

Nutzungsbedingungen für die AI as a Service Plattform AuxData.ai



AuxData.ai

ist eine Marke der

AuxData Space GmbH

Benzstr. 8

86356 Neusäß

Nutzungsbedingungen für die AI as a Service Plattform

AuxData.ai ist eine Marke der AuxData Space GmbH Benzstr. 8 86356 Neusäß

1. Einleitung

AuxData.ai bietet Ihnen die Nutzung von AuxData.ai als AI as a Service (SaaS) Plattform an. Diese Nutzungsbedingungen legen die rechtlichen Grundlagen für die Nutzung der Plattform fest. Durch die Nutzung der Plattform erklären Sie sich mit diesen Nutzungsbedingungen einverstanden.

2. Geltungsbereich

Diese Nutzungsbedingungen gelten für alle Nutzer der AuxData.ai Plattform. Die Plattform kann von natürlichen Personen ab 18 Jahren und Unternehmen genutzt werden. Die Nutzung der Plattform durch Minderjährige ist nicht gestattet.

3. Registrierung und Zugangsdaten

Um die Plattform nutzen zu können, müssen Sie Ihre Organisation registrieren und einen Benutzernamen und ein Passwort wählen. Sie sind für die Geheimhaltung Ihrer Zugangsdaten verantwortlich und haften für jegliche Nutzung Ihres Benutzerkontos.

4. Leistungsumfang der Plattform

Die Plattform bietet verschiedene Funktionen, darunter die Verarbeitung von natürlicher Sprache und künstlicher Intelligenz. AuxData.ai behält sich das Recht vor, den Funktionsumfang der Plattform jederzeit zu erweitern oder zu ändern.

5. Datenschutz

AuxData.ai verpflichtet sich, Ihre personenbezogenen Daten gemäß den geltenden Datenschutzgesetzen und -richtlinien zu schützen. Weitere Informationen zum Datenschutz finden Sie in der Datenschutzerklärung der Plattform.

6. Nutzungsrechte

Sie sind berechtigt, die Plattform für den persönlichen oder geschäftlichen Gebrauch gemäß diesen Nutzungsbedingungen zu nutzen. Es ist Ihnen nicht gestattet, die Plattform oder deren Inhalte zu verändern, zu kopieren, zu verbreiten oder für gewerbliche oder kommerzielle Zwecke ohne vorherige schriftliche Genehmigung von AuxData.ai zu nutzen.

7. Haftungsausschluss

AuxData.ai übernimmt keine Gewährleistung für die Richtigkeit, Vollständigkeit oder Aktualität der auf der Plattform bereitgestellten Informationen. AuxData.ai haftet nicht für Schäden, die durch die Nutzung oder die Unmöglichkeit der Nutzung der Plattform entstehen, es sei denn, der Schaden beruht auf Vorsatz oder grober Fahrlässigkeit von AuxData.ai.

KI-spezifischer Haftungsausschluss: AuxData.ai haftet nicht für Entscheidungen, die der Kunde auf Basis von KI-generierten Inhalten oder automatisierten Ausgaben der

Plattform trifft. Die fachliche Überprüfung und Bewertung von KI-Outputs sowie die Verantwortung für deren Verwendung obliegt ausschließlich dem Kunden.

8. Änderungen der Nutzungsbedingungen

AuxData.ai behält sich das Recht vor, diese Nutzungsbedingungen jederzeit zu ändern. Änderungen werden auf der Plattform veröffentlicht und treten mit ihrer Veröffentlichung in Kraft. Durch die weitere Nutzung der Plattform nach einer Änderung stimmen Sie den geänderten Nutzungsbedingungen zu.

9. Anwendbares Recht und Gerichtsstand

Diese Nutzungsbedingungen unterliegen dem Recht der Bundesrepublik Deutschland. Ausschließlicher Gerichtsstand für Streitigkeiten im Zusammenhang mit diesen Nutzungsbedingungen und der Nutzung der Plattform ist Augsburg.

10. KI-Regulierung und Pflichten nach dem EU AI Act (NEU)

10.1 Rollenklarstellung — Anbieter und Betreiber

AuxData Space GmbH stellt die Plattform als **Anbieter (Provider)** im Sinne von Art. 3 Nr. 3 der Verordnung (EU) 2024/1689 (EU AI Act) zur Verfügung.

