Vertrag über die Auftragsverarbeitung gemäß Art. 28 DS-GVO

- **4.B.DVZU2026010_F-**

zwischen der

.....

Universität Potsdam

vertreten durch den Präsidenten,Herrn Prof. Oliver Günther, Ph. D.,

dieser vertreten durch den Kanzler, Herrn Hendrik Woithe,

Am Neuen Palais 10,

14469 Potsdam

- Verantwortlicher - nachstehend Auftraggeber genannt –

und dem/der

.....

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

.....]

§ 1 Einleitung, Geltungsbereich, Definitionen

(1) Dieser Vertrag regelt die Rechte und Pflichten von Auftraggeber und -nehmer (im Folgenden „Parteien“ genannt) im Rahmen einer Verarbeitung von personenbezogenen Daten im Auftrag.

(2) Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen Mitarbeiter des Auftragnehmers oder durch ihn beauftragte Unterauftragnehmer personenbezogene Daten des Auftraggebers verarbeiten.

(3) In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der EU Datenschutz-Grundverordnung (DS-GVO) zu verstehen. Soweit Erklärungen im Folgenden „schriftlich“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint.

§ 2 Gegenstand und Dauer des Auftrags

(1) Gegenstand

☒ Der Gegenstand des Auftrags ergibt sich aus dem EVB-IT Dienstvertrag mit der Vertragsnummer 4.B.DVZI2026010_F auf den hier verwiesen wird (im Folgenden Hauptvertrag).

oder

☐ Gegenstand des Auftrags zur Datenverarbeitung ist die Durchführung folgender Aufgaben durch den Auftragnehmer:
……

(2) Dauer

☒ Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrags.

oder

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

oder

☐ Die Dauer dieses Auftrags (Laufzeit) ist befristet bis zum .....

oder

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

§ 3 Konkretisierung des Auftragsinhalts

(1) Art und Zweck der vorgesehenen Verarbeitung von Daten

☒ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind:

Im Rahmen der Tätigkeit als Support- Weiterentwicklungs- und Pflege-Dienstleister für das TYPO3-System werden personenbezogene Daten ausschließlich zur Erfüllung der vertraglich vereinbarten Aufgaben verarbeitet.

Dies umfasst insbesondere:

- Entgegennahme und Bearbeitung von Supportanfragen, inklusive E-Mail-, Telefon- oder Ticketsystem-Kommunikation;

- Analyse und Behebung von technischen Problemen, die personenbezogene Daten betreffen können

- Einrichtung, Verwaltung oder Anpassung von Benutzerkonten innerhalb des Systems;

- Dokumentation von Supportfällen und technischen Maßnahmen zur Qualitätssicherung;
- Temporäre Einsicht in personenbezogene Daten, soweit dies zur Lösung des Supportfalls erforderlich ist.

oder

☐ Nähere Beschreibung des Auftragsgegenstands im Hinblick auf Art und Zweck der Verarbeitung durch den Auftragnehmer

(2) Art der Daten

☒ Gegenstand der Verarbeitung personenbezogener Daten und sind folgende Datenarten/-kategorien (Aufzählung/Beschreibung der Datenkategorien)

☒ Namen,

☒ Dienstadressen,

☒ Email- Adressen,

☒ Telefonnummern

☒ alle mithilfe von Powermail-Formularen erfassten Daten (z.B. Angaben zur beruflichen Tätigkeit und zum Arbeitgeber)

☐ ggf. Immatrikulationsdaten,

☐ Daten von Vertragspartnern,

☐ Vertragsabrechnungs- Zahlungsdaten,

☐ Planungs- und Steuerungsdaten

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

(3) Kategorien betroffener Personen

☐ Die Kategorien der durch die Verarbeitung betroffenen Personen sind im Hauptvertrag konkret beschrieben unter: .....

oder

☒ Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

☒ Studierende
☒ Lehrbeauftragte
☒ Promovierende
☒ Prüfungskandidatinnen und Prüfungskandidaten
☒ Externe/weitere Nutzende von Hochschuleinrichtungen
☒ Beschäftigte
☒ Teilnehmerinnen und Teilnehmer einer Studie

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

(2) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

(3) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren. Diese Pflicht besteht auch nach Beendigung des Vertrags fort.

