Anlage 6 *(zur Leistungsbeschreibung)*

Vereinbarung (Auftrag) zur Auftragsverarbeitung gemäß Art. 28 Abs. 3 DSGVO

Zwischen

der Landeshauptstadt München,
vertreten durch den Oberbürgermeister,
dieser vertreten durch die Kommunalreferentin,
diese vertreten durch die Leiterin des GeodatenService München

Denisstraße 2
80335 München

- im Folgenden Auftraggeberin (AG) genannt -

und

…
…
…
…

- im Folgenden Auftragnehmerin (AN) genannt -

wird folgende Vereinbarung zur Auftragsverarbeitung geschlossen:

Präambel und Glossar

Aus Vereinfachungsgründen wird im folgenden Text ausschließlich die weibliche Form hinsichtlich AG und AN verwendet. Die männliche Form ist selbstverständlich und soweit einschlägig ebenso gemeint und erfasst.

Die AG und die AN verstehen die in der folgenden Vereinbarungen verwendeten Abkürzungen und Begrifflichkeiten im Rahmen dieser Vereinbarungen einheitlich wie folgt:

DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

BayDSG	Bayerisches Datenschutzgesetz vom 15. Mai 2018
VerpflG	Verpflichtungsgesetz vom 2. März 1974 (BGBl. I S. 469, 547), das durch § 1 Nummer 4 des Gesetzes vom 15. August 1974 (BGBl. I S. 1942) geändert worden ist
Verarbeitung	Jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Ziffer 2 DSGVO).

§ 1 Gegenstand und Dauer der Vereinbarung / Laufzeit der Vereinbarung / Ansprechpartner der AG / Form der Kommunikation

I. (1) Mit Vertrag vom … hat die AG die AN mit … beauftragt. (2) Gegenstand dieser Vereinbarung ist die Fixierung der Vorgaben zur Verarbeitung aller personenbezogenen Daten im Rahmen des Vertragsverhältnisses (Satz 1).

II. Soweit in dieser Vereinbarung von dem Vertragswerk bzw. Vertrag oder Vertragsverhältnis gesprochen wird, ist der Vertrag zwischen der AG und der AN gemeint, dessen Anlage diese Vereinbarung ist (§ 1 Absatz 1 Satz 1 dieser Vereinbarung).

III. Die AG und die AN sind sich darüber einig, dass es sich bei den unter § 2 Absatz 2 dieser Vereinbarung genannten Daten um personenbezogene Daten im Sinne der einschlägigen datenschutzrechtlichen Bestimmungen handelt.

IV. (1) Die Laufzeit dieser Vereinbarung korrespondiert mit der Laufzeit des Vertragswerkes. (2) Soweit nach dem Vertragswerk oder dieser Vereinbarung abweichende Regelungen für Teilaspekte (z.B. Geheimhaltung) getroffen werden, gehen diese Regelungen der Regelung in Satz 1 vor.

V. (1) Die AG benennt als Ansprechpartner für diese Vereinbarung:

Herrn Thomas Graßinger
Datenschutzbeauftragter des Kommunalreferats
089-233-24083
Roßmarkt 3
80331 München

und dessen Stellvertreter in der Funktion des örtlichen Datenschutzbeauftragten (unter der gleichen Anschrift)

Herrn Helmut Wagner
089-233-520610

(2) Die vorgenannte Person ist für die AN im Rahmen dieser Vereinbarung vollwertiger Ansprechpartner. (3) Aus Vereinfachungsgründen wird in den folgenden Regelungen durch-

gängig die Bezeichnung „Ansprechpartner der AG“ verwendet. (4) Der Ansprechpartner der AG ist zur Vornahme aller Handlungen und Ausübung aller Rechte, insbesondere auch der Weisungs- und Kontrollrechte der AG gegenüber der AN im Rahmen dieser Vereinbarung berechtigt, soweit es sich nicht um eine Vertragsänderung im Sinne des § 13 dieser Vereinbarung handelt.

VI. (1) Die Kommunikation im Zusammenhang mit dieser Vereinbarung ist ausschließlich schriftlich zu führen. (2) Als Kontaktadresse bei der AG ist die Büroanschrift des Ansprechpartners der AG zu verwenden.(3) Der Schriftverkehr ist als vertraulich zu kennzeichnen. (4) Der Ansprechpartner der AG kann anderweitige Kommunikationsmöglichkeiten und Kontaktadressen gegenüber der AN für zulässig erklären.

VII. (1) Diese Vereinbarung besteht aus diesem Dokument (Seite 1 – 11). Soweit in dieser Vereinbarung keine Regelungen zu einer Thematik getroffen werden, gelten diejenigen des übrigen Vertragswerkes (§ 1 Absatz 1 Satz 1 dieser Vereinbarung).

VIII. (1) Die AN unterwirft sich hinsichtlich der von dieser Vereinbarung betroffenen Vorgängen denselben datenschutzrechtlichen Anforderungen, die für die AG gelten und damit auch der Kontrolle durch den Bayerischen Landesbeauftragten für den Datenschutz. (2) Die AN hat demnach insbesondere die Vorgaben der DSGVO und des BayDSG zu beachten.