Der Kunde ist **Betreiber (Deployer)** im Sinne von Art. 3 Nr. 4 EU AI Act für alle KI-Systeme, die er auf der Plattform konfiguriert und betreibt — insbesondere für selbst angelegte Agenten, AI Services, Workflows und Wissensdatenbanken.

Die regulatorischen Pflichten des Betreibers nach Art. 26 EU AI Act obliegen dem Kunden eigenverantwortlich und können nicht auf AuxData Space GmbH übertragen werden.

10.2 Verbotene KI-Praktiken

Die Nutzung der Plattform für die folgenden Zwecke ist ausdrücklich untersagt (Art. 5 Verordnung (EU) 2024/1689, gültig seit Februar 2025):

- **(a)** Unterschwellige oder manipulative Beeinflussung von Personen ohne deren Wissen
- **(b)** Ausnutzung von Schutzbedürftigkeit bestimmter Personengruppen, insbesondere Kinder oder ältere Menschen
- **(c)** Bewertung oder Klassifizierung natürlicher Personen durch öffentliche Behörden auf Grundlage ihres sozialen Verhaltens (Social Scoring)
- **(d)** Echtzeit-biometrische Fernidentifizierung von Personen im öffentlichen Raum
- **(e)** Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen
- **(f)** Biometrische Kategorisierung von Personen nach sensiblen Merkmalen wie ethnischer Herkunft, politischer Überzeugung, Religionszugehörigkeit, sexueller Orientierung oder ähnlichen Merkmalen

Ein Verstoß gegen diese Bestimmungen berechtigt AuxData Space GmbH zur **sofortigen Sperrung des Plattformzugangs** ohne vorherige Abmahnung. Schadensersatzansprüche bleiben vorbehalten.

10.3 Transparenzpflichten gegenüber Endnutzern

Der Kunde ist verpflichtet sicherzustellen, dass Endnutzer seiner auf der Plattform konfigurierten KI-Systeme — insbesondere Chatbots, Agenten und AI Services — **erkennbar darüber informiert werden, dass sie mit einem KI-System interagieren** (Art. 50 Verordnung (EU) 2024/1689, gültig ab 2. August 2026).

Dies umfasst insbesondere:

- Die eindeutige Kennzeichnung von Chatbots und KI-Agenten als solche gegenüber dem Endnutzer zu Beginn der Interaktion
- Die Kennzeichnung KI-generierter Inhalte aus AI Services als maschinell erzeugt
- Das Verbot, konfigurierte Personas oder Avatare so zu gestalten, dass Endnutzer über die KI-Natur des Systems getäuscht werden

AuxData Space GmbH stellt die technische Grundlage für die Erfüllung dieser Pflicht bereit. Die organisatorische und inhaltliche Umsetzung liegt in der Verantwortung des Kunden.

10.4 Pflicht zur eigenverantwortlichen Risikobewertung

Vor der Produktivschaltung selbst konfigurierter Agenten, AI Services oder Workflows ist der Kunde verpflichtet, eigenverantwortlich zu prüfen, ob der geplante Einsatzfall die Kriterien eines **Hochrisiko-KI-Systems nach Anhang III der Verordnung (EU) 2024/1689** erfüllt.

Risikorelevante Einsatzbereiche umfassen insbesondere:

- Personalentscheidungen (z. B. Bewerberauswahl, Leistungsbewertung)
- Kreditvergabe und Versicherungsentscheidungen
- Bildungszugang und Prüfungsbewertungen
- Kritische Infrastrukturen
- Strafverfolgung und Justiz
- Biometrische Identifikation

Das Ergebnis dieser Risikobewertung ist vom Kunden zu **dokumentieren**. Der Kunde informiert AuxData Space GmbH, wenn ein Hochrisiko-Einsatz geplant ist. AuxData Space GmbH stellt auf Anfrage Dokumentationsvorlagen zur Verfügung.

10.5 KI-Kompetenz der Mitarbeiter

Der Kunde bestätigt, dass er geeignete Maßnahmen ergriffen hat oder ergreift, um eine **ausreichende KI-Kompetenz** derjenigen Mitarbeiter sicherzustellen, die die Plattform konfigurieren oder betreiben (Art. 4 Verordnung (EU) 2024/1689, gültig seit Februar 2025).

Dies betrifft insbesondere Organisations-Administratoren und Agenten-Administratoren, die eigenständig KI-Systeme auf der Plattform einrichten und verantworten.

