### Vertrag über die Verarbeitung personenbezogener Daten im Auftrag

**zwischen**

Einrichtung/Fakultät/Fachgebiet

TU Berlin

Straße des 17. Juni 135

10623 Berlin

nachfolgend „**Auftraggeber**“ genannt

**und**

nachfolgend „**Auftragnehmer**“ genannt

**Präambel**

(1) Gemäß

[Vertragstitel, Vertragsgegenstand, Vertragsdatum, Vertragspartner]

beabsichtigt der Auftraggeber, den Auftragnehmer mit der Durchführung von

[Beschreibung der Sach-, Dienst- oder Finanzleistung gemäß o. g. Vertrag]

zu beauftragen.

(2) In diesem Zusammenhang wird der Auftragnehmer mit personenbezogenen Daten des Auftraggebers in Berührung kommen. Mit diesem Vertrag werden die datenschutzrechtlichen Verpflichtungen der Vertragsparteien, die sich aus der Erbringung von dem in dem vorgenannten Vertrag geregelten Leistungsumfang durch den Auftragnehmer ergeben, festgehalten. Dieser Vertrag findet dabei Anwendung auf alle Tätigkeiten, die mit dem Projekt in Zusammenhang stehen und bei denen Mitarbeiter des Auftragnehmers oder durch den Auftragnehmer beauftragte Dritte mit personenbezogenen Daten des Auftraggebers in Berührung kommen oder kommen können.

(3) Der Auftragnehmer ist verpflichtet, mit der gebotenen Sorgfalt darauf hinzuwirken, dass alle Personen, die von ihm mit der Bearbeitung oder Erfüllung von Aufträgen betraut sind, die gesetzlichen Bestimmungen über den Datenschutz beachten und die aus dem Bereich des Auftraggebers erlangten Informationen, und zwar personenbezogene und sonstige Daten, nicht an Dritte weitergeben oder sonst verwerten.

**§ 1 Definitionen:**

(1) Legaldefinition der EU Datenschutz-Grundverordnung (DSGVO)

In diesem Vertrag verwendete Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen.

(2) Prinzip der Schriftlichkeit

Soweit Erklärungen im Folgenden „schriftlich“ / in „Schriftform“ zu erfolgen haben, ist die Schriftform nach § 126 BGB gemeint. Im Übrigen können Erklärungen auch in anderer Form erfolgen, soweit eine angemessene Nachweisbarkeit gewährleistet ist.

(3) Weisung

Weisung ist die auf einen bestimmten datenschutzmäßigen Umgang (zum Beispiel Anonymisierung, Sperrung, Löschung, Herausgabe) des Auftragnehmers mit personenbezogenen Daten gerichtete schriftliche Anordnung des Auftraggebers. Die Weisungen werden im Rahmen des Projektes festgelegt und können vom Auftraggeber danach durch eine einzelne Weisung geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Weisungen des Auftraggebers sind schriftlich oder per E-Mail zu erteilen.

**§ 2 Gegenstand und Dauer des Auftrages**

(1) Der Auftragnehmer übernimmt dabei folgende Verarbeitungen:

[Beschreibung]

(2) Dieser Vertrag beruht auf dem zwischen den Parteien bestehenden Dienstleistungsvertrag

[Vertragstitel, Vertragsgegenstand, Vertragsdatum, Vertragspartner]

(3) Der Vertrag tritt mit seiner Unterzeichnung durch beide Parteien in Kraft und gilt unbefristet. Das Recht zur außerordentlichen Kündigung bleibt unberührt. Jede Kündigung bedarf der Schriftform.

**§ 3 Gegenstand, Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten und Kategorien der betroffenen Personen**

Umfang, Art und Zweck der Verarbeitung sind ebenso wie die Art der Daten und der Kreis der Betroffenen in **Anhang 1** beschrieben. Insbesondere ist der Auftragnehmer zur Erfüllung des Vertragsgegenstandes unter Einhaltung der Bestimmungen dieses Vertrages zur Durchführung aller erforderlichen Verarbeitungsschritte und Nutzungen der vom Auftraggeber überlassenen sowie der ggf. für ihn erhobenen Daten (z. B. Duplizieren von Beständen für die Verlustsicherung, Anlegen von Log-Files, Zwischendateien und Arbeitsbereichen etc.) berechtigt, soweit dies nicht zu einer inhaltlichen Umgestaltung führt.

**§ 4 Weisungsgebundenheit des Auftragnehmers**

(1) Der Auftragnehmer verarbeitet oder nutzt die vom Auftraggeber überlassenen Daten ausschließlich im Rahmen der Bestimmungen dieses Vertrages und der speziellen Einzelweisungen des Auftraggebers. Gleiches gilt für das Erheben von Daten im Auftrag des Auftraggebers. Mündliche Weisungen wird der Auftraggeber unverzüglich schriftlich oder per
E-Mail (in Textform) bestätigen.

(2) Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in **Anhang 2**.

(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.

(6) Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren.

**§ 5 Weitere Pflichten des Auftragnehmers**

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung und überwacht ihre Einhaltung.

