Vereinbarung zur Auftragsverarbeitung gem. Art. 28 DSGVO

zwischen

- nachstehend **Auftraggeber** genannt -

und der

TAFEU GmbH, Hauptstraße 1, 55257 Budenheim, Deutschland

- nachstehend **Auftragnehmer** genannt -

Präambel

Im Rahmen der Leistungserbringung nach dem vom Auftraggeber erteilten Auftrag (nachfolgend „**Hauptvertrag**“ genannt) ist es erforderlich oder zumindest nicht auszuschließen, dass der Auftragnehmer mit personenbezogenen Daten umgeht, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert. Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Vertragsparteien im Zusammenhang mit dem Umgang des Auftragnehmers mit den Daten des Auftraggebers zur Durchführung des Hauptvertrags.

§ 1 Anwendungsbereich, Gegenstand und Dauer der Verarbeitung

(1) Diese Datenschutzvereinbarung findet Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(2) Der Gegenstand und die Dauer des Auftrages sowie Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber ergeben sich aus dem Hauptvertrag.

(3) Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des Hauptvertrags. Eine Kündigung des Hauptvertrags bewirkt automatisch auch eine Kündigung dieser Vereinbarung. Das Recht zur außerordentlichen Kündigung bleibt unberührt.

(4) Gegenstand der Erhebung und Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

☐ Personenstammdaten (z.B. Name, Vorname, Anschrift, Geburtsdatum)

☐ Kommunikationsdaten (z.B. Telefonnummern, E-Mail-Adressen)

☐ Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)

☐ Kundenhistorie

☐ Vertragsabrechnungs- und Zahlungsdaten

☐ Auskunftsangaben (von Dritten, z.B. Auskunfteien oder öffentlichen Verzeichnissen)

☐ Sonstige Daten: _____

(5) Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

(durch den Auftraggeber vollständig und richtig auszufüllen/anzukreuzen!)

☐ Kunden

☐ Interessenten

☐ Abonnenten

☐ Beschäftigte

☐ Lieferanten

☐ Handelsvertreter

☐ Ansprechpartner

☐ Sonstige Betroffene: _____

(6) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich 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 Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

§ 2 Definitionen

(1) Personenbezogene Daten

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).

(2) Datenverarbeitung im Auftrag

Datenverarbeitung im Auftrag ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Sinne des Art. 28 DSGVO.

(3) Weisung

Eine Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Berichtigung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden anfänglich durch den Hauptvertrag und diese Vereinbarung festgelegt und können vom Auftraggeber danach in schriftlicher Form durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung).

§ 3 Verantwortlichkeit für die Datenverarbeitung

(1) Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung, verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO). Sollten Dritte gegen den Auftragnehmer aufgrund der Erhebung, Verarbeitung oder Nutzung von Daten des Auftraggebers Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

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

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer sichert die Umsetzung und Einhaltung der im Vorfeld der Auftragsvergabe dargelegten technischen und organisatorischen Maßnahmen gem. Art. 32 DSGVO vor Beginn der Verarbeitung zu. Diese sind durch den Auftragnehmer in der beigefügten Anlage 1„Übersicht über die technisch-organisatorischen Maßnahmen“ dokumentiert.

(2) Die in der vorgenannten Anlage dokumentierten Maßnahmen sind Grundlage dieser Vereinbarung. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Soweit die Prüfung / ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, sofern das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen schriftlichen Zustimmung des Auftraggebers und sind vom Auftragnehmer zu dokumentieren und dem Auftraggeber auf Anforderung zur Verfügung zu stellen.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer hat Daten nur nach Weisung des Auftraggebers unter Beachtung von § 7 dieser Vereinbarung zu verarbeiten. Der Auftragnehmer hat ausschließlich nach Weisung des Auftraggebers die Daten, die im Auftrag verarbeitet werden, zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken. Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zwecks Berichtigung oder Löschung seiner Daten oder Auskunft über die gespeicherten Daten des Auftraggebers wenden sollte, wird der Auftragnehmer dieses Ersuchen zeitnah an den Auftraggeber weiterleiten.