(4) Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen. Diese Verpflichtung gilt sowohl für die Zeit einer Tätigkeit beim Auftragnehmer als auch für die Zeit nach Beendigung des Beschäftigungsverhältnisses.

(5) Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

(6) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten:

a. Der Auftragnehmer gewährleistet die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, welche die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

b. Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind vorzuhalten und dem Auftraggeber auf Anforderung unverzüglich zuzuleiten.

c. Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

d. Wird der Auftragnehmer durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen, informiert der Auftragnehmer den Auftraggeber unverzüglich. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

(7) Der Auftragnehmer unterstützt den Auftraggeber – nach Möglichkeit mit geeigneten technisch-organisatorischen Maßnahmen – bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Art. 12 ff. DS-GVO genannten Rechte von betroffenen Personen. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

(8) Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der

Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde (Anlage 4). Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(9) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

(10) 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 Art. 44 ff. DS-GVO erfüllt sind.

§ 5 Technisch-organisatorische Maßnahmen

(1) Die in der Anlage 1 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt. Sie definieren das vom Auftragnehmer geschuldete Minimum. Die Beschreibung der Maßnahmen muss so detailliert erfolgen, dass für einen sachkundigen Dritten allein aufgrund der Beschreibung jederzeit zweifelsfrei erkennbar ist, was das geschuldete Minimum sein soll. Ein Verweis auf Informationen, die dieser Vereinbarung oder ihren Anlagen nicht unmittelbar entnommen werden können, ist nicht zulässig.

(2) Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

(3) Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

(4) Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

(5) Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

(6) Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

§ 6 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit und auch über die Beendigung dieses Vertrags hinaus Folge leisten.

§ 7 Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, wie z.B. Telekommunikationsleistungen, Post-/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 ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

a. ☐ Der Auftraggeber stimmt der Beauftragung der in Anlage 2 genannten Unterauftragnehmer zu soweit:
   - eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird,
   - dem Unterauftragnehmer darin vertraglich mindestens Datenschutzpflichten auferlegt werden, die den in diesem Vertrag vereinbarten vergleichbar sind,
   - der Auftraggeber auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Unterauftragnehmer erhält,
   - die Rechte des Auftraggebers auch gegenüber dem Unterauftragnehmer wirksam ausgeübt werden können, wobei der Auftraggeber insbesondere berechtigt sein muss, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Unterauftragnehmern durchzuführen oder durch Dritte durchführen zu lassen,
   - die Verantwortlichkeiten des Auftragnehmers und des Unterauftragnehmers eindeutig voneinander abgrenzbar sind,
   - der Auftragnehmer den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der vom Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig auswählt,
   - der Auftragnehmer die Einhaltung der Pflichten des Unterauftragnehmers regelmäßig, spätestens alle 12 Monate, angemessen überprüft. Die Prüfung und ihr Ergebnis sind so aussagekräftig zu dokumentieren, dass sie für einen fachkundigen Dritten nachvollziehbar sind. Die Dokumentation ist dem Auftraggeber unaufgefordert vorzulegen.

b. ☐ Die Beauftragung von Unterauftragnehmern
und/oder
☐ der Wechsel bestehender Unterauftragnehmer
sind zulässig, soweit:
- der Auftraggeber schriftlich zustimmt und
- die weiteren Voraussetzungen aus § 7 Abs. 2 lit. a erfüllt sind.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☒ ist nicht gestattet;
☐ bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);
☐ bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

(6) Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

§ 8 Rechte und Pflichten des Auftraggebers

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

(2) Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

(3) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

(4) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

(5) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach dieser Vereinbarung und Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(6) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch ……

- ☐ die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- ☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- ☐ aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- ☐ eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

§ 9 Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Auch begründete Verdachtsfälle hierauf sind mitzuteilen. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine weisungsberechtigte Person des Auftraggebers (Anlage 3) zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

a. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
b. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
c. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
d. eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragserledigung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

§ 10 Weisungsbefugnis des Auftraggebers

(1) Die Auftraggeberin behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in der Anlage 3.

(3) Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

(4) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der

entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

(5) Der Auftragnehmer hat ihm erteilte Weisungen und deren Umsetzung zu dokumentieren.

§ 11 Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers 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.

