Vertrag zur Auftragsverarbeitung

zwischen

XXX

als Verantwortlicher (in der Folge „Auftraggeber“) einerseits

und

XXX

als Auftragsverarbeiter (in der Folge „Auftragnehmer“) andererseits

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in Punkt III. genannten Leistungen beauftragen, in deren Zuge vom Auftragnehmer personenbezogene Daten verarbeitet werden. Zur Wahrung der Anforderungen an die Auftragsverarbeitung gem. Art. 28 EU-DSGVO schließen die Parteien daher die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

Dieser Vertrag orientiert sich an den Standardvertragsklauseln der EU-Kommission, die mit DURCHFÜHRUNGSBESCHLUSS (EU) 2021/915 vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates eingeführt wurden.

I. Angabe der zuständigen Datenschutz-Aufsichtsbehörde

Zuständige Aufsichtsbehörde für die Vertragsparteien ist die Österreichische Datenschutzbehörde, Barichgasse 40-42, 1030 Wien. Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Vertrag zur Auftragsverarbeitung

II. Vertragsgegenstand

(1) Der Auftragnehmer erbringt auf Grundlage des Vertrags/Auftrags/Bestellung vom xx.xx.xxxx für den Auftraggeber Leistungen im Bereich xxx zum Zweck der … (in der Folge „Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich, soweit vorstehend nicht näher ausgeführt, aus dem Hauptvertrag, die Prüfung der Zulässigkeit der Datenverarbeitung obliegt ausschließlich dem Auftraggeber.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung, wobei hinsichtlich datenschutzrechtlicher Rechte und Pflichten die Bestimmungen dieses Vertrages allenfalls widersprechenden Bestimmungen des Hauptvertrags stets vorgehen.

(3) Die Pflichten aus diesem Vertrag betreffen alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei in deren Zuge der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden.

III. Kategorien der verarbeiteten Daten und der betroffenen Personen

(1) Die Kategorien der von der Datenverarbeitung betroffenen Personen sind:

. . . . . .

(2) Kategorien personenbezogener Daten, die verarbeitet werden:

. . . . . .

(3) Verarbeitete sensible Daten (falls zutreffend) und angewandte Beschränkungen oder Garantien, die der Art der Daten und den verbundenen Risiken in vollem Umfang Rechnung tragen, z. B. strenge Zweckbindung, Zugangsbeschränkungen (einschließlich des Zugangs nur für Mitarbeiter, die eine spezielle Schulung absolviert haben), Aufzeichnungen über den Zugang zu den Daten, Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen:

. . . . . .

. . . . . .

(4) Art der Verarbeitung

. . . . . .

IV. Weisungsrecht des Auftraggebers

(1) Der Auftragnehmer ist verpflichtet, Daten ausschließlich im Rahmen des Hauptvertrags und gemäß den ausdrücklichen Weisungen des Auftraggebers zu erheben, zu verarbeiten oder zu nutzen; dies betrifft auch die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Sofern der Auftragnehmer durch das Recht der Europäischen Union oder eines Mitgliedstaates, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet ist, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Pflichten des Auftragnehmers werden durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Zur Erteilung entsprechender Weisungen ist der Auftraggeber jederzeit berechtigt, wobei dies auch Weisungen zu Berichtigung, Löschung und Sperrung von Daten umfasst. Erteilte Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer schriftlich zu dokumentieren.

(3) Sofern der Auftragnehmer zur Ansicht gelangt, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen und ist in diesem Fall berechtigt, die Durchführung dieser Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

(4) Der Auftragnehmer verarbeitet die personenbezogenen Daten nur für den/die vereinbarten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Auftraggebers erhält.

(5) Die Daten werden vom Auftragnehmer nur während der vereinbarten Dauer verarbeitet.

V. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer stellt dem Auftraggeber alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind.

(2) Der Auftraggeber ist berechtigt, vor der Aufnahme der Datenverarbeitung und in weiterer Folge regelmäßig die technischen und organisatorischen Maßnahmen des Auftragnehmers zu prüfen. In diesem Rahmen kann der Auftraggeber die technischen und organisatorischen Maßnahmen des Auftragnehmers nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Auftraggeber einschlägige Zertifizierungen des Auftragnehmers berücksichtigen.

(3) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers erforderlich sind.

(4) Der Auftraggeber dokumentiert das Kontrollergebnis und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

VI. Datenschutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ergreift mindestens die in Anhang ./1 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes personenbezogener Daten“). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

(2) Der Auftragnehmer gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten („sensible Daten“), wendet der Auftragnehmer spezielle Beschränkungen und/oder zusätzlichen Garantien an.

VII. Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Auftraggeber dazu ermächtigt.

(2) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragnehmer den Auftraggeber bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten befolgt der Auftragnehmer die Weisungen des Auftraggebers.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen zudem bei der Einhaltung der folgenden Pflichten:

a. Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung“), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;

b. Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Auftraggeber keine Maßnahmen zur Eindämmung des Risikos trifft;

c. Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragnehmer den Auftraggeber unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;

d. Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679 und Artikel 36 bis 38 der Verordnung (EU) 2018/1725.

