

AV-Vertrag

Vertrag zur Verarbeitung personenbezogener
Daten im Auftrag (AVV) gemäß Art. 28 Abs. 3
Datenschutz-Grundverordnung (DSGVO)

Soziales | Gesundheit | Bildung | Kultur | Heimat | Umwelt

Vertrag zur Verarbeitung personenbezogener Daten im Auftrag (AVV) gemäß Art. 28 Abs. 3 Datenschutz-Grundverordnung (DSGVO)

zwischen

Bezirk Oberbayern
Prinzregentenstr. 14
80535 München

vertreten durch den Bezirkstagspräsidenten

Verantwortlicher (im folgenden Auftraggeber genannt)

und

vertreten durch

Auftragsverarbeiter (im folgenden Auftragnehmer genannt)

§ 1 Allgemeines

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten für den Auftraggeber im Auftrag (Art. 28 DSGVO). Hierbei hat der Auftraggeber ihn im Rahmen seiner Sorgfaltspflichten als Dienstleister ausgewählt.
- (2) Dieser Vertrag enthält nach dem Willen der Parteien den schriftlichen Auftrag zur Auftragsverarbeitung und regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Datenverarbeitung.
- (3) Diesem Vertrag liegt folgende Leistungsvereinbarung (im folgenden Hauptauftrag genannt), der die eigentliche/n Leistung/en des Auftragnehmers gegenüber dem Auftraggeber regelt, zugrunde:

- (4) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat der Europäischen Union (EU) oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

§ 2 Gegenstand und Dauer der Auftragsvertragsverarbeitung

- (1) Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Leistungen (z.B. Betrieb von Software, Wartung von Hardware, etc.), zu deren Zweckerreichung personenbezogene Daten verarbeitet werden. (zutreffendes bitte eintragen)

- (2) Die Laufzeit dieses Vertrages ist an die Laufzeit des diesem Vertrag zugrundeliegenden Hauptvertrages gebunden. Mit Kündigung und Beendigung des Hauptvertrags endet auch dieser Vertrag.

Das Sonderkündigungsrecht des Auftraggebers gemäß § 13 dieses Vertrags bleibt davon unberührt.

§ 3 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

- (1) Art der Verarbeitung gemäß Art. 4 Nr. 2 DSGVO
(z.B. Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich und Verknüpfung, Einschränkung, Löschen oder Vernichten von personenbezogenen Daten, etc.) (zutreffendes bitte eintragen)

- (2) Zweck der Verarbeitung (zutreffendes bitte eintragen)

Die Verarbeitung dient
Der zugrundeliegende Zweck der Verarbeitung ist dem Hauptvertrag zu entnehmen.
Der zugrundeliegende Zweck der Verarbeitung ist der Leistungsbeschreibung des Hauptvertrags (Anlage __ zum Hauptvertrag) zu entnehmen.

- (3) Art der verarbeiteten personenbezogenen Daten gemäß Art. 4 Nr. 1 DSGVO
(z.B. Beschäftigten-, System-, Inhaltsdaten, etc.) (zutreffendes bitte eintragen)

- (4) Kategorien betroffener Personen gemäß Art. 4 Nr. 1 DSGVO
(z.B. Mitarbeitende, Sozialhilfeempfänger, etc.) (zutreffendes bitte eintragen)

§ 4 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

- (1) Der Auftraggeber ist Verantwortlicher gemäß Art. 4 Abs. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Er allein ist für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO verantwortlich.
- (2) Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber ist verpflichtet, das Ergebnis in geeigneter Weise zu dokumentieren. Er informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten bei der Überprüfung feststellt.
- (3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang, und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen.
- (4) Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich, was auch in einem elektronischen Format erfolgen kann. Mündliche Weisungen sind unverzüglich schriftlich, was auch in einem elektronischen Format erfolgen kann, zu bestätigen.
- (5) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.
- (6) Für den Fall, dass eine Informationspflicht gegenüber Dritten besteht, ist ausschließlich der Auftraggeber für die Erfüllung dieser Pflichten verantwortlich. Die Verpflichtungen des Auftragnehmers zur Unterstützung des Auftraggebers zwecks Wahrung der Betroffenenrechte gemäß § 6 Abs. 11 und 12 dieses Vertrages bleiben unberührt.

§ 5 Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

- (1) Weisungsberechtigte Personen des Auftraggebers sind:

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

- (2) Weisungsempfänger des Auftragnehmers sind:

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

(Vorname, Name, Organisationseinheit, Telefon, E-Mail)

- (3) Für die Erteilung von Weisungen sind folgende Kommunikationskanäle zu nutzen:

a) E-Mail

b) Postalisch

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder einem dokumentierten elektronischen Format die Nachfolger bzw. die Vertreter mitzuteilen.

