Vereinbarung zur Verarbeitung von Daten im Auftrag

zwischen

Firma
Straße, Hausnummer
PLZ, Stadt
– Verantwortlicher / Auftraggeber –

und

Firma
Straße, Hausnummer
PLZ, Stadt
– Auftragsverarbeiter / Auftragnehmer –

Präambel

Führt ein Auftragsverarbeiter Leistungen im Auftrag seines Vertragspartners (Verantwortlicher) aus, müssen die Anforderungen der jeweils gültigen Datenschutzgesetze Berücksichtigung finden und insbesondere bei den Verarbeitungstätigkeiten ein angemessenes Datenschutzniveau garantiert sein. Die vorliegende Vereinbarung berücksichtigt die besonderen Anforderungen aus der EU-Datenschutzgrundverordnung[1].

§ 1 Gegenstand des Auftrags

(1) Der Verantwortliche beauftragt den Auftragsverarbeiter mit der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten.

(2) Die mit der Durchführung dieses Auftrags betrauten Personen des Auftragnehmers

Kommentiert [A1]: Eingefügt, um verfahrensspezifische und verfahrensunabhängige TOM zu unterscheiden.

☐ arbeiten in den Geschäftsräumen und in der IT-Umgebung des Auftraggebers.

☐ arbeiten von den Geschäftsräumen des Auftragnehmers aus
☐ arbeiten vom Homeoffice aus

☐ in der IT-Umgebung des Auftraggebers.
☐ in der IT-Umgebung des Auftragnehmers.
☐ in der IT-Umgebung des Auftraggebers.
☐ in der IT-Umgebung des Auftragnehmers.

(3) Der Gegenstand des Auftrags und damit der Zweck, die Art und der Umfang der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten

☒ ergibt sich aus dem zugrunde liegenden Hauptvertrag (Rahmenvertrag, Ausschreibung, Abrufkontingent, Bestellung) vom xx.xx.xxxx

[1] Verordnung 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, EU-DSGVO).

- ☐ ist die Durchführung der folgenden Aufgabe(n) durch den Auftragsverarbeiter: xxx [bitte so beschreiben, dass die Tätigkeiten und der Bezug zu personenbezogenen Daten deutlich wird]
- ☐ ist die (Fern-)Wartung von Systemen, wobei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.
- ☐ Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen Voraussetzungen der einschlägigen Datenschutzgesetze erfüllt sind.

§ 2 Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Die Beurteilung der Zulässigkeit der Datenverarbeitung obliegt allein dem Auftraggeber. Dem Auftragnehmer steht nach Ziff. 4 Abs. 6 das Recht zu, den Auftraggeber auf seiner Meinung nach rechtlich unzulässige Datenverarbeitungen hinzuweisen.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren.

(4) Der Auftraggeber kann weisungsberechtigte Personen benennen. Weisungsberechtigte Personen des Auftraggebers sind:

xxx [Konzerngesellschaft]

xxx [Konzerngesellschaft]

Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer schriftlich oder in Textform mitteilen.

(5) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(6) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

§ 3 Dauer des Auftrags

☐ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages.

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

☐ Der Auftrag wird bis zum _____ erteilt.

☐ Dem Auftrag liegt ein Mengenkontingent von Stunden zugrunde. Bei dem geplanten Einsatz von Personen wird der Auftrag in ca. Wochen abgearbeitet.

Kommentiert [A2]: Eingefügt aufgrund vorliegender Auftragsverhältnisse

☐ Der Auftrag ist unbefristet erteilt und kann von beiden Parteien mit einer Frist von Monat(en) zum Quartalsende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

§ 4 Art der Daten

Gegenstand der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten sind Daten aus folgenden Datenkategorien:

☐ Abrechnungsdaten	☐ Adressdaten	☐ Bankverbindungsdaten
☐ Biometrische Daten	☐ Bonitätsdaten	☐ Funktionsbezeichnung
☐ Geburtsdatum	☐ Gesundheitsdaten	☐ Interessen
☐ IT-Nutzungsdaten	☐ Kontaktdaten	☐ Lohn- und Gehaltsdaten
☐ Name	☐ Personalstammdaten	☐ Planungsdaten
☐ Qualifikationsdaten	☐ Sozialversicherungsdaten	☐ Telefonate
☐ Vertragsdaten	☐ Vertragsstammdaten	☐ Videoaufzeichnungen
☐ Zahlungsdaten	☐ Zeiterfassungsdaten	☐ sonstige (vgl. Anlage)