(2) Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl dem Auftraggeber entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist. Eine physische Vernichtung erfolgt gemäß DIN 66399.

(3) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. datenschutzgerechte Löschung auch bei Unterauftragnehmern herbeizuführen.

(4) Der Auftragnehmer hat den Nachweis der ordnungsgemäßen Vernichtung zu führen und dem Auftraggeber unverzüglich vorzulegen.

(5) Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

§ 12 Vergütung

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

§ 13 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Der Auftragnehmer trägt die Beweislast dafür, dass ein Schaden nicht Folge eines von ihm zu vertretenden Umstandes ist, soweit die relevanten Daten von ihm unter dieser Vereinbarung verarbeitet wurden. Solange dieser Beweis nicht erbracht wurde, stellt der Auftragnehmer den Auftraggeber auf erste Anforderung von allen Ansprüchen frei, die im Zusammenhang mit der Auftragsverarbeitung gegen den Auftraggeber erhoben werden. Unter diesen Voraussetzungen ersetzt der Auftragnehmer dem Auftraggeber ebenfalls sämtliche entstandenen Kosten der Rechtsverteidigung.

(3) Der Auftragnehmer haftet dem Auftraggeber für Schäden, die der Auftragnehmer, seine Mitarbeiter bzw. die von ihm mit der Vertragsdurchführung Beauftragten oder die von ihm eingesetzten Subdienstleister im Zusammenhang mit der Erbringung der beauftragten vertraglichen Leistung schuldhaft verursachen.

(4) Die Absätze (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

§ 14 Vertragsstrafe

(1) Verstößt der Auftragnehmer schuldhaft und nicht unerheblich gegen die Bestimmungen dieses Vertrags, ist der Auftraggeber berechtigt, eine nach seinem billigen Ermessen bestimmte und im Streitfalle durch das zuständige Amts- oder Landgericht überprüfbare Vertragsstrafe je Einzelfall zu fordern („neuer Hamburger Brauch“). Die Vertragsstrafe wird insbesondere bei Mängeln in der Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen verwirkt. Bei dauerhaften Verstößen gilt jeder Kalendermonat, in dem der Verstoß ganz oder teilweise vorliegt, als Einzelfall. Die Einrede des Fortsetzungszusammenhangs für vorsätzlich begangene Verstöße ist ausgeschlossen.

(2) Die Geltendmachung eines darüber hinaus gehenden Anspruchs auf Schadenersatz bleibt dem Auftraggeber vorbehalten. Die Höhe der verwirkten Vertragsstrafe wird auf einen Schadenersatzanspruch angerecht, soweit zwischen diesen Ansprüchen eine Interessenidentität besteht.

§ 15 Sonderkündigungsrecht

(1) Der Auftraggeber kann den Hauptvertrag und diese Vereinbarung jederzeit ohne Einhaltung einer Frist kündigen („außerordentliche Kündigung“), wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieser Vereinbarung vorliegt, der Auftragnehmer eine rechtmäßige Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert.

(2) Ein schwerwiegender Verstoß liegt insbesondere vor, wenn der Auftragnehmer die in dieser Vereinbarung bestimmten Pflichten, insbesondere die vereinbarten technischen und organisatorischen Maßnahmen in erheblichem Maße nicht erfüllt oder nicht erfüllt hat.

(3) Bei unerheblichen Verstößen setzt der Auftraggeber dem Auftragnehmer eine angemessene Frist zur Abhilfe. Erfolgt die Abhilfe nicht rechtzeitig, so ist der Auftraggeber zur außerordentlichen Kündigung, wie in diesem Abschnitt beschrieben, berechtigt.

(4) Der Auftragnehmer hat dem Auftraggeber alle Kosten zu erstatten, die diesem durch die verfrühte Beendigung des Hauptvertrags oder dieses Vertrags in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

§ 16 Sonstiges

(1) Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

(2) Sollte Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

(3) Für Nebenabreden ist die Schriftform erforderlich.