- (4) Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

§ 6 Rechte und Pflichten des Auftragnehmers

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden). In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen 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 Satz 2 Buchstabe a DSGVO).
- (2) Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen als die von den Parteien vereinbarten, insbesondere nicht für eigene, Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.
- (3) Der Auftragnehmer sichert zu, die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt zu trennen.
- (4) Der Auftragnehmer wird die Daten, die er im Auftrag des Auftraggebers verarbeitet, auf geeignete Weise kennzeichnen. Sofern die Daten für verschiedene Zwecke verarbeitet werden, wird der Auftragnehmer sie mit dem jeweiligen Zweck kennzeichnen. Eingang und Ausgang sowie laufende Verwendung werden dokumentiert.

- (5) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Auftraggeber nach Überprüfung bestätigt oder geändert wird.
- (6) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnete Interessen des Auftragnehmers nicht entgegenstehen.
- (7) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder Betroffene darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
- (8) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 Buchstabe b DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.
- (9) Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Mitarbeitern des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicherzustellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.
- (10) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.
- (11) Der Auftragnehmer unterstützt den Auftraggeber gemäß Art. 28 Abs. 3 Satz 2 Buchstabe e und f DSGVO bei der Erfüllung der Rechte betroffener Personen nach Kap. III DSGVO sowie bei der Einhaltung der in Art. 32 bis 36 genannten Pflichten. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
- (12) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung der Verarbeitung, Löschung, Datenübertragbarkeit oder Widerspruch - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers ergreifen.
- (13) Der Auftragnehmer unterstützt den Auftraggeber in angemessener Weise bei der Anfertigung der Beschreibung der Verarbeitungstätigkeit (Art. 30 DSGVO) oder bei erforderlichen Datenschutz-Folgeabschätzungen (Art. 35 DSGVO). Er hat die hierzu erforderlichen Angaben an den Auftraggeber zu liefern.
- (14) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind.
- (15) Der Auftragnehmer sichert zu, für seine im eigenen Betriebsablauf durchgeführten Tätigkeiten zur Verarbeitung personenbezogener Daten insbesondere derer, die für den Auftraggeber durchgeführt werden, ein Verzeichnis der Verarbeitungstätigkeiten zu führen und dieses der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.
- (16) Beim Auftragnehmer ist als Beauftragte(r) für den Datenschutz bestellt:

(Vorname, Name, Organisationseinheit, Telefon)

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

§ 7 Kontrollrechte des Auftraggebers

- (1) Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung (Art. 28 Abs. 3 Satz 2 Buchstabe h DSGVO).

(beispielhafte Aufzählung:

- Ergebnisse eines Selbstaudits
- Zertifikat zu Datenschutz- und/oder Informationssicherheit (z.B. ISO 27001)
- Genehmigte Verhaltensregeln gemäß Art. 40 DSGVO
- Verbindliche interne Datenschutzvorschriften gemäß Art. 47 DSGVO
- Zertifizierungen gemäß Art. 42 DSGVO
- aktuelles Testat und/oder Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren)

Folgende/r Nachweis/e ist/sind diesem Vertrag als Anlage/n beigelegt:

Sofern einschlägig, verpflichtet sich der Auftragnehmer, den Auftraggeber über den Ausschluss von genehmigten Verhaltensregeln nach Art. 41 Abs. 4 DSGVO und den Widerruf einer Zertifizierung nach Art. 42 Abs. 7 DSGVO unverzüglich zu informieren.

- (2) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherung sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 Buchstabe h DSGVO).
- (3) Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.
- (4) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme verlangen. Eine Einsicht in den Quellcode ist hiervon explizit, aus geheimhaltungs- und geschäftspolitischen Gründen des Auftragnehmers, ausgeschlossen.
- (5) Der Auftraggeber kann nach vorheriger Anmeldung mit einer angemessenen Frist die Kontrolle im Sinne des Absatzes 2 in der Betriebsstätte des Auftragnehmers zu den jeweils

üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden.

- (6) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen.

§ 8 Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

- (1) Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO.
- (2) Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

§ 9 Unterauftragsverhältnisse mit Subunternehmern

- (1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer gemäß Art. 28 Abs. 3 Satz 2 Buchstabe d DSGVO nur mit Erlaubnis des Auftraggebers gestattet.
- (2) Ein zustimmungsbedürftiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Nicht als Subunternehmerverhältnis im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Hierzu zählen z.B. Telekommunikationsleistungen, Wartung und Nutzerservice (wenn kein Zugriff auf Daten des Auftraggebers erfolgen kann), Reinigungskräfte und Prüfer. Der Auftragnehmer wird jedoch auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen treffen und erforderliche Kontrollmaßnahmen ergreifen, um den Schutz und die Sicherheit der Daten des Auftraggebers zu gewährleisten.
- (3) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig aus. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.
- (4) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber

berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

- (5) Der Vertrag mit dem Subunternehmer muss gemäß Art. 28 Abs. 9 DSGVO schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann.
- (6) Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.
- (7) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.
- (8) Die zum Zeitpunkt des Abschlusses dieses Vertrages bestehenden Unterauftragsverhältnisse mit Subunternehmern sind in Anlage ___ mit Namen, Anschrift und Auftragsinhalt dokumentiert. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.
- (9) Der Auftragnehmer informiert den Auftraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber gemäß Art. 28 Abs. 2 Satz 2 DSGVO die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Einspruch muss durch den Auftraggeber binnen einer Woche nach Zugang der Information über die beabsichtigte Änderung der Subunternehmerverhältnisse erklärt werden.
- (10) Die Benachrichtigung über eine geplante Änderung sowie die Erklärung eines Einspruchs gemäß Abs. 9 ist gegenüber den in § 5 genannten Ansprechpartnern und über die dort festgelegten Kommunikationskanäle schriftlich, was auch in einem elektronischen Format erfolgen kann, zu erklären.
- (11) Kann eine einvernehmliche Lösung der Parteien nicht herbeigeführt werden, erfolgt im Falle eines wirksam erklärten Einspruchs keine Bestellung des Subunternehmers für die Verarbeitung der Daten des Auftraggebers.
- (12) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