VIII. Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragnehmer mit dem Auftraggeber zusammen und unterstützt ihn entsprechend, damit der Auftraggeber seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragnehmer die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

(1) Verletzung des Schutzes der vom Auftraggeber verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftraggeber verarbeiteten Daten unterstützt der Auftragnehmer den Auftraggebern wie folgt:

a. bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Auftraggeber die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b. bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Auftraggebers anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1. die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

2. die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

3. die vom Auftraggeber ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c. bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

(2) Verletzung des Schutzes der vom Auftragnehmer verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragnehmer verarbeiteten Daten meldet der Auftragnehmer diese dem Auftraggeber unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a. eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b. Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c. die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

IX. Einsatz von Subunternehmern

(1) Der Auftragnehmer besitzt die allgemeine Genehmigung des Auftraggebers für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragnehmer unterrichtet den Auftraggebern mindestens einmal jährlich im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Auftraggeber damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragnehmer stellt dem Auftraggeber die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

(2) Beauftragt der Auftragnehmer einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Auftraggebers), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragnehmer gemäß diesen Klauseln gelten. Der Auftragnehmer stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragnehmer entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

(3) Der Auftragnehmer stellt dem Auftraggeber auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

(4) Der Auftragnehmer haftet gegenüber dem Auftraggeber in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragnehmer geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Auftraggebern, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

(5) Der Auftragnehmer vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Auftraggeber – im Falle, dass der Auftragnehmer faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

X. Internationale Datenübermittlungen

(1) Jede Übermittlung von Daten durch den Auftragnehmer an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Auftraggebers oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragnehmer unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

(2) Der Auftraggeber erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragnehmer einen Unterauftragsverarbeiter für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Auftraggebers) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragnehmer und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.x

XI. Verstöße gegen den Vertrag und Beendigung des Vertrags

(1) Falls der Auftragnehmer seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Auftraggeber – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragnehmer anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält

oder der Vertrag beendet ist. Der Auftragnehmer unterrichtet den Auftraggebern unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

(2) Der Auftraggeber ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

a. der Auftraggeber die Verarbeitung personenbezogener Daten durch den Auftragnehmer gemäß (1) ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

b. der Auftragnehmer in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

c. der Auftragnehmer einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

(3) Der Auftragnehmer ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Auftraggeber auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragnehmer darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen verstoßen.

(4) Nach Beendigung des Vertrags löscht der Auftragnehmer nach Wahl des Auftraggebers alle im Auftrag des Auftraggebers verarbeiteten personenbezogenen Daten und bescheinigt dem Auftraggeber, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Auftraggeber zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragnehmer weiterhin die Einhaltung dieser Klauseln.

XII. Schlussbestimmungen

(1) Die Einrede eines Zurückbehaltungsrechts durch den Auftragnehmer aufgrund nicht gehörig erfüllten Vertrags oder jeder anderen Rechtsgrundlage ist hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen.

(2) Änderungen dieser Vereinbarung bedürfen der Schriftform, dies betrifft insbesondere auch das Abgehen vom Schriftformerfordernis selbst.

(3) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein, bleibt davon die Wirksamkeit der übrigen Bestimmungen unberührt. Die Parteien werden die unwirksame Bestimmung unverzüglich durch eine wirksame Bestimmung ersetzen, die dem Zweck der unwirksamen Bestimmung am nächsten kommt und rechtswirksam ist. Mangels Einigung gilt eine solche Bestimmung als vereinbart, die dem ursprünglichen Parteiwillen am nächsten kommt und rechtswirksam ist.

(4) Diese Vereinbarung unterliegt dem Recht der Republik Österreich unter Ausschluss der Kollisionsnormen. Ausschließlicher Gerichtsstand ist das für [XXX] örtlich und sachlich zuständige Gericht.

(5) Dieser Vereinbarung liegt folgende Anlage bei, die einen integrierenden Bestandteil des Vertrages bildet:

- **Anlage ./1** – Technische und organisatorische Maßnahmen des Auftragnehmers

Vertrag zur Auftragsverarbeitung

Ort, am TT.MM.JJJJ

Anlage ./1 – Technische und organisatorische Maßnahmen des Auftragnehmers

Bitte geben Sie die in Ihrem Unternehmen vorhandenen technischen und organisatorischen Maßnahmen durch Ankreuzen oder selbstständige Ergänzung an. Für allfällige Fragen stehen wir gerne zur Verfügung.