§ 2 Art und Umfang der Auftragsverarbeitung / betroffene personenbezogene Daten / Kreis der Betroffenen

I. Im Rahmen dieses Vertragsverhältnisses findet eine Auftragsverarbeitung in folgenden Situationen statt:

lfd. Nr.	Situationen
01.	Befahrung des Straßenraums zur Erstellung von 360° Panoramabilder und einer 3D-Punktwolke gemäß § 2.1 und 2.2 der Leistungsbeschreibung
02.	Anonymisierung der Bilder gemäß § 2.1.9 der Leistungsbeschreibung
03.	Bereitstellung einer Webanwendung zur Nutzung der Daten aus 01. gemäß § 2.3 der Leistungsbeschreibung

II. Folgende Datenarten sind Gegenstand der Auftragsdatenverarbeitung:

lfd. Nr.	Datenarten
01.	Panoramabilder gemäß § 2.2.1 der Leistungsbeschreibung

III. Sind besonders schützenswerte personenbezogene Daten von der Auftragsverarbeitung betroffen?

Kategorie	Betroffenheit
Artikel 9 DSGVO	☐ ja ☒ nein
personenbezogene Daten, die dem Sozialgeheimnis unterliegen	☐ ja ☒ nein
personenbezogene Daten, die dem Steuergeheimnis unterliegen	☐ ja ☒ nein

IV. Der Kreis der durch den Umgang mit den personenbezogen Daten im Rahmen des Vertragswerkes und dieser Vereinbarung Betroffenen umfasst folgende Personenkategorien:

Personenkategorie	Situation (lfd. Nr. aus Absatz 1)	Datenart (lfd. Nr. aus Absatz 2)
Definiert nach § 6 der Leistungsbeschreibung	03.	01. und 02.
Beschäftigte der AN	01.,02. Und 03	01. und 02.

§ 3 Rechte und Pflichten der AG

I. (1) Die AG bleibt unabhängig von der Regelung des § 11 Abs. 3 dieser Vereinbarung gegenüber Dritten für die Einhaltung der datenschutzrechtlichen Vorschriften im Rahmen des Vertragsverhältnisses und dieser Vereinbarung allein verantwortlich (Art. 5 Abs. 2 und 24 DSGVO). (2) Die AG wird von der AN bei der Einhaltung der datenschutzrechtlichen Anforderungen auf schriftliches Verlangen unterstützt. (3) Dies gilt insbesondere für die Einhaltung der in Artikel 32 bis 36 DSGVO genannten Pflicht zur Sicherheit personenbezogener Daten, für Meldepflichten bei Datenpannen und bei Datenschutz-Folgeabschätzungen.

II. (1) Die AG legt die technischen und organisatorischen Maßnahmen fest (§ 6 dieser Vereinbarung), die im Rahmen des Vertragsverhältnisses und dieser Vereinbarung bei der Verarbeitung von personenbezogenen Daten durch die AN einzuhalten sind. (2) Die Regelung des § 6 Absatz 4 dieser Vereinbarung ist zu beachten.

III. (1) Die AG informiert die AN unverzüglich, wenn sie Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt und regelt im Wege ihres Weisungsrechts (§ 5 dieser Vereinbarung) das weitere Vorgehen. (2) Im Fall einer Inanspruchnahme der AN durch eine betroffene Person nach Artikel 82 DSGVO verpflichtet sich die AG, die AN bei der Abwehr der Ansprüche zu unterstützen.

IV. Die AG räumt der AN keinerlei Nutzungsrechte an urheberrechtlich oder durch sonstige gewerbliche Schutzrechte geschützten Daten bzgl. der vertragsgegenständlichen personenbezogenen Daten oder sonstigen von der AG stammenden Informationen ein.

§ 4 Pflichten der AN

I. Die AN darf personenbezogene Daten nur im Rahmen der im Vertragswerk festgelegten Rahmenbedingungen und der darüber hinaus erteilten Weisungen der AG (§ 5 dieser Vereinbarung) verarbeiten, soweit nicht ein Ausnahmefall im Sinne des Artikel 28 Absatz 3 Satz 2 lit. a DSGVO vorliegt oder die AN in sonstiger Weise gesetzlich zur Verarbeitung verpflichtet ist.

II. (1) Die AN sichert die Einhaltung aller in dieser Vereinbarung getroffenen technischen und organisatorischen Maßnahmen, insbesondere der Vorgaben in § 6 dieser Vereinbarung und dem dazugehörigen Anhang, ausdrücklich zu. (2) Die Regelung des § 6 Absatz 4 dieser Vereinbarung ist zu beachten.

III. (1) Die AN benennt unverzüglich nach Vertragsschluss gegenüber dem Ansprechpartner der AG einen eigenen Ansprechpartner. (2) Die AG darf darauf vertrauen, dass dem Ansprechpartner der AN die gleichen Befugnisse auf Seiten der AN zustehen, wie sie in § 1 Absatz 5 dieser Vereinbarung für den Ansprechpartner der AG geregelt sind.

IV. (1) Die AN bestellt – soweit dies gesetzlich vorgeschrieben ist – eine/einen Datenschutzbeauftragte/-n (extern oder betrieblich), der seine Tätigkeit nach den jeweils einschlägigen datenschutzrechtlichen Vorgaben, insbesondere gemäß Artikel 38 und 39 DSGVO, ausüben kann. (2) Die Kontaktdaten der/des Datenschutzbeauftragten der AN sind dem Ansprechpartner der AG zur Ermöglichung einer direkten Kontaktaufnahme nach Abschluss dieser Vereinbarung unverzüglich zu übermitteln.