(2) Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

(3) 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.

(4) 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.

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

(6) 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.

(7) Die Verarbeitung oder Nutzung der vom Auftraggeber überlassenen oder für den Auftraggeber erhobenen Daten zu anderen als den vertragsgegenständlichen Zwecken ist nicht gestattet. Insbesondere ist der Auftragnehmer nicht berechtigt, die Daten für eigene Zwecke zu verarbeiten und die Daten an Dritte weiterzugeben. Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

(8) 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.

(9) 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. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

(10) Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR. Jegliche Verlagerung in ein Drittland darf nur mit Zustimmung des Auftraggebers und unter den in Kapitel V der Datenschutz-Grundverordnung enthaltenen Bedingungen sowie bei Einhaltung der Bestimmungen dieses Vertrags erfolgen.

(11) Ist der Auftragnehmer nicht in der Europäischen Union niedergelassen, bestellt er einen verantwortlichen Ansprechpartner in der Europäischen Union gem. Art. 27 Datenschutz-Grundverordnung. Die Kontaktdaten des Ansprechpartners sowie sämtliche Änderungen in der Person des Ansprechpartners sind dem Auftraggeber unverzüglich mitzuteilen.

**§ 6 Technische und organisatorische Maßnahmen**

(1) Die im **Anhang 3** 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 diesem Vertrag oder seinen 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, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(6) Die Verarbeitung von Daten im Auftrag in Privatwohnungen oder mit Privatgeräten ist nicht gestattet.

(7) 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.

(8) Der Auftragnehmer führt den regelmäßigen Nachweis der Erfüllung seiner Pflichten, insbesondere der vollständigen Umsetzung der vereinbarten technischen und organisatorischen Maßnahmen sowie ihrer Wirksamkeit. Der Nachweis ist dem Auftraggeber spätestens alle 12 Monate unaufgefordert und sonst jederzeit auf Anforderung zu überlassen. Der Nachweis kann durch genehmigte Verhaltensregeln oder ein genehmigtes Zertifizierungsverfahren erbracht werden. Hierzu kann der Auftragnehmer auch aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz) vorlegen.

(9) Nähere Einzelheiten zu den vom Auftragnehmer getroffenen, technischen und organisatorischen Maßnahmen sind in **Anhang 3** zu diesem Vertrag beschrieben. Eine Risikoanalyse nach Art. 32 Absatz 2 DSGVO ist als **Anhang 4** beigefügt.

**§ 7 Mitteilungspflichten**

(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 vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

* 1. 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;
	2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
	3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
	4. 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.

(3) Soweit Prüfungen der Datenschutzaufsichtsbehörden (auch wegen des Verdachts auf Verstöße gegen datenschutzrechtliche Bußgeld- oder Strafvorschriften) durchgeführt werden, verpflichtet sich der Auftragnehmer, den Auftraggeber unverzüglich über die Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde zu informieren und das Ergebnis im Hinblick auf das Auftragsverhältnis dem Auftraggeber bekannt zu geben. Die im Prüfbericht feststellten Mängel wird der Auftragnehmer unverzüglich abstellen.

(4) Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 33 und 34 Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

(5) Der Auftraggeber benennt die im Rahmen des Notfallmanagements zu kontaktierenden Personen in **Anhang 2**.

**§ 8 Pflichten und Kontrollrechte 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 ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie sonstige Kontrollen vor Ort zu kontrollieren. Den mit der Kontrolle betrauten Personen ist vom Auftragnehmer soweit erforderlich Zutritt und Einblick zu ermöglichen. Der Auftragnehmer ist verpflichtet, erforderliche Auskünfte zu erteilen, Abläufe zu demonstrieren und Nachweise zu führen, die zur Durchführung einer Kontrolle erforderlich sind.

(5) Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Soweit der Auftragnehmer den Nachweis der korrekten Umsetzung der vereinbarten Datenschutzpflichten wie unter § 6 (8) dieses Vertrages vorgesehen erbringt, soll sich eine Kontrolle auf Stichproben beschränken.

(6) Die Namen und Kontaktdaten der anweisungs-, empfangs- und kontrollberechtigten Personen beim Auftraggeber werden in **Anhang 2** dokumentiert.

**§ 9 Datenschutzbeauftragter des Auftragnehmers**

(1) Die Kontaktdaten des betrieblichen Datenschutzbeauftragten des Auftragnehmers ergeben sich aus **Anhang 2**.

(2) Der Datenschutzbeauftragte hat auf Seiten des Auftragnehmers auf die Einhaltung der DSGVO im Hinblick auf das Auftragsverhältnis hinzuwirken. Stellt der Datenschutzbeauftragte in diesem Zusammenhang Unregelmäßigkeiten fest, gilt § 7 dieses Vertrages. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten des Auftragnehmers wenden.