(4) Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der im Auftrag verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

(5) Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Ort, Datum	Ort, Datum
Für den Auftraggeber …	Für den Auftragnehmer …

Anlage 1 – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit gem. Art. 32 Abs. 1 lit. b DSGVO

1.1. Zutrittskontrolle[1]

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Alarmanlage	☐ Zutritt für Besucher/innen und externe Dienstleister zu den Serverräumen ist nur in Begleitung eines/r berechtigten Mitarbeiters/in
☐ Chipkarten / Transpondersysteme	☐ der Zutritt zu Räumen mit Servern ist ausschließlich mit personalisierten Transpondern oder Sicherheitsschlüsseln möglich, welche nur für berechtige Mitarbeiter/innen freigeschaltet oder ausgegeben werden
☐ Manuelles Schließsystem	☐ für die ausgegebenen Schlüssel wird ein Schlüsselverzeichnis über Ausgabe, Rücknahme und Verlust von Schlüsseln geführt.
☐ Sicherheitsschlösser	☐ Reinigungspersonal hat keinen Zugang zu den Serverräumen
☐ Schließsystem mit Codesperre	☐ Arbeitsräume mit Arbeitsplatzrechnern die Zugriff auf die Server-Infrastruktur haben, müssen beim Verlassen verschlossen werden.
☐ Absicherung der Gebäudeschächte	☐ Pförtner
☐ Türen mit Knauf Außenseite	☐ Wachdienst
☐ Videoüberwachung	

Weitere Maßnahmen:

1.2. Zugangskontrolle[2]

Technische Maßnahmen	Organisatorische Maßnahmen
☐ IT-Systeme werden nach Anwendungszweck in verschiedenen Netzwerksegmenten betrieben	☐ Passwörter für den Zugang zur virtuellen Maschine liegen beim Ansprechpartner, der bei der Einrichtung einer solchen Maschine benannt werden muss
☐ Login mit Benutzername + Passwort	☐ Externe Dienstleister erhalten Zugriff auf interne IT-Systeme zum Zweck der Wartung von Infrastrukturkomponenten nur nach vorheriger Freischaltung durch den IT-Support. Der Zugriff erfolgt unter Beobachtung bzw. Anwesenheit eines/r Mitarbeiters/in des Supports oder der Technik.
☐ Anti-Viren-Software Server	☐ Das gesamte Netzwerk und die

[1] Maßnahmen der **Zutrittskontrolle** dienen dazu, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.
[2] Durch die Zugangskontrolle soll verhindert werden, dass Datenverarbeitungssysteme/Datenträger von Unbefugten genutzt/gelesen werden können.

	Netzwerksegmente werden durch den Einsatz von Firewalls voneinander getrennt, Zugang zu den jeweiligen Netzwerksegmenten erhalten nur die jeweils zugangsberechtigten Personenkreise.
☐ Anti-Virus-Software Clients	☐ Fernzugriffe während der Arbeit im Home-Office oder auf Dienstreisen erfolgen über einen gesicherten VPN-Tunnel mit personalisiertem Nutzerzertifikat und Passwort.
☐ Anti-Virus-Software mobile Geräte	☐ Alle Mitarbeiter/innen sind zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutzgrundverordnung (DSGVO) - Datengeheimnis/Vertraulichkeit (Art. 5, 24, 32 DSGVO) - verpflichtet.
☐ Firewall	☐ Spätestens nach dem Austritt von Mitarbeiter/innen erfolgt der Entzug von Zugriffsrechten für IT-Systeme, insbesondere für IT-Systeme, die aus dem Internet zu erreichen sind.
☐ Intrusion Detection Systeme	☐ Mitarbeiter/innen erhalten Zugriffsberechtigungen gemäß ihrem Aufgabenbereich. Eine Erweiterung der Zugangsberechtigung muss durch Vorgesetzte über das interne Ticketsystem beantragt werden, um eine entsprechende Protokollierung sicherzustellen.
☐ Einsatz VPN bei Remote-Zugriffen	☐ Richtlinie „Sicheres Passwort“
☐ Verschlüsselung von Datenträgern	
☐ Gehäuseverriegelung	
☐ BIOS Schutz	
☐ Sperre externe Schnittstellen (USB)	
☐ Verschlüsselung von Notebooks / Tablets	
☐ Die Eingabe von Passwörtern erfolgt immer über eine verschlüsselte Verbindung	
☐ Netzwerkverbindungen zu Außenstellen dürfen nur über verschlüsselte Verbindungen hergestellt werden, die in den jeweiligen Gebäuden beginnen bzw. enden	
☐ Authentifizierung / Login mit biometrischen Merkmalen (z.B. Fingerabdruck /Iris-Scan/Face-ID)	