V. (1) Die AN verpflichtet sich zur Wahrung des Datengeheimnisses. (2) Weiter wird die AN alle Beschäftigten, die bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten im Sinne dieser Vereinbarung tätig sind oder von diesen Daten unter Umständen Kenntnis nehmen könnten, auf das Datengeheimnis verpflichten. (3) Die Verpflichtung der Beschäftigten hat schriftlich zu erfolgen.

VI. Soweit Daten im Sinne von § 2 Absatz 3 dieser Vereinbarung betroffen sind, darf die AN nur Personen einsetzen, die vorher nach dem VerpflG verpflichtet wurden und – soweit betroffen – eine Verpflichtung auf das Steuer- und/oder Sozialgeheimnis unterzeichnet haben.

VII. (1) Die AN versichert, dass ihr die maßgeblichen datenschutzrechtlichen Vorschriften bekannt sind. (2) Weiter sichert die AN zu, dass sie alle bei der Vertragsabwicklung beteiligten Beschäftigten rechtzeitig mit den für sie maßgeblichen Vorschriften vertraut gemacht hat. (3) Die AN ist zur ständigen Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften verpflichtet.

VIII. Die AN erteilt Auskünfte über personenbezogene Daten, welche sie im Rahmen des Vertragsverhältnisses und dieser Vereinbarung verarbeitet erst nach vorheriger Zustimmung durch den Ansprechpartner der AG.

IX. Die AN wird personenbezogene Daten, die im Rahmen des Vertragsverhältnisses und dieser Vereinbarung von der AN verarbeitet werden, auf und gemäß der Weisung der AG unverzüglich berichtigen, löschen oder sperren.

X. (1) Die Verarbeitung der personenbezogenen Daten durch die AN im Rahmen dieser Vereinbarung findet ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union statt. (2) Jede Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung durch den Ansprechpartner der AG, die nur erteilt werden kann, wenn die Voraussetzungen der Artikel 44 ff. DSGVO vorliegen. (3) Die Verarbeitung der personenbezogenen Daten im Rahmen des Vertragswerkes und dieser Vereinbarung darf nur an der/den Betriebsstätte/n der AN stattfinden.

XI. Für die Sicherheit der personenbezogenen Daten erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren, welche die AN

zur Umsetzung der Vorgaben dieser Vereinbarung ergreift, sind mit dem Ansprechpartner der AG abzustimmen.

XII. Die AN verpflichtet sich, hinreichende Maßnahmen zur Katastrophenvorsorge zu treffen.

XIII. Soweit die AG einer Kontrolle durch Aufsichtsbehörden, einem Ordnungswidrigkeits- oder Strafverfahren, einem Haftungs- oder Auskunftsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung bei der AN ausgesetzt ist, hat ihn die AN nach besten Kräften zu unterstützen.

XIV. Die AN führt ein Verzeichnis im Sinne des Artikel 30 Absatz 2 DSGVO.

§ 5 Weisungsbefugnis der AG

I. (1) Die AN ist verpflichtet, allen zur Verarbeitung von personenbezogenen Daten im Rahmen des Vertragsverhältnisses und dieser Vereinbarung erteilten Weisungen der AG Folge zu leisten und diese unverzüglich umzusetzen. (2) Die Regelung des § 5 Absatz 3 dieser Vereinbarung geht vor.

II. (1) Weisungen im Sinne dieser Vereinbarung darf der Ansprechpartner der AG erteilen. (2) Der Ansprechpartner der AG kann gegenüber der AN jederzeit weitere weisungsberechtigte Personen benennen. (3) Die AN darf bis zu einer gegenteiligen Information durch den Ansprechpartner der AG darauf vertrauen, dass die durch ihn benannten Personen tatsächlich weisungsbefugt sind. (4) Den so ernannten Personen steht das Recht zur Benennung weiterer Weisungsberechtigter nicht zu.

III. Soweit die AN der Ansicht ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt, so ist sie berechtigt, die Umsetzung der Weisung bis zur schriftlichen Entscheidung eines Weisungsbefugten der AG auszusetzen.

§ 6 Technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen

I. (1) Die von der AN konkret sicherzustellenden technischen und organisatorischen Maßnahmen ergeben sich aus dem Anhang zu den technisch-organisatorischen Maßnahmen. (2) Die AN hat die Umsetzung der dort genannten Maßnahmen vor Beginn der Verarbeitung von personenbezogenen Daten für die AG im Rahmen des Vertragswerkes hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und zu bestätigen und dem Ansprechpartner der AG mit hinreichendem zeitlichen Vorlauf (mindestens vier Wochen) vor Beginn der Verarbeitung zur Prüfung zu übermitteln. (3) Die Dokumentation bezieht sich auch auf alle Unterauftragsverarbeiter. (4) Soweit Daten im Sinne des § 2 Absatz 3 dieser Vereinbarung betroffen sind, muss die AN die eingesetzten Personen in der Dokumentation benennen. (5) Vor der Freigabe durch den Ansprechpartner der AG darf mit der Verarbeitung im Rahmen dieses Vertragswerkes nicht begonnen werden. (6) Darüber hinaus hat die AN ein angemessenes Schutzniveau gemäß Artikel 32 DSGVO eigenverantwortlich zu gewährleisten.