**§ 10 Rechte Betroffener; Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten**

(1) Die Rechte der durch die Datenerhebung, -verarbeitung und -nutzung beim Auftragnehmer betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen. Er ist verantwortlich für die Wahrung dieser Rechte. Er ist dabei insbesondere für die Benachrichtigung der und die Auskunftserteilung an die Betroffenen (Art. 15 DSGVO) sowie die Berichtigung, Löschung und Einschränkung der Verarbeitung von Daten (Art. 16-18 DSGVO) verantwortlich. Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder in der Verarbeitung einschränken. Sollte sich ein Betroffener direkt an den Auftragnehmer wenden, so wird der Auftragnehmer die Anfrage unverzüglich an den Auftraggeber weiterleiten. Im Übrigen hat der Auftragnehmer den Auftraggeber bei der Wahrung der Rechte Betroffener, insbesondere im Hinblick auf die Benachrichtigung, Auskunftserteilung, Berichtigung, Einschränkung der Verarbeitung und Löschung, im Rahmen seiner Möglichkeiten zu unterstützen.

(2) Ist der Auftraggeber aufgrund der geltenden Datenschutzbestimmungen gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereit zu stellen.

**§ 11 Inanspruchnahme weiterer Auftragsverarbeiter (Subunternehmer)**

(1) Die Beauftragung von Subunternehmern ist nur mit schriftlicher Zustimmung des Auftraggebers im Einzelfall zugelassen.

(2) Die Zustimmung ist nur möglich, wenn dem Subunternehmer vertraglich mindestens Datenschutzpflichten auferlegt wurden, die den in diesem Vertrag vereinbarten vergleichbar sind. Der Auftraggeber erhält auf Verlangen Einsicht in die relevanten Verträge zwischen Auftragnehmer und Subunternehmer.

(3) Die Rechte des Auftraggebers müssen auch gegenüber dem Subunternehmer wirksam ausgeübt werden können. Insbesondere muss der Auftraggeber berechtigt sein, jederzeit in dem hier festgelegten Umfang Kontrollen auch bei Subunternehmern durchzuführen oder durch Dritte durchführen zu lassen.

(4) Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

(5) Eine weitere Subbeauftragung durch den Subunternehmer ist nicht zulässig.

(6) Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

(7) Die Weiterleitung von im Auftrag verarbeiteten Daten an den Subunternehmer ist erst zulässig, wenn sich der Auftragnehmer dokumentiert davon überzeugt hat, dass der Subunternehmer seine Verpflichtungen vollständig erfüllt hat. Der Auftragnehmer hat dem Auftraggeber die Dokumentation unaufgefordert vorzulegen.

(8) Die Beauftragung von Subunternehmern, die Verarbeitungen im Auftrag nicht ausschließlich aus dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in § 5 (10) und (11) dieses Vertrages genannten Bedingungen möglich. Sie ist insbesondere nur zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet. Der Auftragnehmer teilt dem Auftraggeber mit, welche konkreten Datenschutzgarantien der Subunternehmer bietet und wie ein Nachweis hierüber zu erlangen ist.

(9) Der Auftragnehmer hat die Einhaltung der Pflichten des Subunternehmers regelmäßig, spätestens alle 12 Monate, angemessen zu überprüfen. 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.

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

(11) Zurzeit sind die in **Anhang 5** mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt und durch den Auftraggeber genehmigt. Die hier niedergelegten sonstigen Pflichten des Auftragnehmers gegenüber Subunternehmern bleiben unberührt.

(12) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

**§ 12 Rückgabe und Löschung von Daten bei Vertragsbeendigung**

(1) Sämtliche im Zuge dieses Vertrages überlassenen Daten sind Eigentum des Auftraggebers. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten beim Auftraggeber liegt.

(2) Auch überlassene Datenträger sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen verbleiben im Eigentum des Auftraggebers. Der Auftragnehmer hat diese sorgfältig zu verwahren, so dass sie Dritten nicht zugänglich sind. Der Auftragnehmer ist verpflichtet, den Auftraggeber jederzeit unaufgefordert zu informieren, soweit seine Daten und Unterlagen von einem unberechtigten Zugriff durch Dritte betroffen sind. Der Auftragnehmer stellt eine datenschutzkonforme Vernichtung von Test- und Ausschussmaterial sicher. In besonderen, vom Auftraggeber zu bestimmenden Fällen erfolgt anstelle der Vernichtung eine Aufbewahrung bzw. Übergabe.

(3) Nach Beendigung des Auftrages oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die vom Auftraggeber überlassenen Daten sowie die für den Auftraggeber erhobenen, verarbeiteten und/oder genutzten Daten sowie etwaige Kopien davon dem Auftraggeber herauszugeben. Ist eine Herausgabe der Daten sowie etwaiger Kopien der Daten aus technischen Gründen nicht möglich, bspw. infolge elektronischer Speicherung auf fest installierten oder – soweit datenschutzrechtlich zulässig - gemeinsam genutzten Medien, sind die entsprechenden Daten vom Auftragnehmer in Abstimmung mit dem Auftraggeber datenschutzkonform zu löschen. Elektronisch gespeicherte Daten sind auf Wunsch des Auftraggebers entweder in einem marktüblichen Format auf elektronischen Datenträgern herauszugeben oder online zu übertragen.