(2) Der Auftragnehmer stellt sicher und kontrolliert regelmäßig, dass die Datenverarbeitung und -nutzung im Rahmen der Leistungserbringung nach dem Hauptvertrag in seinem Verantwortungsbereich, der Unterauftragnehmer nach § 10 dieser Vereinbarung einschließt, in Übereinstimmung mit den Bestimmungen dieser Vereinbarung erfolgt.

(3) Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsdatenverarbeitung keine Kopien oder Duplikate der Daten des Auftraggebers anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Hauptvertrag (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(4) Der Auftragnehmer unterstützt den Auftraggeber bei Kontrollen durch die Aufsichtsbehörde im Rahmen des Zumutbaren und Erforderlichen, soweit diese Kontrollen die Datenverarbeitung durch den Auftragnehmer betreffen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, nachzuweisenden Aufwände und Kosten.

(5) Der Auftragnehmer teilt dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit (sofern ein solcher vom Auftragnehmer nach den gesetzlichen Bestimmungen zu bestellen ist) und den Ansprechpartner für im Rahmen des Vertrags anfallende Datenschutzfragen.

(6) Der Auftragnehmer hat die bei der Verarbeitung von Daten des Auftraggebers beschäftigten Personen gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DSGVO zur Vertraulichkeit zu verpflichten.

(7) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er feststellt, dass er oder ein Mitarbeiter bei der Verarbeitung von Daten des Auftraggebers gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus dieser Vereinbarung verstoßen haben und die Voraussetzungen der Artt. 33, 34 DSGVO vorliegen. Soweit den Auftraggeber gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von Daten des Auftraggebers (insbesondere nach Artt. 33, 34 DSGVO) treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden, nachzuweisenden Aufwände und Kosten zu unterstützen. Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung durchführen.

§ 6 Pflichten des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von betroffenen Personen ist allein der Auftraggeber verantwortlich.

(2) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(3) Dem Auftraggeber obliegen die aus Art. 33, 34 DSGVO resultierenden Meldepflichten.

§ 7 Weisungsbefugnis des Auftraggebers

(1) Der Auftragnehmer verarbeitet die Daten des Auftraggebers ausschließlich in Übereinstimmung mit den Weisungen des Auftraggebers, wie sie abschließend in den Bestimmungen dieser Vereinbarung und den Festlegungen des Hauptvertrags Ausdruck finden. Weisungen des Auftraggebers dürfen die vertraglich vereinbarten Leistungspflichten aus dem Hauptvertrag nicht unmöglich machen. Einzelweisungen, die von den Festlegungen dieser Vereinbarung abweichen oder zusätzliche Anforderungen aufstellen, bedürfen einer vorherigen Zustimmung des Auftragnehmers. Ziehen Einzelweisungen Mehrkosten nach sich, insbesondere wenn diese über den vertraglich vereinbarten Leistungsumfang hinausgehen, sind diese dem Auftragnehmer zu vergüten.

(2) Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder in Textform (z.B. per E-Mail) bestätigen.

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 S. 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

§ 8 Unterstützungspflichten

(1) Ist der Auftraggeber auf Grund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Informationen oder Auskünfte zur Verarbeitung von Daten dieser Person zu geben oder die Rechte von betroffenen Personen nach Kapitel III (Artt. 12 bis 23) der DSGVO zu gewährleisten, wird der Auftragnehmer den Auftraggeber soweit vereinbart bei der Erfüllung dieser Pflichten mit geeigneten technischen und organisatorischen Maßnahmen entsprechend Art. 28 Abs. 3 lit. e DSGVO unterstützen.
(2) Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten entsprechend Art. 28 Abs. 3 lit. f DSGVO bei der Einhaltung der in den Artt. 32 bis 36 DSGVO genannten Pflichten.
(3) Bei der Erbringung der Unterstützungsleistungen nach Abs. 1 und 2 dem Auftragnehmer entstehenden und nachzuweisenden Aufwände und Kosten sind vom Auftraggeber zu ersetzen.
(4) Im Falle einer Inanspruchnahme einer Vertragspartei durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO verpflichtet sich die in Anspruch genommene Vertragspartei, die andere Vertragspartei unverzüglich zu informieren. Die Vertragsparteien werden sich bei der Abwehr des Anspruchs gegenseitig unterstützen.