II. (1) Die im Anhang aufgeführten Maßnahmen stellen einen Mindeststandard dar, welchen die AN zu keiner Zeit unterschreiten, aber jederzeit überschreiten darf. (2) Die AN regelt die innerbetriebliche Organisation so, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. (3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. (4) Insoweit ist es der AN gestattet, alternative adäquate Maßnahmen nach Zustimmung durch den Ansprechpartner

der AG umzusetzen. (5) Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. (6) Wesentliche Änderungen sind zu dokumentieren. (7) Sollte sich im Laufe der Vertragslaufzeit herausstellen, dass die technisch-organisatorischen Maßnahmen nicht mehr dem Stand der Technik entsprechen oder durch neue gesetzliche Vorgaben höhere Anforderungen gestellt werden müssen, kann die AG im Rahmen ihres Weisungsrechts eine Anpassung auf den aktuellen Stand der Technik verlangen. (8) Soweit die in Satz 7 beschriebenen Ausnahmesituationen eintreten sollten, werden sich AG und AN über die Höhe und Verteilung der hierdurch entstehenden Kosten abstimmen und die Vereinbarung entsprechend anpassen (§ 13 dieser Vereinbarung).

III. (1) Die AN hat darüber hinaus sicher zu stellen, dass alle in dieser Vereinbarung geforderten Maßnahmen und ihre tatsächliche Umsetzung durch die AN in einem umfassenden und aktuellen Datenschutz- und Sicherheitskonzept dokumentiert sind. (2) Unabhängig von einer konkreten Aufforderung durch die AG übermittelt die AN das aktuelle Datenschutz- und Sicherheitskonzept zumindest ein Mal jährlich zum 15.12. dem Ansprechpartner der AG.

IV. Wenn und soweit die Auftragsverarbeitung ausschließlich darin besteht, dass die AN in den Räumlichkeiten der AG und unter Aufsicht von Beschäftigten der AG personenbezogene Daten verarbeitet und ausgeschlossen werden kann, dass die AN die personenbezogenen Daten aus dem unmittelbaren Zugriff der AG bringen kann, finden die Regelungen dieses Paragrafen keine Anwendung.

§ 7 Kontrollrechte der AG

I. (1) Die AN erklärt sich damit einverstanden, dass der AG das jederzeitige Recht zur Durchführung von datenschutzrechtlichen Kontrollhandlungen zusteht. (2) Der Ansprechpartner der AG kann sich zur Durchführung der Kontrollmaßnahmen weiterer (auch externer) Personen bedienen. (3) Der AN wird mit der Ankündigung der Kontrollmaßnahmen durch den Ansprechpartner der AG auch der Name der Person/-en mitgeteilt, welche die Kontrollmaßnahme federführend vornehmen wird/ werden.

II. (1) Gegenstand der Kontrollhandlungen ist die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und der hierzu in dieser Vereinbarung geschlossenen Regelungen (insb. - aber nicht ausschließlich - der technischen und organisatorischen Maßnahmen). (2) Denkbare Kontrollhandlungen sind beispielsweise die Einsichtnahme in das Datenschutz- und IT-Sicherheitskonzept der AN, die Einsichtnahme in bereits erfolgte Datenschutzaudits bzw. deren Beauftragung, die Einsichtnahme in Zertifizierungen (Artikel 40 DSGVO) der AN oder auch die Inaugenscheinnahme vor Ort. (3) Die Inaugenscheinnahme vor Ort bei der AN erfolgt nur in Ausnahmefällen, wenn sich die AG ansonsten keinen hinreichenden Überblick verschaffen kann. (4) Die Entscheidung darüber, ob eine entsprechende Situation im Sinne des Satzes 3 vorliegt, trifft ausschließlich die AG.

III. (1) Soweit sich die AG zu einer Inaugenscheinnahme vor Ort bei der AN entscheiden sollte, ist die AN verpflichtet, der AG den Zutritt zu den Arbeitsräumen und dem Serverraum / Rechenzentrum - zumindest in Begleitung - zu ermöglichen. (2) Weiter wird die AN im Hinblick auf den unter Absatz 2 Satz 1 beschriebenen Kontrollgegenstand vollumfänglich Auskunft und Einblick in die für die AG erhobenen, verarbeiteten und genutzten personenbezogenen Daten und die Datenverarbeitungsprogramme gewähren. (3) Schließlich legt die AN nach Aufforderung auch einen Nachweis über die Verpflichtung ihrer Mitarbeiterinnen und Mitarbeiter auf das Datengeheimnis und weitere einschlägige Verpflichtungserklärungen vor. (4) Die Kontrollhandlungen finden während der gewöhnlichen Geschäftszeiten der AG statt (Mo - Do ca. zwischen 08.00 und 18.00 Uhr / Fr ca. zwischen 08.00 und 14.00 Uhr). (5) Die AG wird darauf achten, dass der Betriebsablauf der AN durch die Kontrollhandlungen so gering wie möglich gestört wird.