1. Zugangskontrolle

Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte

1.1 *bauliche Maßnahmen*

O versperrte Eingangs- und Innentüren

O Einbruchssicherung

O Zutrittskontrollsysteme

O Videoüberwachung

O Sonstiges:

1.2 *technische Maßnahmen*

O Verfahren zur User-Anmeldung und Abmeldung

O Verwaltung von Admin-Rechten

O Passwortvorgaben (IT-Richtlinie)

O Sonstiges:

1.3 *organisatorische Maßnahmen*

O Besucher werden am Betriebsgelände nicht unbeaufsichtigt gelassen

O eigene Besprechungszimmer, in denen keine Akten zugänglich sind

O Protokollierung über Besuche (wer, wann, bei wem, warum)

O Sonstiges:

2. Datenträgerkontrolle

Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern

2.1 *technische Maßnahmen*

O sichere Aufbewahrung der Speichermedien (versperrt)

O Dokumentieren und Kontrollieren der Anfertigung von Kopien

O verschlüsseltes Speichern

O datenschutzgerechte Entsorgung von Geräten mit Speichermedien (z.B. auch Druckern)

O datenschutzgerechtes Löschen und Wiederverwenden von Speichermedien (Sticks)

O Sonstiges:

2.2 *organisatorische Maßnahmen*

O Dokumentation der Ausgabe und Verwendung von mobilen Speichermedien (Wer hat welchen USB-Stick oder sonstiges Speichermedium? Nummerierung und Zuordnung)

O Kontrolle über die Datenweitergabe

O Sonstiges:

3. Speicherkontrolle

Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

3.1 *technische Maßnahmen*

O Bildschirm- und Computersperre bei Verlassen des Arbeitsplatzes

O Benutzeridentifizierung

O Protokollierung des Verhaltens der Nutzer

O Verschlüsselte Speicherung der Daten

O Trennung von Administration- und Produktionsbereich

O Sonstiges:

3.2 *organisatorische Maßnahmen*

O Protokollierung der Art und Weise des Zugriffes auf die Daten

O Sonstiges:

4. Benutzerkontrolle

Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

4.1 technische Maßnahmen

O Firewall, Intrusion Detection/Prevention

O Benutzeridentifizierung

O sichere technische Passwortvorgabe

O Absicherung der Geräte und Netzwerke

O Sonstiges:

4.2 *organisatorische Maßnahmen*

O Festlegung der Personen, die Nutzungsberechtigungen haben (Zuständigkeiten)

O Protokollierung der Nutzer und Aktivitäten

O Passwortpolicy / Passwortrichtlinie

O Clean-Desk-Policy

O Sonstiges:

5. Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben

5.1 *technische Maßnahmen*

O Berechtigungskonzept

O Benutzeridentifizierung

O Schnittstellensicherung

O Verschlüsselung

O Kopierkontrolle

O Netzwerkkontrolle (kein Anschluss von nicht betriebseigenen Geräten)

O Berechtigungsprüfung (automatisiert)

O Sonstiges:

5.2 *organisatorische Maßnahmen*

O Verwaltung und Kontrolle der Zugriffsberechtigungen

O Kontrolle der Zugriffe (Protokollierung)

O Dokumentation der Maßnahmen zur Datenvernichtung

O Sonstiges:

6. Übertragungskontrolle

Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können

6.1 *technische Maßnahmen*

O Protokollierung von Datenübermittlungen

O Auswertungsmöglichkeiten (Feststellung der Sender und Empfänger)

O Sonstiges:

6.2 organisatorische Maßnahmen

O Festlegung von Übermittlungswegen (wie wird an welche Empfängerkategorie übermittelt)

O Sonstiges:

7. Eingabekontrolle

Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind

7.1 *technische Maßnahmen*

O Benutzeridentifizierung

O Protokollierung der Eingabe, Änderung und Löschung personenbezogener Daten

O Einsatz von elektronischen Signaturen

O Sonstiges:

7.2 *organisatorische Maßnahmen*

O Festlegung von Berechtigungen

O sichere Ablage und fristgerechte Löschung von Protokollen

O Sonstiges:

8. Transportkontrolle

Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können

8.1 *technische Maßnahmen*

O Verschlüsselte Übertragung und Speicherung auf Datenträgern

O Zugriff mittels verschlüsselten VPNS

O Protokollierung der Übermittlung von Daten

O Duplizieren von Datenträgern

O Schutz vor Schadsoftware (z.B. Viren)

O sicheres Löschen auf Datenträgern

O Verwendung von sicheren Transportbehältern

O Sonstiges:

8.2 *organisatorische Maßnahmen*

O Sicherstellung von sicheren Transporten von Datenträgern (zuverlässige Personen oder Unternehmen)

O Kontrolle des Transportweges und der Transportzeit (Rückfrage)

O Datenträger-Eingangs- und Ausgangsverzeichnis

O Sonstiges:

9. Verfahren zur Wiederherstellung der Systeme

Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können

9.1 *Technische Maßnahmen*

O Datensicherungen erfolgen in periodischen Abständen

O Datensicherungen werden an betriebsfremden Orten aufbewahrt

O Sonstiges:

9.2 *Organisatorische Maßnahmen*

O Wiederherstellungs-Stresstest

O Sonstiges:

10. Gewährleistung der Zuverlässigkeit und Integrität

Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

10.1 *technische Maßnahmen*

O Datensicherungen erfolgen in periodischen Abständen

O Einsatz von Virenscannern, Firewalls, Spam-Filter

O Sicherstellung der Stromversorgung bei Ausfall

O Einsatz von elektronischen Signaturen

O Sonstiges:

10.2 *organisatorische Maßnahmen*

O Datensicherungs- und Wiederherstellungskonzept

O Systemüberwachung der relevanten Hard- und Software

O Sonstiges:

Ort, am TT.MM.JJJJ