(4) Der Auftragnehmer wird sämtliche Daten, von denen der Auftraggeber keine Herausgabe wünscht, löschen bzw. vernichten und die Löschung/Vernichtung dem Auftraggeber schriftlich oder per Email bestätigen. Dies gilt nicht für Schriftwechsel und für andere nach gesetzlichen Vorschriften aufzubewahrende Dokumente und Unterlagen oder zum Verbleib bei dem Auftragnehmer bestimmte Unterlagen. Weitergehende gesetzliche Löschungsverpflichtungen und Löschungsansprüche bleiben von vorstehenden Regelungen unberührt.

(5) Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

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

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

**§ 13 Vergütung**

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

**§ 14 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) Nummern (2) und (3) gelten nicht, soweit der Schaden durch die korrekte Umsetzung der beauftragten Dienstleistung oder einer vom Auftraggeber erteilten Weisung entstanden ist.

**§ 15 Vertragsstrafe**

Für jeden Fall der Zuwiderhandlung gegen diesen Vertrag durch den Auftragnehmer ist der Auftraggeber berechtigt, von dem Auftragnehmer die Zahlung einer von dem Auftraggeber in dessen billigem Ermessen festzusetzende Vertragsstrafe, die ggf. auf Antrag des Auftragnehmers durch gerichtliche Verfügung auf eine dem jeweiligen Verstoß angemessene Höhe zu vermindern ist, zu verlangen ohne dass dadurch das Recht des Auftraggebers beeinträchtigt wird, weitergehende Rechte geltend zu machen. Die Vertragsstrafe ist auf etwaige weitergehende Schadensersatzansprüche anzurechnen.

**§ 16 Außerordentliches Kündigungsrecht**

(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 Hauptvertrages oder dieses Vertrages in Folge einer außerordentlichen Kündigung durch den Aufraggeber entstehen.

(5) Der Auftraggeber ist ferner berechtigt, bei einem Verstoß gegen die Sicherheitsvorschriften den Austausch der betreffenden Personen auf Seiten des Auftragnehmers zu verlangen. Weitergehende Rechte des Auftraggebers bleiben hiervon unberührt.

**§ 17 Schlussbestimmungen**

(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.

(6) Fügt der Auftragnehmer dem Auftraggeber durch eine vertrags- oder weisungswidrige Verarbeitung oder Nutzung personenbezogener Daten des Auftraggebers einen Schaden zu, ist er dem Auftraggeber zum Schadensersatz nach Maßgabe der gesetzlichen Bestimmungen verpflichtet.

(7) Änderungen und Ergänzungen dieses Vertrages und aller seiner Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(8) Es gilt deutsches Recht.

|  |  |
| --- | --- |
|                           |                      |
| (Ort, Datum)  | (Auftragnehmer) |
|                           |                      |
| (Ort, Datum)  | (Auftraggeber) |

**ANHANG 1**

**Einzelheiten zur Verarbeitung personenbezogener Daten im Auftrag**

1. **Gegenstand des Auftrages**

*[Verweis auf Vertragstitel, Vertragsgegenstand, Vertragsdatum, Vertragspartner oder inhaltliche Wiedergabe, z. B. in Form einer Aufzählung; unbedingt auch angeben: Dauer des Auftrags wie oben in § 2]*

1. **Umfang, Art und Zweck der Verarbeitung**

Die Verarbeitung ist folgender Art: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung von Daten

Die Verarbeitung dient folgendem Zweck:

[*Beschreibung, gegebenenfalls* *Verweis auf Vertragstitel, Vertragsgegenstand, Vertragsdatum und Vertragspartner oder inhaltliche Wiedergabe des Vertragsinhaltes]*

1. **Art der Daten**

*Gegenstand der Erhebung, Verarbeitung und / oder Nutzung sind personenbezogene Daten gemäß Artikel 4 Nr. 1 DSGVO.*

*Die Verarbeitung personenbezogener Daten im Auftrag umfasst die folgenden Datenarten und -kategorien (Aufzählung / Beschreibung der Datenkategorien):*