IV. (1) Die AN ist zur Unterstützung der AG bei den Kontrollhandlungen verpflichtet und hat die Maßnahmen zu dulden. (2) Soweit die AG Unterlagen bei ihr anfordert, hat sie diese der AG (Absatz 1 Satz 3) innerhalb von 10 Kalendertagen zu übermitteln, soweit die AG

keine längere Frist vorgibt. (3) Soweit die AG die Inaugenscheinnahme vor Ort beabsichtigt, kündigt die AG (Absatz 1 Satz 3) dies der AN grds. mindestens 10 Kalendertage vorher an, es sei denn, dass der AG konkrete Anhaltspunkte für erhebliche Datenschutzverstöße bei der AN vorliegen. (4) Im letztgenannten Fall des Satzes 3 ist die Inaugenscheinnahme durch die AG unverzüglich, zumindest innerhalb von drei Kalendertagen, durch die AN zu ermöglichen. (5) Die Entscheidung darüber, ob eine entsprechende Situation im Sinne des Satzes 4 vorliegt, trifft ausschließlich die AG.

V. Für die Ermöglichung von Kontrollen durch die AG und die Unterstützung und Begleitung der AG dabei kann die AN keinen Vergütungsanspruch geltend machen.

§ 8 Mitteilungspflichten der AN

I. Die AN unterrichtet den Ansprechpartner der AG - unter Berücksichtigung der Verpflichtungen nach Artikel 33 und 34 DSGVO - unverzüglich:

- und unabhängig davon, ob diese Aktivitäten im Zusammenhang mit der Auftragsverarbeitung für die AG stehen, bei Kontrollhandlungen, Maßnahmen oder Ermittlungen des bayerischen Landesbeauftragten für Datenschutz oder anderen Aufsichtsbehörden (Datenschutz) bei ihr über den Umstand;

- und detailliert unter Benennung der Regelung, gegen die verstoßen wurde und der betroffenen personenbezogenen Daten, wenn durch sie eine bei der AN beschäftigte Person oder einen Unterauftragsverarbeiter Verstöße gegen Vorschriften zum Schutz personenbezogener Daten, die im Auftrag der AG verarbeitet wurden oder werden, oder gegen die in dieser Vereinbarung getroffenen Festlegungen vorgefallen sind;

- wenn es unabhängig von der Verantwortlichkeit der AN zu schweren Betriebsstörungen bei der AN oder einem Unterauftragsverarbeiter gekommen ist und nicht ausgeschlossen werden kann, dass Unbefugte Zugriff auf die personenbezogenen Daten erlangt haben könnten, die im Auftrag für die AG verarbeitet wurden oder werden;

- wenn unabhängig von der unmittelbaren Betroffenheit der Daten, die für die AG verarbeitet werden, zu befürchten ist, dass Unbefugte im Verantwortungsbereich der AN oder eines Unterauftragsverarbeiters Kenntnis von personenbezogenen Daten nehmen konnten;

- wenn die personenbezogen Daten, die im Auftrag der AG verarbeitet werden, durch Maßnahmen von sonstigen Dritten, etwa durch Pfändungen oder sonstige Ereignisse mittelbar betroffen sein könnten;

- wenn sie oder ein Unterauftragsverarbeiter den Wechsel der Betriebsstätte beabsichtigt;

- soweit die AN der Ansicht ist, dass eine Weisung gegen gesetzliche Vorschriften verstößt.

II. (1) Die Information hat unverzüglich telefonisch an den Ansprechpartner der AG zu erfolgen. (2) Zusätzlich übermittelt die AN dem Ansprechpartner zumindest nachträglich die Dokumentation des jeweiligen Vorgangs (wenn nicht Rechte Dritter entgegenstehen), wenn der Ansprechpartner der AG nicht im Rahmen des Weisungs- und Kontrollrechts andere oder weitergehende Anforderungen an die AN stellt.

III. Die AN hat in den Fällen des § 8 Absatz 1 dieser Vereinbarung das weitere Vorgehen im Rahmen des Vertrages mit dem Ansprechpartner der AG abzustimmen und unverzüglich alle Maßnahmen einzuleiten, die erforderlich sind, um eine weitere Gefährdung aller personenbezogenen Daten auszuschließen.

§ 9 Aufbewahrungs-, Lösch- und Rückgabekonzept

I. (1) Die AN wird die von ihr im Rahmen des Vertragsverhältnisses und dieser Vereinbarung verarbeiteten personenbezogen Daten sorgsam und gemäß den Vorgaben dieser Vereinbarung aufbewahren. (2) Die AN bewahrt die personenbezogen Daten nicht länger auf, als dies die AG bestimmt.

II. (1) Die AN wird ohne vorherige Zustimmung der AG keine Kopien oder Reproduktionen erstellen. (2) Ausgenommen hiervon sind die Erstellung von Sicherungsdateien und solchen Sicherungen, die für die Umsetzung der Vorgaben dieser Vereinbarung oder gesetzlichen Aufbewahrungspflichten zwingend erforderlich sind. (3) Überlassene Datenträger und sämtliche hiervon gefertigte Kopien und Reproduktionen durch die AN verbleiben im Eigentum der AG.

III. (1) Nicht mehr benötigte Unterlagen mit personenbezogenen Daten dürfen erst nach vorheriger Zustimmung der AG datenschutzgerecht vernichtet werden oder sind an die AG auf deren Verlangen auszuhändigen. (2) Gleiches gilt für die Löschung von personenbezogen Daten im Sinne dieser Vereinbarung von Speichermedien der AN, sowie Ausschuss- und Testmaterial, welches personenbezogene Daten enthält.