§ 5 Kreis der Betroffenen

Der Kreis, der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen, umfasst folgende Kategorien:

☐ Mitarbeiter / Rentner	☐ Lieferanten	☐ Veranstaltungsteilnehmer
☐ Bewerber	☐ Handelsvertreter	☐ Abonnenten
☐ Dienstleister	☐ Ansprechpartner	☐ Patienten
☐ Kunden / Mandanten	☐ Besucher / Gäste	☐ Passanten
☐ Interessenten		

§ 6 Technisch-organisatorische Maßnahmen

(1) Der Auftragsverarbeiter hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Verantwortlichen zur Prüfung zu übergeben (Anlage 2 „Technisch-organisatorische Maßnahmen“). Bei Akzeptanz durch den Verantwortlichen werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung / ein Audit des Verantwortlichen einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen. Die technisch-organisatorischen Maßnahmen sollen die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sowie die Systembelastbarkeit im Zuge der Datenverarbeitung sicherstellen. Aus den angegebenen Maßnahmen muss ein angemessenes Sicherheitsniveau ableitbar sein. Der Auftragsverarbeiter hat den

Verantwortlichen bei der Ergreifung technisch-organisatorischer Maßnahmen bestmöglich zu unterstützen.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragsverarbeiter gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

§ 7 Berichtigung, Sperrung, Einschränkung und Löschung von Daten

Der Auftragsverarbeiter hat nur nach Weisung des Verantwortlichen die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen, einzuschränken oder zu sperren. Soweit ein Betroffener sich unmittelbar an den Auftragsverarbeiter zwecks Berichtigung oder Löschung seiner Daten wenden sollte, wird der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Verantwortlichen weiterleiten.

§ 8 Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragsverarbeiter hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags folgende Pflichten:

(1) Schriftliche Bestellung – soweit gesetzlich vorgeschrieben – eines Datenschutzbeauftragten. Dessen Kontaktdaten werden dem Verantwortlichen zum Zweck der direkten Kontaktaufnahme mitgeteilt.

(2) Die Wahrung der Vertraulichkeit. Alle Personen, die auftragsgemäß auf personenbezogene Daten des Auftraggebers zugreifen können, müssen auf zur Vertraulichkeit verpflichtet und über die sich aus diesem Auftrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehrt werden.

(3) Der Auftragsverarbeiter stellt sicher, dass er die Verarbeitung personenbezogener Daten ausschließlich auf Grundlage dokumentierter Weisungen des Verantwortlichen vornimmt (vergl. § 12 dieses Vertrages). Sofern der Auftragsverarbeiter zu einer Verarbeitung gesetzlich verpflichtet ist, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

(4) Der Auftragsverarbeiter hat den Verantwortlichen bei seiner Pflicht zur Wahrung der Betroffenenrechte zu unterstützen. Dies ist durch geeignete organisatorische Maßnahmen zu gewährleisten.

(5) Sofern den Verantwortlichen aufgrund eines voraussichtlich hohen Risikos der Verarbeitung die Pflicht zur Datenschutz-Folgenabschätzung trifft, hat der Auftragsverarbeiter ihn hierbei zu unterstützen. Dies gilt ebenso für die Pflicht zur vorherigen Konsultation der Aufsichtsbehörde, sofern sich eine solche aus der vorangegangenen Folgenabschätzung ergibt.

(6) Die unverzügliche Information des Verantwortlichen über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde. Dies gilt auch, soweit eine zuständige Behörde beim Auftragsverarbeiter ermittelt.

(7) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen (Homeoffice) ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig. Sofern Daten in einer Privatwohnung verarbeitet werden, ist der Zugang zur Wohnung

Kommentiert [A3]: Zur Klarstellung eingefügt, da allgemeiner Sprachgebrauch.

zuvor mit dem Auftragnehmer abzustimmen. Der Auftragnehmer sichert zu, dass auch etwaige andere Mitbewohner der Privatwohnung mit dieser Regelung einverstanden sind.