|  |  |
| --- | --- |
| ☒ | Personenstammdaten (z. B. Name, Anschrift, Geburtsdatum, Familienstand, Berufsbezeichnung, Firmenzugehörigkeit) |
| ☐ | Sozialdaten (d.h. alle Daten, die bspw. durch Gesundheitsbehörden, Gesundheitseinrichtungen, Ärzte, Sozialleistungsträger sowie deren Verbände und Arbeitsgemeinschaften gem. § 35 SGB I verarbeitet werden) |
| ☐ | Besondere, personenbezogene Daten nach Art. 9 DSGVO, d. h.  |
|  | ☐ | Daten zur rassischen und ethnischen Herkunft |
|  | ☐ | Daten zu politischen Meinungen |
|  | ☐ | Daten zu religiösen oder weltanschaulichen Überzeugungen |
|  | ☐ | Daten zur Gewerkschaftszugehörigkeit |
|  | ☐ | Genetischen Daten |
|  | ☐ | Biometrischen Daten zur eindeutigen Identifikation einer natürlichen Person |
|  | ☐ | Gesundheitsdaten |
|  | ☐ | Daten zu Sexualleben oder sexueller Orientierung |
|  | der nachfolgend aufgeführten, betroffenen Personen |
| ☒ | Kommunikationsdaten (z.B. Telefon, E-Mail) |
| ☐ | Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse) |
| ☐ | Kundenhistorie |
| ☒ | Vertragsabrechnungs- und Zahlungsdaten |
| ☐ | Planungs- und Steuerungsdaten |
| ☐ | Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen) |
| ☒ | sonstige: Die Art der verwendeten Daten ist der Leistungsbeschreibung zu entnehmen. insbesondere handelt es sich um Personenstammdaten der Studienbewerber, Kommunikationsdaten sowie Daten zum Hochschulzugang, zum Studium, zur Promotion, An- und Abmeldung zu Prüfungen, Prüfungsergebnisse, Gebührendaten sowie Daten zur Beschreibungen der akademischen Strukturen, Räume und Termine. |

1. **Kategorien betroffener Personen**

|  |  |
| --- | --- |
| ☐ | Beschäftigte i. S. d. § 3 Abs. 11 BDSG |
| ☐ | Probanden, Praktikanten |
| ☐ | Mitarbeiter verbundener Unternehmen |
| ☐ | Bewerber |
| ☐ | Pensionäre / Hinterbliebene |
| ☐ | Kunden |
| ☐ | Abonnenten (z. B. Informationsschriften, Newsletter) |
| ☐ | Lieferanten |
| ☐ | Interessenten (z. B. Aktionäre, Werbungsempfänger) |
| ☐ | Dienstleister (z. B. externe Berater, externe Beauftragte) |
| ☐ | Prüfer (z. B. Sachverständige, Gutachter, externe Auditoren) |
| ☐ | Handelsvertreter |
| ☒ | sonstige: Studienbewerber, Studierende, Prüfende, Promovenden, Habilitanden, Lehrende, weitere Mitarbeiter und Mitarbeiterinnen der Hochschule |

**ANHANG 2**

1. **Berechtigte Personen**

Die nach § 6 Abs. (3) des Vertrages zur Weisung berechtigten Personen beim Auftraggeber sind:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Vorname** | **Titel/Funktion** | **Anschrift** | **Telefon** | **E-Mail** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. **Notfallmanagement**

Datenschutzrelevante Vorfälle gemäß § 5 Abs. (4) des Vertrages sind unmittelbar nach ihrer Feststellung und ohne schuldhafte Verzögerung vom Auftragnehmer an den Auftraggeber zu melden. Hierfür sind **auf Seiten des Auftraggebers** die folgenden Personen **innerhalb der üblichen Geschäftszeiten** zu informieren:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Vorname** | **Titel/Funktion** | **Anschrift** | **Telefon** | **E-Mail** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Außerhalb der üblichen Geschäftszeiten** sind **auf Seiten des Auftraggebers** die folgenden Personen zu informieren

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Vorname** | **Titel/Funktion** | **Anschrift** | **Telefon** | **E-Mail** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Als Ansprechpartner bezüglich des Datenschutzes auf **Seiten des Auftragnehmers** stehen die folgenden Personen zur Verfügung:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Vorname** | **Titel/Funktion** | **Anschrift** | **Telefon** | **E-Mail** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**ANHANG 3**

**Beschreibung der technischen und organisatorischen im Serverstandort des Auftragnehmers gemäß Artikel 32 DSGVO**

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragnehmer mindestens einzurichten und laufend aufrecht zu erhalten hat. Ziel ist die Gewährleistung insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit der im Auftrag verarbeiteten Informationen.

Die Maßnahmen müssen im Interesse beider Parteien so konkret wie möglich beschrieben werden! Sie sind Maßstab für Kontrollen durch den Auftraggeber und auch für die Frage entscheidend, ob möglicherweise ein Pflichtverstoß vorliegt. In dieser Anlage wird ganz maßgeblich festgelegt, was der Auftragnehmer zu leisten und nachzuweisen hat und was nicht. Unklare oder interpretationsfähige Umschreibungen sind dringend zu vermeiden!

Für die Vernichtung gem. DIN 66399 gilt Schutzklasse 1.

1. Organisation der Informationssicherheit
2. Personalsicherheit
3. Verwaltung der Werte
4. Zugangssteuerung
5. Kryptographie
6. Physische und umgebungsbezogene Sicherheit
7. Betriebssicherheit
8. Kommunikationssicherheit
9. Anschaffung, Entwicklung und Instandhaltung von Systemen
10. Lieferantenbeziehungen
11. Handhabung von Informationssicherheitsvorfällen
12. Informationssicherheitsaspekte beim Business Continuity Management
13. Compliance

**Bisher (BDSG) war dies ausreichend:**

1. **Vertraulichkeit**

Maßnahmen, die verhindern, dass Unbefugte personenbezogene Daten zur Kenntnis nehmen können.