10.6 Menschliche Aufsicht bei automatisierten Entscheidungen

Bei der Konfiguration von Workflows und Agenten, die automatisierte Entscheidungen mit Auswirkungen auf natürliche Personen treffen, ist der Kunde verpflichtet:

- **Kompetente Personen** zu benennen, die für die menschliche Aufsicht dieser Systeme zuständig sind
- Sicherzustellen, dass eine menschliche Überprüfung von Entscheidungen mit Auswirkungen auf Gesundheit, Sicherheit oder Grundrechte von Personen **technisch und organisatorisch gewährleistet** ist
- Vollautomatisierte Entscheidungen ohne Überprüfungsmöglichkeit in risikorelevanten Bereichen zu unterlassen

10.7 Aufbewahrung von Logs

Der Kunde ist verpflichtet, die automatisch erzeugten Nutzungslogs seiner KI-Systemkonfigurationen **mindestens sechs Monate** aufzubewahren. AuxData Space GmbH stellt entsprechende Logs über die Nutzungsstatistiken der Plattform bereit. Die Sicherung und Archivierung dieser Logs liegt in der Verantwortung des Kunden. Weitergehende gesetzliche Aufbewahrungspflichten — insbesondere aus dem Datenschutz- oder Steuerrecht — bleiben unberührt und haben Vorrang.

10.8 Meldepflicht bei schwerwiegenden KI-Vorfällen

Der Kunde informiert AuxData Space GmbH **unverzüglich**, wenn er bei der Nutzung der Plattform ein ernsthaftes Risiko oder einen schwerwiegenden Vorfall im Sinne von Art. 3 Nr. 49 Verordnung (EU) 2024/1689 feststellt — insbesondere bei Vorfällen, die zu Schäden an Gesundheit, Sicherheit oder Grundrechten von Personen geführt haben oder führen könnten.

AuxData Space GmbH koordiniert im Bedarfsfall die Meldung an die zuständige Marktüberwachungsbehörde. Diese Regelung ergänzt die DSGVO-Meldepflichten gemäß AVV §6 und tritt neben diese.

10.9 Grundrechte-Folgenabschätzung

Öffentliche Einrichtungen sowie private Unternehmen, die öffentliche Dienstleistungen erbringen, und Betreiber von Hochrisiko-KI-Systemen in den Bereichen Kredit oder Versicherung sind verpflichtet, vor der Produktivschaltung eine **Grundrechte-Folgenabschätzung (FRIA)** gemäß Art. 27 Verordnung (EU) 2024/1689 durchzuführen.

Die Durchführung der FRIA obliegt dem Kunden eigenverantwortlich. AuxData Space GmbH stellt auf Anfrage Dokumentationsvorlagen bereit und unterstützt bei der Umsetzung im Rahmen des Zumutbaren.

10.10 Übernahme der Anbieterrolle durch den Kunden

Stellt der Kunde auf Basis der Plattform eigene KI-Produkte unter **eigenem Markennamen Dritten zur Verfügung** oder nimmt er wesentliche Modifikationen vor, die ein neues oder verändertes KI-System entstehen lassen, übernimmt er die **Rolle des Anbieters** im Sinne von Art. 25 Verordnung (EU) 2024/1689.

In diesem Fall obliegen ihm sämtliche Anbieterpflichten nach der Verordnung eigenverantwortlich — insbesondere Konformitätsbewertung, technische Dokumentation, CE-Kennzeichnung und Registrierung in der EU-Datenbank für Hochrisiko-KI-Systeme. AuxData Space GmbH ist hierüber unverzüglich zu informieren.

Stand: **02.08.2026**

AuxData Space GmbH Benzstr. 8 86356 Neusäß

Anlage: Bedingungen der Auftragsverarbeitung

Vorbemerkung

Im Rahmen der Leistungserbringung ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als Verantwortlicher im Sinne der datenschutzrechtlichen Vorschriften fungiert. Diese Auftragsverarbeitungsvereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten oder wenigstens Zugriffsmöglichkeit haben

1. Gegenstand, Dauer, Spezifizierung der Auftragsverarbeitung

(1) Aus dem Hauptvertrag ergeben sich Gegenstand und Dauer des Auftrages. Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages.