(8) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Verantwortlichen. Hierzu kann der Auftragsverarbeiter auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, IT-Sicherheitsabteilung, Datenschutzbeauftragter, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) oder andere hinreichende Garantien vorlegen.

§ 9 Unterauftragsverhältnisse

(1) ☐ Der Auftragsverarbeiter setzt keine Unterauftragnehmer zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Sinne dieser Vereinbarung ein (Anlage 1 bleibt leer).

Kommentiert [A4]: An Position (1) gesetzt, um Bedeutung für die weiteren Angaben hervorzuheben.

(2) Soweit bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten des Verantwortlichen Unterauftragsverarbeiter für die vorliegende Verarbeitung von Daten im Auftrag einbezogen werden sollen, wird dies genehmigt, wenn folgende Voraussetzungen vorliegen:

a) Die Einschaltung von Unterauftragsverarbeitern ist nur mit schriftlicher Zustimmung des Verantwortlichen gestattet. Der Auftragsverarbeiter hat den Verantwortlichen bei jeder Hinzuziehung oder Änderung von Unterauftragsverhältnissen rechtzeitig vorab zu informieren. Der Verantwortliche hat das Recht, einzelnen Unterauftragsvergaben oder Änderungen zu widersprechen. Die in der Anlage1 „Genehmigte Unterauftragsverarbeiter“ aufgeführten Unterauftragsverarbeiter gelten als genehmigt.

b) Der Auftragsverarbeiter hat die vertraglichen Vereinbarungen mit dem / den Unterauftragnehmer(n) so zu gestalten, dass sie den Datenschutzbestimmungen im Vertragsverhältnis zwischen Auftragsverarbeiter und Verantwortlichem entsprechen. Es müssen hinreichende Garantien dafür geboten sein, dass die technischen und organisatorischen Maßnahmen den Anforderungen an die rechtmäßige Datenverarbeitung genügen.

c) Bei der Unterbeauftragung sind dem Verantwortlichen Kontroll- und Überprüfungsrechte entsprechend dieser Vereinbarung beim Unterauftragsverarbeiter einzuräumen. Dies umfasst auch das Recht des Verantwortlichen, vom Auftragsverarbeiter auf schriftliche Anforderung Auskunft über den wesentlichen Vertragsinhalt und die Umsetzung der datenschutzrelevanten Verpflichtungen im Unterauftragsverhältnis, erforderlichenfalls durch Einsicht in die relevanten Vertragsunterlagen, zu erhalten.

(3) Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z. B. Telekommunikationsleistungen, Wartung und Benutzerservice, Prüfer, Post- und Kurierdienste, Transportleistungen, Bewachungsdienste etc. Der Auftragsverarbeiter ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Verantwortlichen auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

§ 10 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, eine Auftragskontrolle mit dem Auftragsverarbeiter durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, Stichproben-kontrollen zu den jeweils üblichen Geschäftszeiten vorzunehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören. Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf Anforderung die zur Wahrung seiner Verpflichtung zur Auftragskontrolle erforderlichen Auskünfte zu geben und die entsprechenden Nachweise verfügbar zu machen.

(2) Im Hinblick auf die Kontrollverpflichtungen des Verantwortlichen vor Beginn der Datenverarbeitung und während der Laufzeit des Auftrags stellt der Auftragsverarbeiter sicher, dass sich der Verantwortliche von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen kann. Hierzu weist der Auftragsverarbeiter dem Verantwortlichen auf Anfrage die Umsetzung der technischen und organisatorischen Maßnahmen nach. Dabei kann der Nachweis der Umsetzung solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, auch durch Vorlage eines aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz) oder durch andere hinreichende Garantien erbracht werden.

§ 11 Mitteilung bei Verstößen des Auftragsverarbeiters

(1) Der Auftragsverarbeiter erstattet in allen Fällen dem Verantwortlichen eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Verantwortlichen oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.

