# Vertrag über die Auftragsverarbeitung gemäß Art. 28 DS-GVO

zwischen der

................................................................................................

Hochschule für Wirtschaft und Recht Berlin

Vertreten durch

Bandensche Str. 52

10825 Berlin

- 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 Hauptvertrag vom ..................., 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 konkret beschrieben im Hauptvertrag unter ………………

oder

[ ]  Nähere Beschreibung des Auftragsgegenstands im Hinblick auf Art und Zweck der Verarbeitung durch den Auftragnehmer: ........................................

Damit verbunden sind folgende Zugriffe:

[ ]  z.B. Einspielen von Softwarepatches, Releases, Versionen und Updates für das o.g. Produkt

[ ]  z.B. Datenbankupdates

[ ]  Lesende / [ ]  Schreibende Zugriffe auf

[ ]  Lesende / [ ]  Schreibende Zugriffe auf

[ ]  Lesende / [ ]  Schreibende Zugriffe auf

 (2) Art der Daten

[ ]  Die Art der verwendeten personenbezogenen Daten ist im Hauptvertrag konkret beschrieben unter: .......................

oder

[ ]  Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten und Datenkatgorien

[ ]  Personenstammdaten (Name, Vorname, Geburtsdatum, etc.)

[ ]  Kommunikationsdaten (Telefon, E-Mail)

[ ]  Immatrikulationsdaten (Beginn, Ende, Unterbrechungen)

[ ]  Daten von Vertragspartnern (Name, Firma, Telefon)

[ ]  Vertragsabrechnungs- und Zahlungsdaten (Kontonummer, BLZ)

[ ]  Planungs- und Steuerungsdaten

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

…

1. 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

[ ]  Promovierende

[ ]  Prüfungskandidatinnen und Prüfungskandidaten

[ ]  Externe Nutzerinnen und Nutzer von Hochschuleinrichtungen

[ ]  Beschäftigte

[ ]  Teilnehmerinnen und Teilnehmer einer Studie

[ ]  Lehrende und Lehrbeauftragte

...

## § 4 Pflichten des Auftragnehmers

1. Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder auf dokumentierte Weisung des Auftraggebers, 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 darf Auskünfte an Dritte oder Betroffene nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen. Ist der Auftragnehmer gerichtlich oder gesetzlich verpflichtet, Auskunft zu erteilen, so hat er den Auftraggeber hierüber unverzüglich zu informieren. Der Auftragnehmer darf Auskünfte an den Auftraggeber nur gegenüber den autorisierten Personen erteilen.
7. Ist der Auftragnehmer gesetzlich zur Bestellung einer/s Datenschutzbeauftragten verpflichtet, so ist dieser vor Beginn der Vertragsdurchführung zu bestellen. Der Auftragnehmer teilt der Auftraggeberin deren bzw. dessen Kontaktdaten mit. Entsprechendes gilt bei einem Wechsel in der Person der/s Datenschutzbeauftragten. Ist der Auftragnehmer gesetzlich nicht zur Bestellung einer/s Datenschutzbeauftragten verpflichtet, benennt sie eine Ansprechperson für Fragen des Datenschutzes und der Datensicherheit und teilt der Auftraggeberin deren bzw. dessen Kontaktdaten mit. Entsprechendes gilt bei einem Wechsel dieser Ansprechperson.
8. Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten:
	1. 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.
	2. 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.
	3. 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.
	4. 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.
9. 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.
10. 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.
11. 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. Das Ergebnis der Kontrollen ist zu dokumentieren und unaufgefordert im Abstand von max. 2 Jahren an die weisungsberechtigte Person zu senden. Dies gilt im Besonderen für:
* Entspricht die erbrachte Leistung aktuellen Vorgaben zu Privacy by design und Privacy by Default
* Entspricht die erbrachte Leistung aktuellen Vorgaben zur Datenminimierung
* Entspricht die erbrachte Leistung aktuellen Vorgaben zur Informationssicherheit, sodass personenbezogene Daten vor unbefugtem Zugriff, Manipulation und Zerstörung geschützt sind und Integrität, Vertraulichkeit und Verfügbarkeit vollständig gewährleistet sind.
* Entspricht die erbrachte Leistung aktuellen Vorgaben zur Transparenz.
* Entspricht die erbrachte Leistung aktuellen Vorgaben zur Geltendmachung der Betroffenenrechte.
* Entspricht die Datenschutzorganisation des Auftragnehmers den gesetzlichen Anforderungen.
1. 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.

Das angemessene Schutzniveau in ……………………….

[ ]  ist festgestellt durch einen Angemessenheitsbeschluss der Kommission (Art. 45 Abs. 3 DS-GVO);

[ ]  wird hergestellt durch verbindliche interne Datenschutzvorschriften (Art. 46 Abs. 2 lit. b i.V.m. Art. 47 DS-GVO);

[ ]  wird hergestellt durch Standarddatenschutzklauseln (Art. 46 Abs. 2 lit. c und d DS-GVO);

[ ]  wird hergestellt durch genehmigte Verhaltensregeln (Art. 46 Abs. 2 lit. e i.V.m. Art. 40 DS-GVO);

[ ]  wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. Art. 42 DS-GVO);

[ ]  wird hergestellt durch sonstige Maßnahmen: ……………………………. (Art. 46 Abs. 2 lit. a, Abs. 3 lit. a und b DS-GVO).

1. Für die Erfüllung der Pflichten aus diesem Vertrag gebührt der Auftragnehmerin keinerlei Entgelt oder Aufwandersatz.

## § 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. Die Verarbeitung von Daten in Privatwohnungen (Homeoffice und Telearbeit) ist ausgeschlossen. Die Verarbeitung von Daten mit Privatgeräten ist unter keinen Umständen 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.