§ 10 Datengeheimnis

- (1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung des Datengeheimnisses im Sinne des § 53 Bundesdatenschutzgesetz (BDSG) / Art. 11 Bayerisches Datenschutzgesetz (BayDSG) verpflichtet.
- (2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter mit den für sie maßgeblichen Bestimmungen des Datenschutzes vertraut macht und diese auf das Datengeheimnis verpflichtet werden.
- (3) Der Auftraggeber verpflichtet sich, sofern er besonderen Geheimnisschutzregeln bezüglich der hier im Vertrag genannten relevanten Daten und Verarbeitungszwecken unterworfen ist, diese Geheimschutzregeln vor Vertragsabschluss dem Auftragnehmer anzuzeigen und vollständig bekannt zu machen. Unterlässt der Auftraggeber diese Anzeige und

Bekanntmachung, so sichert er damit zu, keinen besonderen Geheimschutzregeln unterworfen zu sein, die vom Auftragnehmer beachtet werden müssen.

§ 11 Verschwiegenheitspflichten

- (1) Beide Parteien verpflichten sich, Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Diese Verpflichtung gilt auch nach Beendigung des Vertrages fort. Dies betrifft insbesondere Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.
- (2) Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

§ 12 Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

- (1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.
- (2) Die umgesetzten technischen und organisatorischen Maßnahmen des Auftragnehmers sind in Anlage __ dieses Vertrags beschrieben.
- (3) Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
- (4) Wesentliche Änderungen technisch organisatorischer Maßnahmen muss der Auftragnehmer den in § 5 genannten Ansprechpartnern über die dort festgelegten Kommunikationskanäle schriftlich, was auch in einem elektronischen Format erfolgen kann, mitteilen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftragnehmer unverzüglich.
- (5) Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 Buchstabe d DSGVO). Bei der Prüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen seiner Subunternehmer kann der Auftragnehmer insbesondere auf das Vorliegen einschlägiger gültiger und aktueller Zertifizierungen (z.B. Informationssicherheit

gemäß der Norm ISO 27001) durch externe Gutachter abstellen. Das Prüfergebnis ist dem Auftraggeber auf Anfrage mitzuteilen.

§ 13 Sonderkündigungsrecht

- (1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer seine Pflichten aus § 12 dieses Vertrages bezüglich der vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt hat.
- (2) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung, wie in Abs. 1 beschrieben, berechtigt.
- (3) Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die vorfrühte Beendigung des Hauptvertrages und dieser Vereinbarung in Folge einer außerordentlichen Kündigung durch den Auftraggeber entstehen.

§ 14 Nachvertragliche Pflichten

- (1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist ebenfalls unverzüglich zu löschen.
- (2) Auf Verlangen des Auftraggebers händigt der Auftragnehmer nach Beendigung des Vertrages vor der Löschung entsprechend Abs. 1 sämtliche in seinen Besitz gelangte Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber aus.
- (3) Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Löschung und Rückgabe der Daten beim Auftragnehmer zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des Auftragnehmers erfolgen.

§ 15 Vergütung

Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt. Eine gesonderte Vergütung oder Kostenerstattung im Rahmen dieses Vertrages erfolgt nicht.

§ 16 Haftung

- (1) Die Vertragsparteien haften entsprechend der einschlägigen Bestimmungen gemäß Art. 82 DSGVO.
- (2) Im Falle einer Inanspruchnahme des Auftraggebers durch eine Person hinsichtlich etwaiger Schadensersatzansprüche nach Art. 82 DSGVO verpflichtet sich der Auftragnehmer, den Auftraggeber bei der Abwehr der Ansprüche im Rahmen seiner Möglichkeiten zu unterstützen.

§ 17 Schlussbestimmungen

- (1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.
- (2) Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.
- (3) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 des bürgerlichen Gesetzbuches (BGB) wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.
- (4) Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.
- (5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.
- (6) Soweit sich nicht aus dem Hauptvertrag ein anderer Gerichtsstand ergibt, ist ausschließlicher Gerichtsstand für Streitigkeiten aus diesem Vertrag beim Sitz des Auftraggebers.

Unterschriften:

Ort, Datum

Auftraggeber

Ort, Datum

Auftragnehmer

Anlagen:

Anlage 1 Technische und organisatorische Maßnahmen des Auftragnehmers zur Gewährleistung der Datensicherheit

Anlage 2

Anlage 3