IV. (1) Bei jeglicher Beendigung des Vertragsverhältnisses oder dieser Vereinbarung händigt die AN sämtliche in ihren Besitz gelangten Unterlagen und Speichermedien der AG und von ihr erstellte Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit der Auftragsverarbeitung stehen, der AG unverzüglich aus. (2) Die von der AN im Rahmen des Vertragswerkes und dieser Vereinbarung verarbeiteten personenbezogenen Daten sind ebenfalls der AG bei jeglicher Beendigung des Vertragsverhältnisses oder dieser Vereinbarung in geeigneter, von der AG zu bestimmender Form zu überlassen. (3) Anschließend sind alle personenbezogen Daten, welche der AN im Rahmen des Vertragsverhältnisses oder dieser Vereinbarung verarbeitet hat überlassen oder von ihr erhoben wurden und sich auf Speichermedien befinden, unwiederbringlich und datenschutzgerecht zu löschen. (4) Dies gilt auch für alle Archivierungs- und Sicherungsdateien. (5) Soweit die personenbezogenen Daten in sonstiger Form weiterhin bei der AN vorhanden sind, bietet sie diese der AG zur kostenlosen Überlassung an oder vernichtet diese nach Aufforderung durch die AG datenschutzgerecht. (6) Die Geltendmachung etwaiger Zurückbehaltungsrechte aus § 273 BGB oder sonstigen gesetzlichen oder vertraglichen Regelungen wird hiermit bzgl. der Daten und Datenträger der AG ausdrücklich ausgeschlossen.

V. (1) Die Löschung sämtlicher personenbezogener Daten ist von der AN zu dokumentieren. (2) Die Dokumentation muss zumindest Angaben zu Anzahl und Art der gelöschten Daten, das jeweils eingesetzte Löschverfahren und den Zeitpunkt der Löschung enthalten. (3) Die Dokumentation wird von der AN auf dem aktuellen Stand gehalten und der AG auf Verlangen unverzüglich die Einsichtnahme ermöglicht.

VI. (1) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Verarbeitung dienen, sind durch die AN entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. (2) Sie kann sie zu ihrer Entlastung bei Vertragsende der AG übergeben.

§ 10 Unterauftragsverhältnisse

I. Die Beauftragung von Unterauftragsverarbeitern durch die AN ist nach Maßgabe der folgenden Absätze, insbesondere der vorherigen schriftlichen Zustimmung (Einwilligung) durch die AG (Absatz 2), grundsätzlich zulässig.

II. (1) Soweit die AN Teile der von ihr nach dem Vertragswerk geschuldeten Leistung durch Unterauftragsverarbeiter (Dritte) erbringen lassen will und hierdurch der Regelungsgehalt dieser Vereinbarung betroffen ist, darf die AN den Unterauftragsverarbeiter nur nach ausdrücklicher vorheriger schriftlichen Zustimmung der AG hiermit beauftragen. (2) Hinsichtlich der im Vergabeverfahren bereits benannten Unterauftragsverarbeiter der AN wird

die Zustimmung hiermit erteilt. (3) Jede Änderung (anderes Unternehmen oder anderer Aufgabenzuschnitt) hinsichtlich derjenigen Unterauftragsverarbeiter, deren Beauftragung die AG nach Satz 1 & 2 bereits zugestimmt hat, unterliegt wiederum dem Zustimmungsvorbehalt nach Satz 1. (4) Soweit sich die AN nicht an die vorgenannten Vorgaben hält oder trotz noch nicht erteilter oder verweigerter Zustimmung einen Dritten einsetzt, ist die AG berechtigt, die Leistung der AN und der Dritten im betroffenen Bereich zu unterbinden und zurückzuweisen. (5) Insbesondere ist die AG in den im Satz 4 genannten Fällen nicht zur Bezahlung der betroffenen Leistungen verpflichtet.

III. (1) Wenn Unterauftragsverarbeiter durch die AN nach der Zustimmung nach Absatz 2 eingeschaltet werden, hat die AN sicherzustellen, dass ihre Vereinbarung mit dem Unterauftragsverarbeiter so gestaltet ist, dass das Datenschutzniveau mindestens demjenigen der Vereinbarung zwischen der AG und der AN entspricht und der AG in der Vereinbarung unmittelbar die Kontroll- und Überprüfungsrechte (entsprechend § 7 dieser Vereinbarung) auch gegenüber dem Unterauftragsverarbeiter zustehen.(2) Weiter hat die AN im Verhältnis zu den Unterauftragsverarbeitern sicherzustellen, dass die AN auf Anforderung der AG berechtigt ist, Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen des Unterauftragsverarbeiters zu erteilen. (3) Schließlich hat die AN sicherzustellen, dass es dem Unterauftragsverarbeiter verboten ist, selbst weitere Unter-Unterauftragsverarbeiter zu beauftragen. (4) Kommt der Unterauftragsverarbeiter seinen im Sinne dieses Absatzes begründeten Datenschutzpflichten nicht nach, haftet die AN gegenüber der AG insoweit (Artikel 28 Absatz 4 Satz 2 DSGVO).

§ 11 Geheimhaltung / Vertragsstrafe / Haftung

I. (1) Die AN ist verpflichtet, die Informationen über alle personenbezogenen Daten im Sinne dieser Vereinbarung streng vertraulich zu behandeln. (2) Diese Verpflichtung gilt auch nach Beendigung des Vertragsverhältnisses und dieser Vereinbarung fort.