* 1. **Zutrittskontrolle**

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

Folgende Maßnahmen sind beim Auftragnehmer umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Absicherung von Gebäudeschächten | ☒ | Protokollierung der Besucher |
| ☒ | Alarmanlage | ☒ | Schließsystem mit Codesperre |
| ☒ | Automatisches Zutrittskontrollsystem | ☒ | Schlüsselregelung (Schlüsselliste) |
| ☒ | Biometrische Zutrittskontrollen | ☒ | Sicherheitstüren und -schlösser |
| ☒ | Chipkarten-/Transponder-Schließsystem | ☒ | Sorgfältige Auswahl von Reinigungspersonal |
| ☒ | Einbruchmeldeanlage | ☒ | Sorgfältige Auswahl von Wachpersonal |
| ☒ | Einsatz von Wachpersonal | ☒ | Tragepflicht von Berechtigungsausweisen |
| ☒ | Lichtschranken / Bewegungsmelder | ☒ | Unterteilung in verschiedene Sicherheitszonen |
| ☒ | Manuelles Schließsystem | ☒ | Videoüberwachung der Zugänge |
| ☒ | Personenkontrolle beim Pförtner / Empfang | ☒ | Zutrittsberechtigungen funktions- und rollenbasiert |
| ☒ | sonstiges: Die markierten Maßnahmen kommen in Abhängigkeit zum Schutzbedarf im Rahmen des mehrstufigen Sicherheitszonenkonzeptes des Auftragnehmers zum Einsatz. Die Überwachung des Geländes/Gebäudes erfolgt außerhalb der Geschäftszeiten sowie an Wochenenden und Feiertagen durch einen externen Wachdienst.  |

* 1. **Zugangskontrolle**

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | 2-Faktor-Authentifizierung | ☒ | Passwortregelung (Mindestlänge, Komplexität, Gültigkeitsdauer, Sperrung/Löschung u.a.) |
| ☒ | Authentifikation mit Benutzername / Passwort | ☒ | Schlüsselregelung (Schlüsselausgabe etc.) |
| ☐ | ~~Authentifikation mit biometrischen Verfahren~~ | ☒ | Sichere Aufbewahrung von Datenträgern (Sicherungsbänder, Festplatten etc.) |
| ☒ | Einsatz eines Aktenvernichters | ☐ | ~~Sorgfältige Auswahl von Transportpersonal und -fahrzeugen~~ |
| ☒ | Einsatz von Anti-Viren-Software | ☒ | Vernichtung von Datenträgern durch dafür zertifizierte Entsorgungsfachbetriebe |
| ☒ | Einsatz einer Hardware-Firewall | ☒ | Vernichtung von Papierdokumenten durch dafür zertifizierte Entsorgungsfachbetriebe |
| ☐ | ~~Einsatz eines Identity Management Systems~~ | ☒ | Verschlüsselung auf Verzeichnis- und Dateiebene |
| ☒ | Einsatz einer Software-Firewall | ☒ | Verschlüsselung von Datenträgern in Laptops / Notebooks |
| ☒ | Einsatz verschließbarer Entsorgungsbehälter für Papier, Akten und Datenträger | ☐ | ~~Verschlüsselung von mobilen Datenträgern (USB-Sticks, CD/DVD etc.)~~ |
| ☒ | Einsatz von VPN-Technologie\* | ☒ | Verschlüsselung von Smartphone Inhalten |
| ☒ | Erstellen von Benutzerprofilen | ☐ | ~~Verwendung sicherer Transportbehälter /-verpackungen beim physischen Transport~~ |
| ☒ | Netzwerk- und Netzwerkzonenkonzept | ☒ | Zuordnung von Benutzerprofilen zu IT-Systemen |
| ☐ | ~~Notfallmanagement für Auftraggeber (u.a. Mehrschichtbetrieb, Rufbereitschaft, Stellvertreterregelung)~~ | ☒ | Zuweisung von Benutzerrechten erfolgt funktions- und rollenbasiert |
| ☒ | sonstiges: Die markierten Maßnahmen kommen in Abhängigkeit zum Schutzbedarf im Rahmen des mehrstufigen Sicherheitszonenkonzeptes des Auftragnehmers zum Einsatz. |

* 1. **Zugriffskontrolle**

Maßnahmen, die gewährleisten, 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.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Anzahl der Administratoren auf ein Minimum begrenzt | ☒ | Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten |
| ☒ | Funktions- und rollenbasiertes Berechtigungskonzept | ☒ | Verwaltung der Zugriffsberechtigungen unter Beachtung der Funktionstrennung und des 4-Augenprinzips |
| ☒ | Protokollierung der Vernichtung von Papier, Akten und Datenträgern |  |  |
| ☒ | sonstiges:  |