Weitere Maßnahmen:

1.3. Zugriffskontrolle[3]

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Verwendung von Aktenschreddern entsprechend der erforderlichen Sicherheitsstufe nach DIN 66399.	☐ Einsatz von Berechtigungskonzepten
☐ Externer Aktenvernichter (DIN 32757)	☐ Minimale Anzahl von Administrator/innen
☐ Physische Löschung von Datenträgern	☐ Verwaltung der Benutzerrechte durch Administrator/innen
☐ Protokollierung von Zugriffen aus Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☐ Mitarbeiter/innen erhalten Zugriffsberechtigungen gemäß ihrem Aufgabenbereich.
☐ mittels Virtualisierung wird ein direkter Zugriff durch die Anwender auf die Hardware-Ebene verhindert	

Weitere Maßnahmen:

1.4. Trennungskontrolle[4]

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Trennung von Produktiv- und Testumgebung	☐ Steuerung über Berechtigungskonzept
☐ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☐ Festlegung von Datenbankrechten
☐ getrennte virtuelle Systeme mit einer eigenständigen Datenbank für jeden Datenbestand	☐ Datensätze sind mit Zweckattributen versehen
☐ getrennte Datenbanken auf einem System mit getrennten Zugriffsrechten	

Weitere Maßnahmen:

1.5. Pseudonymisierung[5]

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Trennung der Zuordnungsdaten (Klarnamenliste) von den restlichen Daten	☐ Beschränkung des Zugriffs auf die Klarnamenliste auf folgende Personen[6]:

[3] Mit Maßnahmen der Zugriffskontrolle soll sichergestellt werden, dass jede/r Mitarbeiter/in im Rahmen seiner/ihrer Tätigkeit nur auf solche Daten zugreifen kann, die er/sie zur Erfüllung seiner Aufgaben tatsächlich benötigt (Need-to-know-Prinzip).

[4] Maßnahmen der Trennungskontrolle sollen sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden (keine gleichzeitige Arbeit an Daten aus unterschiedlichen Beständen).

[5] Die Pseudonymisierung ist eine Maßnahme der Erhöhung der Sicherheit der Datenverarbeitung. Sie erfolgt indem die Klarnamen in Datensätzen durch einen Code/eine Kennung ersetzt werden. Eine Klarnamenliste, mit der eine Zuordnung der Daten zu bestimmten Personen möglich bleibt, wird erstellt und sicher mit beschränkten Zugriffsmöglichkeiten verwahrt.

[6] Angabe von Funktionsbezeichnungen sind ausreichend.

und Aufbewahrung in getrennten und abgesicherten Systemen	
☐ Verschlüsselung / Passwortschutz der elektronisch aufbewahrten Klarnamenliste	☐ Aufbewahrung der Klarnamenliste in Papierform in einem Stahlschrank/Safe
	☐ Interne Anweisung, personenbezogenen Daten im Falle einer Weitergabe oder nach Ablauf der gesetzlichen Löschfrist zu anonymisieren

Weitere Maßnahmen:

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

2.1. Weitergabekontrolle[7]

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Einsatz von VPN	☐ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☐ Protokollierung der Zugriffe und Abrufe	☐ Weitergabe in anonymisierter oder pseudonymisierter Form
☐ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☐ Verwendung verschlossener Transportbehälter
☐ Nutzung von Signaturverfahren	☐ Persönliche Übergabe mit Protokoll
☐ Passwortschutz/Verschlüsselung einzelner Dokumente mit getrennter Kennwortübermittlung	
☐ Verschlüsselung von zum Transport eingesetzten Datenträgern	

Weitere Maßnahmen:

2.2. Eingabekontrolle[8]

Technische Maßnahmen	**Organisatorische Maßnahmen**
☐ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Übersicht mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☐ Manuelle oder automatisierte Kontrolle der Protokolle	☐ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
☐ Protokollierung von Administratoraktivitäten	☐ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

[7] Die Weitergabekontrolle soll die Integrität und Vertraulichkeit der Daten im Zusammenhang mit ihrer Weitergabe gewährleisten.