II. (1) Im Falle eines schuldhaften (Vorsatz & Fahrlässigkeit) Verstoßes gegen die Vorgaben dieser Vereinbarung hat die AN der AG in folgenden Fällen eine Vertragsstrafe in der aufgeführten Höhe zu zahlen:

Regelung in dieser Vereinbarung	Höhe der verwirkten Vertragsstrafe
§ 4	bis zu 0,5 % der Auftragssumme je Verstoß

(2) Die Gesamtsumme der Vertragsstrafen ist pro Jahr auf 5 % der Auftragssumme € beschränkt. (3) Die Geltendmachung der Vertragsstrafe lässt weitergehende Ansprüche (z.B. auf Schadensersatz) unberührt. (4) Die Einrede des Fortsetzungszusammenhangs ist ausgeschlossen. (5) Die Regelung des § 343 BGB bleibt unberührt.

III. (1) Die AN und die AG haften für Schadensersatzansprüche Dritter gemäß der in Artikel 82 DSGVO getroffenen Regelung. (2) Im Falle des Verstoßes gegen die Vorgaben dieser Vereinbarung und/ oder der Weisungen der AG stellt die AN die AG von Schadensersatzansprüchen Dritter wegen Verletzung von datenschutzrechtlichen Vorgaben frei.

§ 12 Sonderkündigungsrecht

(1) Die AG ist berechtigt, den Vertrag und diese Vereinbarung jederzeit und ohne Einhaltung einer Frist zu kündigen/ beenden, wenn die AN schwerwiegend gegen eine Bestimmung dieser Vereinbarung verstößt, einer Weisung der AG unberechtigt nicht Folge leistet, Kontrollmaßnahmen im Sinne des § 7 dieser Vereinbarung verweigert, die Gesamtsumme in § 11 Absatz 2 Satz 2 erreicht ist oder die AN gegen die Regelung des § 4 Absatz 8 dieser Vereinbarung verstößt.

§ 13 Schlussbestimmungen

(1) Mündliche Nebenabreden zu dieser Vereinbarung wurden nicht getroffen. (2) Änderungen, Ergänzungen und Zusätze dieser Vereinbarung außerhalb der Befugnisse des Ansprechpartners der AG haben nur Gültigkeit, wenn sie zwischen AG und AN schriftlich vereinbart wurden. (3) Dies gilt auch für die Änderung der Regelungen des § 13 Absatz 1 Satz 1 und 2 dieser Vereinbarung selbst.

Im Rahmen der oben genannten Vereinbarung gibt die AG folgende konkret durch die AN sicherzustellenden technischen und organisatorischen Maßnahmen (Art. 28 Absatz 3 Satz 2 lit. c, Art. 32 DS-GVO) vor:

Maßnahmen bzgl. Räumlichkeiten & Gebäuden

- Allgemeine Vorgaben für alle Räumlichkeiten und Gebäude
    - Die Eingänge zu allen Räumen und Gebäuden, in denen personenbezogene Daten verarbeitet werden, sind gegen den Zutritt Unbefugter hinreichend zu sichern (z.B. durch Schlüssel, Token oder Zugangskarten). Unbefugten ist der Zugang zu verwehren.
    - Die AN regelt die Zuständigkeit für die Ausgabe der Zugangsmittel schriftlich oder durch eine allen MA zugängliche Anweisung. Die Regelung enthält darüber hinaus auch Vorgaben zu Prüfintervallen hinsichtlich der Berechtigung an den Zugangsmitteln und dem Vorgehen beim Ausscheiden von Beschäftigten. Die Ausgabe und Rückgabe der Zugangsmittel ist zu protokollieren.
    - Beschäftigte und Besucher sind auf Grund von schriftlichen Vorgaben der AN verpflichtet, Dienst- oder Besucherausweise jederzeit und gut sichtbar in den Räumlichkeiten und Gebäuden der AN zu tragen.
    - Die AN stellt durch schriftliche Vorgaben und Kontrollen oder durch eine allen MA zugängliche Anweisung sicher, dass Fenster und Türen bei Verlassen des Raumes und außerhalb der Betriebszeiten der AN verschlossen sind.
- Zusätzliche Vorgaben für Serverräume und Rechenzentren
    - Diese Räumlichkeiten sind gesondert gegen den Zutritt durch Unbefugte zu sichern. Die Sicherung ist so zu gestalten, dass das Betreten entgegen der Sicherung einen gesteigerten kriminellen Aufwand nötig machen würde.
    - Der Eingangsbereich der Serverräume bzw. des Rechenzentrums ist durchgehend von einem Wachdienst besetzt, welcher sicherstellt, dass nur berechtigte Personen Zutritt erhalten. Alternativ ist auch eine elektronische Zugangskontrollanlage mit einer Zwei-Faktor-Authentifizierung zulässig. Das Betreten dieser Räumlichkeiten ist nur durch oder in Begleitung eines Beschäftigten der AN, des Wachdienstes oder SÜG überprüfte Personen zulässig. Der Zutritt zum Serverraum bzw. Rechenzentrum ist lückenlos zu protokollieren.
    - In den eigentlichen Serverräumen gibt es keine Fenster und keine Leitungen usw. mit Flüssigkeiten über der Technik. Die Räumlichkeiten sind mit Gaslöschanlagen ausgestattet. Zumindest alle Außentüren sind videoüberwacht und alarmgesichert.
    - Das Wach- und Reinigungspersonal ist sorgfältig auszuwählen (zumindest unter Vorlage eines Führungszeugnisses ohne einschlägige Eintragungen).
    - Auf die Funktion der Räumlichkeiten bzw. des Gebäudes wird nicht zusätzlich z.B. durch Beschilderung, hingewiesen.
    - Gebäudeschächte sind gegen unberechtigtes Eindringen hinreichend abgesichert.
    - Die wichtigsten Versorgungsleitungen sind redundant ausgelegt. Die AN stellt eine Notstromversorgung (z.B. USV-Anlagen usw.) von drei Stunden sicher.
    - In den Serverräumen gibt es Feuchtigkeits-, Rauch-, und Wärmesensoren deren Werte ständig überwacht werden.
    - Die Mitnahme von Telefonen und Kameras in diese Räumlichkeiten ist nicht gestattet.