(2) Es ist dem Auftragsverarbeiter bekannt, dass Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Verantwortlichen mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Verantwortlichen. Der Auftragsverarbeiter hat im Benehmen mit dem Verantwortlichen angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen.

(3) Soweit den Verantwortlichen Melde- und/oder Benachrichtigungspflichten treffen, hat der Auftragsverarbeiter ihn hierbei zu unterstützen. Dies gilt sowohl für die Meldung einer etwaigen Pflichtverletzung gegenüber der Aufsichtsbehörde als auch für die Benachrichtigung der von der Verletzung des Schutzes personenbezogenen Daten betroffenen Personen.

(4) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei entsprechenden Meldepflichten unterstützen.

§ 12 Weisungsbefugnis des Verantwortlichen

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierter Weisung des Verantwortlichen. Der Verantwortliche behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art, Umfang und Verfahren der Datenverarbeitung vor, das er durch Einzelweisungen konkretisieren kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Verantwortlichen erteilen.

(2) Mündliche Weisungen wird der Verantwortliche unverzüglich schriftlich oder per E-Mail (in Textform) bestätigen. Der Auftragsverarbeiter verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, sie an Dritte weiterzugeben. Kopien und Duplikate werden ohne Wissen des Verantwortlichen nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(3) Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragsverarbeiter ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch eine beim Verantwortlichen befugte Person bestätigt oder geändert wird.

§ 13 Löschung von Daten und Rückgabe von Datenträgern

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Verantwortlichen – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragsverarbeiter sämtliche in seinen Besitz gelangte Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Verantwortlichen übergeben.

§ 14 Haftung

Für Schäden des Verantwortlichen durch schuldhafte Verstöße des Auftragsverarbeiters oder etwaiger Unterauftragsverarbeiter gegen diesen Vertrag sowie gegen die ihn treffenden gesetzlichen Datenschutzbestimmungen gelten die gesetzlichen Haftungsregelungen.

§ 15 Informationspflichten, Schriftformklausel, Rechtswahl, Salvatorische Klausel

(1) Sollten die Daten des Verantwortlichen beim Auftragsverarbeiter durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich darüber zu informieren.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragsverarbeiters – bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Es gilt deutsches Recht sowie das in Deutschland unmittelbar und zwingend anzuwendende Recht der Europäischen Union.

(4) Sollten einzelne Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sein oder nach Vertragsschluss unwirksam oder undurchführbar werden, bleibt davon die Wirksamkeit dieser Vereinbarung im Übrigen unberührt.

(5) An die Stelle der unwirksamen oder undurchführbaren Bestimmung soll diejenige wirksame und durchführbare Regelung treten, deren Wirkungen der (datenschutz-)rechtlichen Zielsetzung am nächsten kommen, welche die Vertragsparteien mit der unwirksamen bzw. undurchführbaren Bestimmung verfolgt haben. Die vorstehenden Bestimmungen gelten entsprechend für den Fall, dass sich der Vertrag als lückenhaft erweist.

_____	_____
Ort, Datum	Stempel / Unterschrift Verantwortlicher

_____	_____
Ort, Datum	Stempel / Unterschrift Auftragsverarbeiter

Anlage 1 - Genehmigte Unterauftragsverarbeiter / Subunternehmer

Anlage 2a - Technische und organisatorische Maßnahmen (Auftragsbezogen)

Anlage 2b - Technische und organisatorische Maßnahmen (Allgemein)

Anlage 1
Genehmigte Unterauftragsverarbeiter / Subunternehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragsverarbeiter“). Der Auftraggeber stimmt mit Unterzeichnung dieses Vertrages der Beauftragung zu, unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 bis 4 DS-GVO:

Dabei handelt es sich um nachfolgende(s) Unternehmen:

Firmenname	**Anschrift / Land**	**Konkrete Leistung hinsichtlich §1 Gegenstand des Auftrags**

Anlage 2a
Technische und organisatorische Maßnahmen im Rahmen § 1 Gegenstand des Auftrags

der
Firma
Straße, Hausnummer
PLZ, Stadt

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen wir technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen. Die folgenden technischen und organisatorischen Maßnahmen sind dazu im Rahmen der Erfüllung des Auftrags umgesetzt (zutreffendes ist angekreuzt):