[8] Mit Maßnahmen der Eingabekontrolle soll die Integrität der Daten sichergestellt werden. Dazu muss nachträglich überprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

☐ Erfassung gescheiterter Zugriffsversuche	☐ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
	☐ Klare Zuständigkeiten für Löschungen

Weitere Maßnahmen:

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle[9]

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Feuer- und Rauchmeldeanlagen	☐ Backup & Recovery Konzept
☐ Feuerlöscher Serverraum	☐ Kontrolle des Sicherungsvorgangs
☐ Serverraumüberwachung Temperatur und Feuchtigkeit	☐ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☐ Serverraum klimatisiert	☐ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☐ Unterbrechungsfreie Stromversorgung	☐ Existenz eines Notfallplans
☐ Schutzsteckdosen Serverraum	☐ Getrennte Partitionen für Betriebssysteme und Daten
☐ RAID System / Festplattenspiegelung	
☐ Alarmmeldung bei unberechtigten Zutritt zu Serverraum	

Weitere Maßnahmen:

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

4.1. Datenschutz-Management[10]

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeiten für Mitarbeiter/innen nach Bedarf / Berechtigung	☐ Datenschutzbeauftragte/r
	☐ Mitarbeiter/innen geschult und auf Vertraulichkeit / Datengeheimnis verpflichtet
	☐ Regelmäßige Sensibilisierung der Mitarbeiter/innen

[9] Maßnahmen der Verfügbarkeitskontrolle dienen dem Schutz der Daten vor Verlust und Zerstörung sowie vorübergehenden Verfügbarkeitsbeschränkungen.

[10] Das Datenschutz-Management ist eine Methode, um die gesetzlichen und innerorganisatorischen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren.

	Der Verantwortliche kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach
	☐ Formalisierter Prozess zur Bearbeitung von Auskunftsfragen seitens Betroffener ist vorhanden

Weitere Maßnahmen:

4.2. Incident Response Management[11]

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Einsatz von Firewall und regelmäßige Aktualisierung	☐ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen
☐ Einsatz von Spamfilter und regelmäßige Aktualisierung	☐ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☐ Einsatz von Virenscanner und regelmäßige Aktualisierung	☐ Einbindung von ☐ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen
☐ Intrusion Detection System (IDS)	☐ Dokumentation von Sicherheitsvorfällen und Datenpannen im Ticketsystem
☐ Intrusion Prevention System (IPS)	☐ Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen

Weitere Maßnahmen:

4.3. Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen	Organisatorische Maßnahmen
☐ Anwendungen / Apps sind so eingestellt, dass nicht mehr personenbezogene Daten erhoben werden, als für den jeweiligen Zweck erforderlich sind	
☐ Einfache Ausübung des Widerrufsrechts des/r Betroffenen durch technische Maßnahmen	

Weitere Maßnahmen:

4.4. Auftragskontrolle[12]

Technische Maßnahmen	Organisatorische Maßnahmen
	☐ Vorherige Prüfung der von Auftragnehmer

[11] Das Incident Response Management umfasst den gesamten organisatorischen und technischen Prozess der Reaktion auf erkannte oder vermutete Sicherheitsvorfälle bzw. Betriebsstörungen in IT-Bereichen sowie entsprechende vorbereitende Maßnahmen und Prozesse.

[12] Mit Maßnahmen der Auftragskontrolle soll gewährleistet werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

	getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☐ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	☐ Abschluss der notwendigen Vereinbarungen zur Auftragsdatenverarbeitung
	☐ Schriftliche Weisungen an den Auftragnehmer
	☐ Verpflichtung der Mitarbeiter/innen des Auftragnehmers auf Datengeheimnis

Anlage 2 – Zugelassene Unterauftragnehmer

Unterauftragnehmer	Anschrift/Land	Leistung

Anlage 3 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Weisungsberechtigte Personen der Auftraggeberin sind:

_____

(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

_____

(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

_____

(genaue postalische Adresse / E-Mail / Telefonnummer)

Anlage 4 – Datenschutzbeauftragter

Derzeit ist als interner / externer Datenschutzbeauftragter beim Auftragnehmer bestellt:

Kontaktdaten

Bei internen Beauftragten: sonstige Aufgaben im Unternehmen

Oder

Beim Auftragnehmer wurde kein Datenschutzbeauftragter bestellt, weil…