* 1. **Weitergabekontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes 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.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | ☒ | Verpflichtung der Mitarbeiter auf das Fernmeldegeheimnis gem. § 88 TKG |
| ☒ | E-Mail-Verschlüsselung | ☒ | Verpflichtung der Mitarbeiter auf das Sozialgeheimnis gem. § 35 SGB I |
| ☒ | Einrichtungen von Standleitungen bzw. VPN-Tunneln\* | ☒ | Verpflichtung der Mitarbeiter auf das Verbot des Verrats von Geschäfts- und Betriebsgeheimnissen gem. §§ 17 ff. UWG |
| ☒ | Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen\* | ☒ | Verpflichtung der Mitarbeiter auf Zweckbindung und Geheimhaltungspflicht gem. § 78 Abs. 1 SGB X |
| ☒ | Verpflichtung der Mitarbeiter auf das Datengeheimnis gem. § 5 BDSG | ☒ | Weitergabe von Daten in anonymisierter oder pseudonymisierter Form\* |
| ☒ | sonstiges: Die Weitergabe von Daten des Auftraggebers erfolgt nur in Abstimmung mit dem Auftraggeber an die vom ihm vorgegeben Empfänger. Alle Mitarbeiter des Auftragnehmers sind zur Wahrung der Verschwiegenheit sowie des Datengeheimnisses als Bestandteil ihres Arbeitsvertrages mit dem Auftragnehmer verpflichtet und über die rechtlichen Konsequenzen im Fall der Zuwiderhandlung schriftlich belehrt.  |

1. **Integrität**

Maßnahmen, die gewährleisten, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben.

* 1. **Eingabekontrolle**

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind | ☒ | Protokollierung der Eingabe, Änderung und Löschung von Daten |
| ☒ | Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. | ☒ | Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |
| ☒ | Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) |  |  |
| ☒ | sonstiges: Die Mitarbeiter des Auftragnehmers erstellen, ändern oder löschen von Daten bzw. Datensätze des Auftraggebers nur auf individuelle, schriftliche Weisung im Rahmen des Incident und Change Managements sinngemäß ISO/IEC 20000-1:2011. Dabei werden sowohl die Freigabe des Auftraggebers als auch die vorgenommenen Änderungen dokumentiert. Eine Übersicht der vorgenommenen Änderungen ist in den monatlichen Berichten an den Auftraggeber enthalten. |

* 1. **Verfügbarkeitskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind.

Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | ☐ | ~~Notfallhandbuch~~ |
| ☒ | Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort | ☐ | ~~Notfallkonzept (BCM)~~ |
| ☒ | Feuer- und Rauchmeldeanlagen | ☐ | ~~Notfallplan~~ |
| ☒ | Feuerlöschanlagen in Serverräumen | ☒ | Regelungen zur Verfügbarkeit und Zuverlässigkeit der vom Auftragnehmer erbachten Leistung\* |
| ☒ | Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | ☒ | Überspannungsschutzkonzept in Serverräumen |
| ☒ | Klimatisierte Serverräume | ☒ | Maßnahmen gegen Wassereinbruch in Serverräume |
| ☒ | Konzept zur Sicherung und Wiederherstellung von Daten (Backup, Restore, Recovery) durch den Auftragnehmer\* | ☒ | Testen von Datenwiederherstellung\* |
| ☒ | Konzept zur Archivierung von Daten durch den Auftragnehmer\* | ☒ | Unterbrechungsfreie Stromversorgung (USV) |
| ☒ | sonstiges: Einzelheiten zu der zwischen Auftraggeber und Auftragnehmer vereinbarten Verfügbarkeit sowie den Backup-, Restore- und Recovery-Maßnahmen sind im zugrundeliegenden Dienstleistungsvertrag beschrieben. Dies gilt auch für die begleitenden, mit \* gekennzeichneten Maßnahmen. |

* 1. **Auftragskontrolle**

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Folgende Maßnahmen werden zusätzlich zu den vorgenannten Kontrollen vom Auftraggeber und vom Auftragnehmer umgesetzt:

|  |  |
| --- | --- |
| *Maßnahmen, die die Auftragsdatenverarbeitung durch den Auftragnehmer regulieren:*: | *Maßnahmen, die eine mögliche Auftragsdatenverarbeitung durch Unterauftragnehmer des Auftragnehmers regulieren:* |
| ☐ | Auswahl des Auftragnehmers durch den Auftraggeber unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | ☐ | ~~Auswahl des Unterauftragnehmers durch den Auftragnehmer unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)~~ |
| ☐ | Prüfung des Auftraggebers auf Bestellung eines Datenschutzbeauftragten beim Auftragnehmer | ☐ | ~~Prüfung des Auftragnehmers auf Bestellung eines Datenschutzbeauftragten beim Unterauftragnehmer~~ |
| ☐ | Prüfung der Dokumentation und der beim Auftragnehmer getroffenen Sicherheits­maßnahmen durch den Auftraggeber vor Beginn der Datenverarbeitung | ☐ | ~~Prüfung der Dokumentation und der beim Unterauftragnehmer getroffenen Sicherheits­maßnahmen durch den Auftragnehmer vor Beginn der Datenverarbeitung~~ |
| ☐ | Schriftliche Weisungen des Auftraggebers an den Auftragnehmer nach § 11 Abs. 2 BDSG (z.B. durch Vertrag der Datenverarbeitung im Auftrag) | ☐ | ~~Schriftliche Weisungen des Auftragnehmers an den Unterauftragnehmer nach § 11 Abs. 2 BDSG (z.B. durch Vertrag der Datenverarbeitung im Auftrag)~~ |
| ☐ | ~~Vertragsstrafen bei Verstößen mit dem Auftragnehmer vereinbart~~ | ☐ | ~~Vertragsstrafen bei Verstößen mit dem Unterauftragnehmer vereinbart~~ |
| ☐ | Wirksame Kontrollrechte des Auftraggebers gegenüber dem Auftragnehmer vereinbart | ☐ | ~~Wirksame Kontrollrechte des Auftragnehmers gegenüber dem Unterauftragnehmer vereinbart~~ |
| ☐ | Sicherstellung der Vernichtung von Daten durch Auftraggeber und Auftragnehmer nach Beendigung des Auftrags | ☐ | Sicherstellung der Vernichtung von Daten durch Auftragnehmer und Unterauftragnehmer nach Beendigung des Auftrags gemäß schriftlicher Weisung des Auftraggebers |
| ☒ | Vertrag zwischen Auftraggeber und Auftragnehmer zum Einsatz von Unterauftragnehmern beim Auftragnehmer |
| ☒ | sonstiges: Weitere Maßnahmen zur Auftragskontrolle siehe Eingabekontrolle. Soweit zwischen Auftraggeber und Auftragnehmer vertraglich nicht anders vereinbart, bedarf der Einsatz von Unterauftragnehmern zur Ausführung der vom Auftraggeber an den Auftragnehmer übergebenen Arbeiten, der schriftlichen Zustimmung des Auftraggebers. Es wird auf den diesem Vertrag zugrundeliegenden Dienstleistungsvertrag zwischen Auftraggeber und Auftragnehmer verwiesen. |

1. **Verfügbarkeit**

Maßnahmen, die gewährleisten, dass personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

Siehe 1) a) – c) und 2) b) – c).

1. **Authentizität**

Maßnahmen, die gewährleisten, dass personenbezogene Daten jederzeit ihrem Ursprung zugeordnet werden können.

* 1. **Trennungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Folgende Maßnahmen sind beim Auftragnehmer zusätzlich zu den vorgenannten Kontrollen umgesetzt:

|  |  |  |  |
| --- | --- | --- | --- |
| ☒ | Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System | ☒ | Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern |
| ☒ | Festlegung von Datenbankrechten | ☐ | ~~Versehen der Datensätze mit Zweckattributen/Datenfeldern~~\* |
| ☒ | Logische Mandantentrennung (software-seitig) | ☒ | Trennung von Produktiv- und Testsystem |
| ☒ | sonstiges: siehe 2) a) Eingabekontrolle. Die Trennungskontrolle obliegt der Maßgabe des Auftraggebers. Wurde mit dem Auftraggeber nicht anderes vereinbart, erfolgt die Datenverarbeitung logisch und physikalisch getrennt.  |

1. **Revisionsfähigkeit**

Maßnahmen, die gewährleisten, dass festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat.

Siehe 2) a) – c) und 4) a).

1. **Transparenz**

Maßnahmen, die gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können.

**ANHANG 4:**

**Risikoanalyse nach Art. 32 Absatz 2 DSGVO**

In der DSGVO aufgezählte Risiken:

* Vernichtung personenbezogener Daten
* Verlust personenbezogener Daten
* Veränderung personenbezogener Daten
* Unbefugte Offenlegung von personenbezogenen Daten
* Unbefugter Zugang zu personenbezogenen Daten

Der Schutzbedarf kann mit einer 3-Stufigen Skala bewertet werden.

|  |  |  |
| --- | --- | --- |
| **Schutzbedarf** | **Skalen-Wert** | **Beispiele** |
| normal | 1 | Daten für die Personalabrechnung wie z.B. VergütungsgruppeKFZ-ZulassungsdatenAdressdaten von Beschäftigten |
| hoch | 2 | SozialdatenGesundheitsdatenReligionszugehörigkeit |
| sehr hoch | 3 | Medizinische Daten lebenserhaltender SystemeIdentitätsdaten von verdeckten Ermittlern |

**Ergebnis der Risikobewertung (Beispiel)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Bedrohtes Objekt** | **Darstellung der Bedrohung** | **Bedrohtes Schutzziel** | **Schutzbedarf** | **Technisch / organisatorische Maßnahmen erforderlich?** |
| 1. Laptop mit gespeicherten Daten | Diebstahl | Vertraulichkeit, Verfügbarkeit | 2 | Ja |
| 2. Laptop mit gespeicherten Daten | Unberechtigter Zugriff z.B. bei Sitzungspausen | Vertraulichkeit, Integrität, Authentizität | 2 | Ja |
| 3. ... |  |  |  |  |