(1) Gebäudeabsicherung

- ☐ Alarmanlage
- ☐ Automatisches Zutrittskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren
- ☐ Lichtschranken / Bewegungsmelder
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☐ Einsatz von sorgfältig ausgewähltem Wachpersonal
- ☐ Absicherung von Gebäudeschächten
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Manuelles Schließsystem
- ☐ Videoüberwachung der Zugänge
- ☐ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen

(2) Absicherung Systemzugang

- ☐ Zuordnung von Benutzerrechten
- ☐ Vorgaben für sichere Passwörter
- ☐ Authentifikation mit Benutzername / Passwort
- ☐ Gehäuseverriegelungen am Server / Rechnern
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☐ Einsatz von Intrusion-Detection-Systemen
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von Datenträgern in Laptops
- ☐ Einsatz von individuellen Benutzernamen
- ☐ Authentifikation mit biometrischen Verfahren
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☐ Einsatz von VPN-Technologie (Fernzugriff)
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum Fern-Löschen)
- ☐ Sichere Passwörter für Smartphones

(3) Sicherstellung von Zugriffsberechtigungen

- ☐ Erstellen eines Berechtigungskonzepts
- ☐ Verwaltung der Rechte durch Systemadministrator
- ☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☐ Protokollierung der Vernichtung
- ☐ Verschlüsselung von Datenträgern
- ☐ Einsatz von Anti-Viren-Software
- ☐ Einsatz einer Hardware-Firewall
- ☐ Einsatz einer Software-Firewall

(4) Sicherheit beim Datentransfer

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ E-Mail-Verschlüsselung
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- ☐ Verschlüsselung externer Datenträger bei Weitergabe (USB-Sticks etc.)

(5) Nachvollziehbarkeit von Änderungen in Datenverarbeitungen

- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

(6) Einbindung von Unterauftragsverarbeitern

- ☐ Auswahl der (Unter-)Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☐ Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z. B. durch Auftragsdatenverarbeitungsvertrag)
- ☐ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt (wenn erforderlich)
- ☐ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- ☐ Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- ☐ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis/ Vertraulichkeit
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

(7) Schutz von Daten vor zufälliger Zerstörung und Verlust

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Serverräume über der Wassergrenze (nur in Hochwassergebieten relevant)
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Erstellen eines Backup- und Recoverykonzepts
- ☐ Erstellen eines Notfallplans
- ☐ Serverräume nicht unter sanitären Anlagen

(8) Maßnahmen zur Zwecktrennung von Daten

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Erstellung eines Berechtigungskonzepts
- ☐ Festlegung von Datenbank-Rechten
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☐ Keine Produktivdaten in Testsystemen

(9) Angaben zur Personenzahl

Anzahl der *Beschäftigten* (regelmäßig): xx

Anzahl der *Personen,* die personenbezogene Daten verarbeiten (regelmäßig): xx

Anzahl der *Personen* mit Zugriff auf Daten des Verantwortlichen: xx

(10) Zusätzliche Bemerkungen

_____	_____
Ort, Datum	Befugte Person (in Druckbuchstaben)
	_____
	Unterschrift der befugten Person

Anlage 2b
Allgemeine technische und organisatorische Maßnahmen

der
Firma
Straße, Hausnummer
PLZ, Stadt

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen wir technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten. Insbesondere sind Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen. Die folgenden technischen und organisatorischen Maßnahmen sind dazu in unserem Unternehmen umgesetzt (zutreffendes ist angekreuzt ODER Anlage eigener Beschreibung):

(1) Gebäudeabsicherung

- ☐ Alarmanlage
- ☐ Automatisches Zutrittskontrollsystem
- ☐ Schließsystem mit Codesperre
- ☐ Biometrische Zugangssperren
- ☐ Lichtschranken / Bewegungsmelder
- ☐ Schlüsselregelung (Schlüsselausgabe etc.)
- ☐ Protokollierung der Besucher
- ☐ Einsatz von sorgfältig ausgewähltem Wachpersonal
- ☐ Absicherung von Gebäudeschächten
- ☐ Chipkarten-/Transponder-Schließsystem
- ☐ Manuelles Schließsystem
- ☐ Videoüberwachung der Zugänge
- ☐ Sicherheitsschlösser
- ☐ Personenkontrolle beim Pförtner / Empfang
- ☐ Sorgfältige Auswahl von Reinigungspersonal
- ☐ Tragepflicht von Berechtigungsausweisen