(2) Art und Zweck der vorgesehenen Verarbeitung von Daten sind IT-Dienstleistungen, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

(3) Art der personenbezogenen Daten sind Personenstammdaten wie Geschlecht, Vorname, Nachname, Adresse, Kommunikationsdaten (Telefon, E-Mail), Vertragsdaten, Vertragsabrechnungs- und Zahlungsdaten, Kundenhistorie, Planungs- und Steuerungsdaten, ebenso ein- und ausgehende E-Mails und sonstige Daten, IT-Nutzungsdaten (User-Id, Passwörter), die im Zusammenhang mit der Erbringung der IT-Dienstleistung eingesehen werden können. Näheres ist in der Anlage 1 „Beschreibung Verarbeitungstätigkeit“ geregelt.

(4) Kategorien betroffener Personen sind Mitarbeiter, Kunden, Interessenten, Dienstleister, Lieferanten oder Ansprechpartner des Auftraggebers.

(5) Der Auftragnehmer verwendet, die zur Kenntnis gelangten, personenbezogenen Daten für keinen anderen als den festgelegten Vertragszweck. Der Auftragnehmer darf die Daten anonymisieren und in anonymisierter Form für eigene Zwecke verarbeiten und nutzen. Die Parteien stimmen darin überein, dass anonymisierte bzw. nach dieser Maßgabe aggregierte Auftraggeber-Daten nicht mehr als Daten im Sinne dieser Bedingungen gelten.

(6) Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer findet grundsätzlich innerhalb der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt. Es ist dem Auftragnehmer gleichwohl gestattet, Auftraggeber-Daten unter Einhaltung der Bestimmungen dieser Bedingungen auch außerhalb des EWR zu verarbeiten, wenn er den Auftraggeber vorab über den Ort der Datenverarbeitung informiert und die Voraussetzungen der Art. 44–48 DSGVO erfüllt sind oder eine Ausnahme nach Art. 49 DSGVO vorliegt

2. Weisungsbefugnisse des Auftraggebers

(1) Weisungsberechtigt auf Seiten des Auftraggebers ist der Auftraggeber selbst, der gesetzliche Vertreter des Auftraggebers und der IT-Leiter. Werden Weisungen durch andere Personen erteilt, müssen diese von den berechtigten Personen bestätigt werden. Mündliche Weisungen bestätigt der Auftraggeber unverzüglich per E-Mail.

(2) Der Auftragnehmer hat den Auftraggeber möglichst zeitnah darauf hinweisen, 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.

(3) Der Auftragnehmer verwendet die Daten ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieses Vertrags Ausdruck finden. Einzelweisungen, die von den Festlegungen dieses Vertrags abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers.

3. Pflichten des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Daten Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

(2) Der Auftraggeber ist Eigentümer der Daten und Inhaber aller etwaigen Rechte, die die Daten betreffen.

(3) Dem Auftraggeber obliegt es, dem Auftragnehmer die Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Richtigkeit der Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

(4) Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DS-GVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

- a) Schriftliche Bestellung eines Datenschutzbeauftragten, sofern nach den gesetzlichen Vorschriften eine Bestellopflicht besteht. Der DSB übt seine Tätigkeit gemäß Art. 38 und 39 DS-GVO aus. Dessen jeweils aktuelle Kontaktdaten werden auf Anforderung zur Verfügung gestellt.

- b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer 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) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.
- 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 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 dieses Vertrages.

5. Technische und 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 auf Anforderung zur Prüfung zu übergeben. 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 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO 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 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 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

6. Mitteilung des Auftragnehmers bei Verstößen

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u. a.

- a) Die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
- b) Die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
- c) Die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
- d) Die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
- e) Die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.
- f) Die unverzügliche Meldung an den Auftraggeber bei Feststellung eines schwerwiegenden Vorfalls im Sinne von Art. 3 Nr. 49 Verordnung (EU) 2024/1689 (EU AI Act), der im Zusammenhang mit der Nutzung von KI-Funktionen der Plattform steht. Diese Pflicht besteht unabhängig davon, ob gleichzeitig eine Verletzung personenbezogener Daten nach Art. 33 DSGVO vorliegt.