§ 9 Kontrollrechte des Auftraggebers

(1) Im Hinblick auf die Kontrollverpflichtungen des Auftraggebers nach Art. 28 Abs. 3 lit. h DSGVO stellt der Auftragnehmer sicher, dass sich der Auftraggeber von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung überzeugen kann.

(2) Der Auftragnehmer gewährt dem Auftraggeber die zur Durchführung dieser Kontrollen erforderlichen Zugangs-, Auskunfts- und Einsichtsrechte.

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

(4) Der Auftraggeber ist berechtigt, im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers die Geschäftsräume des Auftragnehmers, in denen die Daten des Auftraggebers verarbeitet werden, zu betreten, um sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung zu überzeugen.

(5) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung anstatt einer Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz), einer Bestätigung der Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DSGVO oder der Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DSGVO erbracht werden, wenn diese Prüfungsberichte es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen gemäß der Anlage zu dieser Vereinbarung zu überzeugen.

(6) Zur Durchführung der Kontrolle muss der Auftragnehmer nur eine solche Person zulassen, die besonders zur Geheimhaltung, insbesondere in Bezug auf Informationen über den Betrieb des Auftragnehmers, dessen Ausstattung, Geschäftsgeheimnisse des Auftragnehmers und Sicherheitsmaßnahmen, verpflichtet ist. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen. Eine die Kontrolle im Namen des Auftraggebers durchführende Person muss mindestens eine Woche vor Durchführung der Kontrolle ihre Legitimation durch den Auftraggeber schriftlich oder per Telefax nachweisen.

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

(8) Die Kosten für die Durchführung der Kontrolle trägt der Auftraggeber. Das Ergebnis der Prüfung wird dem Auftragnehmer auf Verlangen in geeigneter Form (Gutachten, Testat, Berichte, Berichtsauszüge, etc.) zur Verfügung gestellt.

§10 Unterauftragnehmer (weiterer Auftragsverarbeiter nach Art. 28 Abs. 2 und 4 DSGVO)

(1) Die Weitergabe von Aufträgen im Rahmen der im Hauptvertrag konkretisierten Tätigkeiten an Subunternehmer oder Unterauftragnehmer (im Folgenden einheitlich: Unterauftragnehmer) durch den Auftragnehmer bedarf der vorherigen schriftlichen Zustimmung durch den Auftraggeber. Gleiches gilt für die Ersetzung eines bestehenden Unterauftragnehmers.

(2) Eine solche vorherige Zustimmung darf vom Auftraggeber nur aus wichtigem, dem Auftragnehmer nachzuweisenden Grund verweigert werden. Im Fall der Einschaltung eines nach §§ 15ff. AktG mit dem Auftragnehmer verbundenen Unternehmens als Unterauftragnehmer erteilt der Auftraggeber hiermit ausdrücklich seine Zustimmung. Die vom Auftragnehmer eingesetzten Unterauftragnehmer sind in Anlage 2 aufgeführt. Für die in Anlage 2 genannten Unterauftragnehmer gilt die Genehmigung mit Unterzeichnung dieser Vereinbarung als erteilt. Der Auftragnehmer informiert den Aufraggeber vorab über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen diese Änderung Einspruch zu erheben (Art. 28 Abs. 2 DSGVO). Erfolgt kein Einspruch innerhalb von 14 Tage ab Bekanntgabe, gilt die Zustimmung zur Änderung als gegeben.