(2) Absicherung Systemzugang

- ☐ Zuordnung von Benutzerrechten
- ☐ Vorgaben für sichere Passwörter
- ☐ Authentifikation mit Benutzername / Passwort
- ☐ Gehäuseverriegelungen am Server / Rechnern
- ☐ Sperren von externen Schnittstellen (USB etc.)
- ☐ Einsatz von Intrusion-Detection-Systemen
- ☐ Verschlüsselung von Smartphone-Inhalten
- ☐ Verschlüsselung von Datenträgern in Laptops
- ☐ Einsatz von individuellen Benutzernamen
- ☐ Authentifikation mit biometrischen Verfahren
- ☐ Zuordnung von Benutzerprofilen zu IT-Systemen
- ☐ Einsatz von VPN-Technologie (Fernzugriff)
- ☐ Verschlüsselung von mobilen Datenträgern
- ☐ Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum Fern-Löschen)
- ☐ Sichere Passwörter für Smartphones

(3) Sicherstellung von Zugriffsberechtigungen

- ☐ Erstellen eines Berechtigungskonzepts
- ☐ Anzahl der Administratoren auf das „Notwendigste“ reduziert
- ☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- ☐ Physische Löschung von Datenträgern vor Wiederverwendung
- ☐ Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- ☐ Verschlüsselung von Datenträgern
- ☐ Einsatz einer Hardware-Firewall
- ☐ Verwaltung der Rechte durch Systemadministrator
- ☐ Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- ☐ Sichere Aufbewahrung von Datenträgern
- ☐ Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)
- ☐ Protokollierung der Vernichtung
- ☐ Einsatz von Anti-Viren-Software
- ☐ Einsatz einer Software-Firewall

(4) Sicherheit beim Datentransfer

- ☐ Einrichtungen von Standleitungen bzw. VPN-Tunneln
- ☐ E-Mail-Verschlüsselung
- ☐ Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
- ☐ Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen
- ☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
- ☐ Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
- ☐ Beim physischen Transport: sichere Transportbehälter/-verpackungen
- ☐ Verschlüsselung externer Datenträger bei Weitergabe (USB-Sticks etc.)

(5) Nachvollziehbarkeit von Änderungen in Datenverarbeitungen

- ☐ Protokollierung der Eingabe, Änderung und Löschung von Daten
- ☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- ☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- ☐ Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
- ☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

(6) Einbindung von Unterauftragsverarbeitern

- ☐ Auswahl der (Unter-)Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- ☐ Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z. B. durch Auftragsdatenverarbeitungsvertrag)
- ☐ Auftragsverarbeiter hat Datenschutzbeauftragten bestellt (wenn erforderlich)
- ☐ Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- ☐ Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- ☐ Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis/ Vertraulichkeit
- ☐ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- ☐ Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

(7) Schutz von Daten vor zufälliger Zerstörung und Verlust

- ☐ Unterbrechungsfreie Stromversorgung (USV)
- ☐ Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- ☐ Feuer- und Rauchmeldeanlagen
- ☐ Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- ☐ Testen von Datenwiederherstellung
- ☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- ☐ Serverräume über der Wassergrenze (nur in Hochwassergebieten relevant)
- ☐ Klimaanlage in Serverräumen
- ☐ Schutzsteckdosenleisten in Serverräumen
- ☐ Feuerlöschgeräte in Serverräumen
- ☐ Erstellen eines Backup- und Recoverykonzepts
- ☐ Erstellen eines Notfallplans
- ☐ Serverräume nicht unter sanitären Anlagen

(8) Maßnahmen zur Zwecktrennung von Daten

- ☐ Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- ☐ Erstellung eines Berechtigungskonzepts
- ☐ Festlegung von Datenbank-Rechten
- ☐ Trennung von Produktiv- und Testsystem
- ☐ Logische Mandantentrennung (softwareseitig)
- ☐ Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
- ☐ Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
- ☐ Keine Produktivdaten in Testsystemen