## § 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. 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.
3. [ ]  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 prüft. 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.
4. [ ]  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.
1. Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
2. Eine weitere Auslagerung durch den Unterauftragnehmer

[ ]  ist nicht gestattet;

[ ]  bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

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

1. Kommt der Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.
2. Die Beauftragung eines Unterauftragnehmers außerhalb der EU/des EWR ist nicht gestattet.
3. Der Auftragnehmer überprüft die Einhaltung der Pflichten des Subunternehmers in regelmäßigem Abstand (mind. alle zwei Jahre). 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.

## § 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, 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 **alle** weisungsberechtigte Personen des Auftraggebers (Anlage 3) auf mind. zwei Kommunikationskanälen zu erfolgen. Die Meldung über das Ticketsystem oder an einen beliebigen Angestellten der HWR ist nicht ausreichend. Sie muss mindestens folgende Angaben enthalten:
2. 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;
3. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
4. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
5. 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
6. 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 des Auftraggebers 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.

## § 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 gemäß Art. 82 DSGVO.
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.

§ 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 Wartung, Support und Softwarepflege

1. Der Auftragnehmer teilt dem Auftraggeber bei (Fern-) Wartungstätigkeiten den Namen des entsprechenden Mitarbeiters mit. Sofern technisch möglich, wird diesem ein Fernwartungszugang durch die IT-Abteilung der HWR Berlin bereit gestellt. Erfolgt ein Wechsel des zuständigen Wartungsmitarbeiters, ist dies der IT-Abteilung der HWR unverzüglich mitzuteilen.
2. Ein Wartungszugriff darf nur erfolgen, wenn die HWR eine Wartungsanfrage an den Auftragnehmer stellt. Der Wartungsmitarbeiter nimmt im Anschluss Kontakt zur IT-Abteilung der HWR auf, worauf der Wartungszugang aktiviert wird. Die Beendigung des Wartungszugriffs wird innerhalb von 30 Minuten der IT-Abteilung des Auftraggebers gemeldet.
3. Eine unbefugte Entfernung oder Übertragung personenbezogener Daten im Rahmen der Wartung durch oder an Dritte ist unzulässig. Der Zugriff auf personenbezogene Daten der HWR erfolgt ausschließlich durch den durch die HWR bereitgestellten VPN; diese dürfen das Netz der HWR nicht verlassen. Personenbezogene Daten dürfen nicht auf Datenträgern des Auftragnehmers gespeichert werden, sondern verbleiben im Hoheitsbereich der HWR.

§ 17 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. Eine Übermittlung während oder nach dem Vertragsverhältnis an Dritte bleibt ausgeschlossen. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.
2. Sollten personenebezogene Daten und/oder 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 und eine Kopie des Datenbestandes zur Verfügung zu stellen.
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.

Unterschriften

Ort, Datum Ort, Datum

Auftraggeber Auftragnehmer

# Anlage 1 – Technisch-organisatorische Maßnahmen

|  |  |
| --- | --- |
| Pseudonymisierung |  |
| Verschlüsselung |  |
| Gewährleistung der Vertraulichkeit |  |
| Gewährleistung der Integrität |  |
| Gewährleistung der Verfügbarkeit der Systeme |  |
| Gewährleistung der Belastbarkeit der Systeme |  |
| Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall |  |
| Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen |  |
| Es liegen schriftlich vor | [ ]  interne Verhaltensregeln[ ]  Risikoanalyse[ ]  allgemeine Datensicherheitsbeschreibung[ ]  umfassendes Datensicherheitskonzept[ ]  Wiederanlaufkonzept[ ]  Zertifikat: [ ]  Sonstiges: |
| Ist eine Beeinträchtigung der Sicherheit des Verfahrens bei Gewährung der Einsicht in die Dokumentation der technischen und organisatorischen Maßnahmen zu befürchten? | [ ]  Ja[ ]  NeinBejahendenfalls ist die Dokumentation der technischen und organisatorischen Maßnahmen von der Einsichtnahme durch Betroffene gemäß § 4 Abs. 3 BbgDSG ausgenommen.  |

**Erläuterungen zu den technisch-organisatorische Maßnahmen**

**Pseudonymisierung**

Bei der Pseudonymisierung wird der Name oder ein anderes Identifikationsmerkmal durch ein Pseudonym (zumeist eine mehrstellige Buchstaben- oder Zahlenkombination, auch Code genannt) ersetzt, um die Feststellung der Identität des Betroffenen auszuschließen oder wesentlich zu erschweren. Bitte insoweit auch angeben wo und wie die Liste mit den Klarnamen aufbewahrt wird, wie sie gesichert ist und welche Personen Zugang haben.

**Verschlüsselung**

Welche Verschlüsselungsverfahren werden im Hinblick auf welche Daten eingesetzt, wie werden ggf. die Passwörter gesichert.

**Gewährleistung der Vertraulichkeit**

Wie wird gewährleistet, dass nur Berechtigte Zugang zu den verarbeiteten Daten haben, z.B. durch:

* Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;
* Zugangskontrolle
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
* Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;
* Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

**Gewährleistung der Integrität**

Wie wird die Richtigkeit der zu verarbeitenden Daten gewährleistet, wie werden Änderungen und Löschungen gesteuert.

* Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
* Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

**Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme**

* Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall

**Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall**

* Incident-Response-Management
* Meldewege und Notfallpläne
* Strategie zur Wiederherstellung von Backups (rasche Wiederherstellbarkeit)

**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung**

* Datenschutz-Management;
* Datenschutzfreundliche Voreinstellungen;
* Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

# 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:

* Ulrike Becker, IT-Leitung, ulrike.becker@hwr-berlin.de

(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…