(3) Erteilt der Auftragnehmer unter Beachtung von Abs. 1 Aufträge an Unterauftragnehmer, so obliegt es dem Auftragnehmer, seine Pflichten aus diesem Vertrag dem Unterauftragnehmer zu übertragen.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen nach Artt. 44 ff. DSGVO sicher.

(5) Keiner Zustimmung bedarf die Einschaltung von Unterauftragnehmern, bei denen der Unterauftragnehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach dem Hauptvertrag in Anspruch nimmt, auch wenn dabei ein Zugriff auf die Daten des Auftraggebers nicht ausgeschlossen werden kann; dazu zählen insbesondere Telekommunikationsleistungen, Post- oder Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen. Der Auftragnehmer wird mit solchen Unterauftragnehmern branchenübliche Geheimhaltungsvereinbarungen treffen.

§ 11 Löschung von Daten und Rückgabe von Datenträgern

(1) Nach Abschluss der vertraglichen Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrags – hat der Auftragnehmer sämtliche in seinen Besitz gelangte Daten des Auftraggebers, die Gegenstand dieser Vereinbarung sind, zu löschen und von dem Auftraggeber erhaltene Datenträger, die zu diesem Zeitpunkt noch Daten des Auftraggebers enthalten, an den Auftraggeber auszuhändigen. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(2) Führt eine vom Auftraggeber verlangte Löschung der Daten des Auftraggebers dazu, dass der Auftragnehmer seine Leistungspflichten nach dem Hauptvertrag nicht mehr ordnungsgemäß erbringen kann, wird der Auftragnehmer von der Verpflichtung zur Leistung frei.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 12 Haftung

Eine zwischen den Vertragsparteien im Hauptvertrag vereinbarte Haftungsregelung gilt auch für die Auftragsverarbeitung, es sei denn, die Vertragsparteien haben ausdrücklich etwas anderes vereinbart.

§ 13 Schlussvorschriften

(1) Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrags. Im Fall von Widersprüchen zwischen dieser Vereinbarung und Regelungen aus sonstigen vertraglichen Abreden, insbesondere aus dem Hauptvertrag, gehen die Regelungen aus dieser Vereinbarung vor.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen des Auftragnehmers oder Änderungen der Anlage - 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) Ausschließlicher Gerichtsstand für alle aus diesem Vertrag sich ergebenden Streitigkeiten ist der Sitz des Auftragnehmers.

(4) Es gilt deutsches Recht.

Ort, Datum	Ort, Datum
Auftraggeber	Auftragnehmer

Anlage 1

Übersicht über die technisch-organisatorischen Maßnahmen

In Verbindung mit § 4 der Vereinbarung zur Auftragsverarbeitung verpflichten sich die Vertragsparteien in ihrem jeweiligen Verfügungsbereich und bezogen auf den Vertragsgegenstand, die technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO im erforderlichen sowie angemessenen Umfang und nach dem allgemein anerkannten Stand der Technik umzusetzen.

Im Einzelnen handelt es sich um folgende Maßnahmen:

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren.

Vom Auftragnehmer umgesetzte Maßnahmen:

- Festlegung der zugangsberechtigten Personen
- Closed Shop-Betrieb (nur berechtigte Personen haben Zutritt, alternativ: kein Besucherverkehr)
- Revisionsfähigkeit der Zugangsberechtigungen
- Schaffung von Sicherheitszonen
- Identifikation durch Ausweise etc.
- Einsatz eines Zugangskontrollsystems, Schlüsselregelung und aktuelle Schlüsselliste
- Zugangsregelungen für betriebsfremde Personen
- Maßnahmen zur Innen- und Außenhautsicherung
- Protokollierung der Zu- und Abgänge
- Empfang / Pförtner
- Verschlossene Bürotüren und Fenster bei Abwesenheit
- Sicherung auch außerhalb der Arbeitszeit durch Alarmanlage, und / oder Werkschutz

2. Zugangskontrolle

Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Vom Auftragnehmer umgesetzte Maßnahmen:

- Festlegung der nutzungsberechtigten Personen
- Identifikation und Authentifizierung der Benutzer
- Sicherung der Datenstationen, Netze und Übertragungsleitungen
- Verschlüsselung der zu übertragenden Daten

- Protokollierung der Benutzer und deren Aktivitäten
- Passwortrichtlinie (bzgl. Länge, Änderungsintervall, etc.)
- Verwendung von passwortgeschützten Bildschirmschonern / Sperren

3. Zugriffskontrolle

Es ist Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Vom Auftragnehmer umgesetzte Maßnahmen:

- Identifikation und Authentifizierung der Benutzer
- Maschinelle Überprüfung der Berechtigungen
- Einführung zugriffsbeschränkender Maßnahmen (z. B. nur Leseberechtigung)
- Beschränkung der freien Abfragemöglichkeiten von Datenbanken (Query-Spache)
- Benutzerbezogene Protokollierung der (Fehl-)Zugriffe
- Einsatz von Verschlüsselungsverfahren
- Zentrale Vergabestelle von Benutzerrechten

4. Trennungskontrolle

Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Vom Auftragnehmer umgesetzte Maßnahmen:

- Datenspeicherung wird mit dem Zweck der Datenerhebung versehen (z.B. durch Dateibezeichnung)
- Mandantentrennung - Logische Trennung der Daten (z.B. unterschiedliche Dateiverzeichnisse)
- Mandantentrennung - Physikalische Trennung der Daten (z.B. unterschiedliche Hardware)
- Einsatz unterschiedlicher Verschlüsselungen

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

1. Weitergabekontrolle

Es ist Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Vom Auftragnehmer umgesetzte Maßnahmen:

- Dokumentation der Abruf- und Übermittlungsprogramme
- Festlegung der Übermittlungswege und der Datenempfänger
- Protokollierung der Datenübermittlung
- Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden gezielt feststellen zu können
- Festlegung der für die Übermittlung oder den Transport Berechtigten
- Regelungen für die Versandart und Festlegung des Transportweges
- Sicherung des Übertragungs- und Transportweges
- Physikalische Löschung aller Datenträger vor einer neuen Beschreibung und nach jeder Verarbeitung
- Verschlüsselung der Daten
- Überprüfung aller Daten und Datenträger hinsichtlich Virenbefall
- Vollständigkeits- und Richtigkeitsprüfung (nach der Übertragung)
- Fernwartungskonzept
- Nutzung eines VPN

2. Eingabekontrolle

Es ist Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Vom Auftragnehmer umgesetzte Maßnahmen:

- Festlegung von Eingabebefugnissen
- Protokollierung der Eingaben, Veränderungen und Löschungen
- Speicherung des Veranlassers
- Lückenlose Vorgangsprotokollierung für jeden Einzelfall
- Einsatz der elektronischen Signatur

III. Verfügbarkeit, Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO) und Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Personenbezogene Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.

Vom Auftragnehmer umgesetzte Maßnahmen:

- Backup-Systeme zur Wiederherstellung verlorener Daten
- Testen der Wiederherstellung
- Notfallkonzept mit Wiederanlaufplan
- USV (Unterbrechungsfreie Stromversorgung)
- Redundante Leitungsversorgung
- Notstromaggregat
- Brandmelder
- Brandschutz- und Katastrophenordnung
- Zentrale Datensicherung
- Räumlich getrennte Aufbewahrung der erstellten Datensicherungen
- Objektsicherung insb. der Serverräume
- Virenschutzkonzept
- Klimatisierung

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

<u>Auftragskontrolle</u>

Es ist eine auftrags- und weisungsgemäße Auftragsdatenverarbeitung zu gewährleisten.

Vom Auftragnehmer umgesetzte Maßnahmen:

- Klare Vertragsgestaltung und -ausführung
- Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber
- Sorgfältige Auswahl des Auftragnehmers
- Sanktionen bei Vertragsverletzung