftlich.
- 9.2 Der Auftragnehmer darf nur nach dokumentierter Weisung des Auftraggebers Daten berichtigen, löschen oder ihre Verarbeitung einschränken. Wendet sich eine betroffene Person an den Auftragnehmer, leitet dieser das Ersuchen an den Auftraggeber weiter. Auskünfte darf der Auftragnehmer nur nach vorheriger Zustimmung in Textform durch den Auftraggeber erteilen.
- 9.3 Der Auftragnehmer verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien werden ohne Wissen des Auftraggebers nicht erstellt. Hierzu ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.
- 9.4 Der Auftragnehmer verarbeitet gemäß Ziffer 9.1 bis 9.3 die Daten nur auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; 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.

10. Kontrollrechte des Auftraggebers

- 10.1 Der Auftraggeber hat das Recht, Kontrollen im Benehmen mit dem Auftragnehmer durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobekontrollen, die rechtzeitig anzumelden sind, von der Einhaltung der vertraglichen Pflichten durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.
- 10.2 Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragnehmer dem Auftraggeber auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO nach.

11. Löschung von Daten

- 11.1 Nach Aufforderung durch den Auftraggeber sowie unaufgefordert bei Beendigung der Auftragsverarbeitung wird der Auftragnehmer sämtliche in seinen Besitz gelangte Datenbestände mit personenbezogenen Daten, die im Zusammenhang mit der Auftragsverarbeitung stehen, datenschutzgerecht vernichten/löschen.
- 11.2 Der Auftragnehmer hat an personenbezogenen Daten und Datenträgern kein Zurückbehaltungsrecht.

12. Schlussbestimmungen

Für die Schriftform und den Gerichtsstand gelten die Bestimmungen des Hauptvertrags.