Maßnahmen bzgl. des Zugriffs auf personenbezogene Daten

- Die Zahl der zugriffsberechtigten Personen und insbesondere der Administratoren bei der AN wird durch sie auf das unvermeidbare Minimum begrenzt („need-to-know-Prinzip“). Dies erfolgt z.B. durch abgestufte Zugriffsrechte. Auch die Weitergabe der personenbezogenen Daten innerhalb des Unternehmens der AN ist auf ein absolutes Minimum zu begrenzen.

- Die AN stellt technisch sicher, dass die jeweilige Person ausschließlich auf diejenigen Daten Zugriff hat, auf die sich die Zugriffsberechtigung der Person erstreckt.

- Zu Wartungszwecken müssen gesonderte Zugriffsrechte bestehen, die einen Zugriff auf personenbezogene Daten soweit wie möglich ausschließen.

- <u>Maßnahmen bzgl. Passwörtern</u>

    - Die AN trifft schriftliche Regelungen zur Gestaltung und dem Umgang mit Pass-wörtern. Inhaltlich muss die Regelung zumindest vorgeben, dass die Passwörter mindestens eine Länge von 12 Zeichen aufweisen, jeweils Buchstaben, Zahlen und Sonderzeichen enthalten müssen und von den Beschäftigten geheim zuhalten sind. Weiter ist vorzugeben, dass Gruppenpasswörter nicht zulässig sind.

    - Die AN stellt technisch sicher, dass von den Systemen nur Passwörter akzeptiert werden, die den vorgenannten Vorgaben entsprechen und erzwingt spätestens alle sechs Monate technisch den Wechsel jedes Passworts. Weiter stellt die AN technisch sicher, dass die Passwörter zumindest innerhalb von zwei Jahren nicht erneut verwendet werden können.

    - Bei Arbeitsunterbrechungen ist technisch sicherzustellen, dass spätestens nach fünf Minuten ein passwortgeschützter Sperrbildschirm aktiviert wird.

    - Darüber hinaus gestaltet die AN die Arbeitsbereiche der Beschäftigten so, dass eine zufällige Kenntnisnahme der Passwörter durch Dritte bei der Eingabe durch den Berechtigten weitestgehend ausgeschlossen wird.

Weitere Maßnahmen

- Die AN hat alle Anmeldeversuche und Veränderungen zu protokollieren und technisch sicherzustellen, dass der Anmeldevorgang nach einer einstellbaren Anzahl von Fehlversuchen (max. drei) abgebrochen wird, vor einer Freigabe durch eine zentrale Stelle nicht erneut versucht werden kann und eine Benachrichtigung an eine zentrale Stelle bei der AN erfolgt, die zur Aufklärung des Vorfalls zu verpflichten ist.

- Die AN verpflichtet sich auf allen Datenverarbeitungsanlagen Virenscanner mit täglichen Updates und eine Firewall nach dem aktuellen Stand der Technik einzusetzen.

- Soweit personenbezogene Daten in Dokumenten (Papierform) oder Datenträgern vor-liegen, sind diese sicher zu verschließen, wenn sie nicht gerade zur Erfüllung des Vertrages benötigt werden. Die vorgenannten Vorgaben sind durch schriftliche Vorgaben der AN sicherzustellen.

- Trennung von Produktiv- und Testumgebung

- Die AN hat dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- Soweit die AN neben denjenigen personenbezogenen Daten, die sie im Auftrag für die AG verarbeitet auch im Wege der Auftragsverarbeitung für andere AG tätig ist, muss eine zuverlässige Trennung/ Abschottung der Daten der verschiedenen AG durch die AN erfolgen. Dies erfolgt im Idealfall durch eine physikalische Trennung der Daten. Gleiches gilt für die Daten – unabhängig ob personenbezogen oder nicht – der AN selbst.

- Die AN stellt (soweit dies in ihren Verantwortungsbereich fällt) sicher, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert oder verändert werden können.

- Die AN führt mindestens ein tägliches Backup der Daten (Totalsicherung) durch und stellt sicher, dass die diese Backup-Daten zumindest in einem anderen Brandabschnitt gespeichert werden.
- Bei der AN gibt es schriftliche Vorgaben zur Informationsweitergabe bei Störungen im Betrieb und bei Notfällen sowie Eskalationspläne.