(2) Der Auftragnehmer wird den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden nachzuweisenden Aufwände und Kosten

bei etwa vom Auftraggeber durchzuführenden Datenschutz-Folgenabschätzungen und sich gegebenenfalls anschließenden Konsultationen der Aufsichtsbehörden nach Art. 35, 36 DSGVO unterstützen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftraggeber hat grundsätzlich das Recht, in Abstimmung mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die mit zwei Wochen Vorlauf anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer am Ort der Datenverarbeitung zu überzeugen.

(2) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z. B. nach BSI-Grundschutz – („Prüfungsberichts“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Sofern der Auftraggeber auf Basis tatsächlicher Anhaltspunkte berechnete Zweifel daran geltend macht, dass diese Prüfberichte bzw. Zertifizierungen unzureichend oder unzutreffend sind, oder besondere Vorfälle im Sinne von Art. 33 Abs. 1 DS-GVO im Zusammenhang mit der Durchführung der Auftragsverarbeitung des Kunden dies rechtfertigen, kann er Vor-Ort-Kontrollen durchführen.

(3) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder wenn der Auftragnehmer durch deren Offenbarung gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten – es sei denn, dass diese die Basis des erstattungsfähigen oder durchlaufenden Aufwandes darstellen – zu Qualitätsprüfungs- und Vertrags-Managementberichten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.

(4) Der Auftraggeber hat den Auftragnehmer rechtzeitig (mindestens zwei Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren. Der Auftraggeber darf in der Regel eine Kontrolle pro Kalenderjahr durchführen. Hiervon unbenommen ist das Recht des Auftraggebers, weitere Kontrollen im Fall von besonderen Vorkommnissen durchzuführen.

(5) Der Auftragnehmer erhält vom Auftraggeber eine Aufwandsentschädigung, wenn die Art und Weise einer Kontrolle unverhältnismäßig den Auftragnehmer beeinträchtigt.

(6) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aufgrund dieses Vertrags gegenüber dem Auftragnehmer verpflichtet ist. Zudem hat der Auftraggeber den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten unverzüglich vorzulegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

8. 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 und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Der Auftraggeber stimmt der Beauftragung der in der Anlage genannten Unterauftragnehmer zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO:

Der Wechsel bestehender Unterauftragnehmer ist 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 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an seine Unterauftragnehmer und deren erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Die datenschutzrechtlichen Pflichten aus diesen Bedingungen sind auf alle weiteren Auftragsverarbeiter zu übertragen.

9. Rechte der Betroffenen

(1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

(2) Soweit ein Betroffener sich unmittelbar an den Auftragnehmer zwecks Auskunft, Berichtigung, Löschung oder Sperrung der ihn betreffenden Daten wenden sollte, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

(3) Für den Fall, dass eine betroffene Person ihre Rechte auf Berichtigung, Löschung oder Sperrung von Daten oder auf Auskunft über die gespeicherten Daten, den Zweck der Speicherung und die Personen und Orte, an die Daten regelmäßig übermittelt werden, geltend macht, hat der Auftragnehmer den Auftraggeber bei der Erfüllung dieser Ansprüche in angemessenem und für den Auftraggeber erforderlichen Umfang zu unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung des Auftragnehmers erfüllen kann. Der Auftragnehmer erhält vom Auftraggeber eine angemessene Entschädigung für seinen im Rahmen der Mitwirkung anfallenden Aufwand.

(4) Der Auftragnehmer wird es dem Auftraggeber ermöglichen, Daten zu berichtigen, zu löschen oder zu sperren oder auf Verlangen des Auftraggebers die Berichtigung, Sperrung oder Löschung selbst vornehmen, wenn und soweit das dem Auftraggeber selbst unmöglich ist.

10. 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) Etwaiges Löschkonzept, Gewährleistung Recht auf Vergessen werden, Berichtigung, Datenportabilität und Auskunft sind unmittelbar durch den Auftraggeber sicherzustellen.

11. Löschung und Rückgabe von personenbezogenen Daten

Nach Abschluss der Erbringung der Verarbeitungsleistungen löscht der Auftragnehmer nach Wahl des Auftraggebers entweder alle personenbezogenen Daten oder gibt sie dem Auftraggeber zurück, sofern nicht nach dem Unionsrecht oder nach deutschem Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht oder sich aus den Leistungsbeschreibungen und den jeweiligen vertraglichen Vereinbarungen etwas anderes ergibt.

12. Verhältnis zum Hauptvertrag

Soweit in diesen Bedingungen keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen diesen Bedingungen und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus diesen Bedingungen vor.