

Vertrag zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

zwischen der

FernUniversität in Hagen, Universitätsstr. 47, 58097 Hagen

- Verantwortliche -

nachstehend Auftraggeber genannt (AG)

und dem/der

<< >>

- Auftragsverarbeiter -

nachstehend Auftragnehmer genannt (AN)

ggf. Vertreter gemäß Art. 27 DSGVO

(für AN ohne Niederlassung in der Union):

Der AN verarbeitet personenbezogene Daten im Auftrag des AG i. S. d. Art. 4 Nr. 8 und Art. 28 der Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung (DSGVO). Dieser Vertrag regelt die Rechte und Pflichten der Parteien im Zusammenhang mit der Verarbeitung von personenbezogenen Daten.

1 Gegenstand des Auftrags

- ☐ Die Auftragsverarbeitung erfolgt anlässlich eines zwischen den Parteien geschlossenen Hauptvertrages. Der Gegenstand des Auftrags ergibt sich aus dem Hauptvertrag/ der Leistungsvereinbarung/ SLA/

vom

_____, auf die hier Bezug genommen wird.

Oder

- ☒ Die Auftragsverarbeitung erfolgt anlässlich eines zwischen den Parteien geschlossenen Vertrages über die Prüfung, Implementierung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen des AG oder einer entsprechenden Beratung hierzu, bei dem ein Zugriff auf personenbezogene Daten des AG nicht ausgeschlossen werden kann. In diesem Fall sind die technischen und organisatorischen Details der Tätigkeiten vor Ort und der Fernwartungszugriffe des AN auf IT-Systeme im Netzwerk des AG in **Anlage 5** dieses Vertrages festgelegt und beschrieben.

Oder

- ☐ Der Gegenstand des Auftrags umfasst die Durchführung folgender Aufgaben durch den AN:

-
-
-

2 Dauer des Auftrags

2.1 Art der Vertragsdauer

☒ Die Dauer dieses Auftrags entspricht der Laufzeit des Hauptvertrages.

Oder

☐ Der Auftrag wird zur einmaligen Ausführung erteilt.

Oder

☐ der Auftrag ist unbefristet erteilt und kann von den Parteien mit einer Frist von _____ zum _____ gekündigt werden.
Die fristlose Kündigung bleibt hiervon unberührt.

2.2 Fristlose Vertragskündigung bei Vertragsverstößen

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DS-GVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2.3 Fortgeltung von Rechten und Pflichten über das Vertragsende hinaus

Die Rechte und Pflichten gemäß Zif. 5.1.6 und Zif. 5.4.3 (Datenlöschung, -berichtigung, -einschränkung), Zif. 5.5 (Vertraulichkeit) und Zif. 7 (Geheimhaltung) dieses Vertrages gelten auch über das Vertragsende hinaus.

3 Umfang, Art und Zweck der Datenverarbeitung

Der AN verarbeitet personenbezogene Daten des AG im Rahmen der Tätigkeiten gemäß Zif. 1. dieses Vertrages.

3.1 Umfang der Datenverarbeitung

Die Art der verarbeiteten personenbezogenen Daten und die Kategorien der Betroffenen Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3.2 Art und Zweck der Verarbeitung der personenbezogenen Daten

Der Zweck der Verarbeitung der personenbezogenen Daten ergibt sich aus Zif. 1. dieses Vertrages. Sofern nicht bereits in Zif. 1. oder in den darüber in Bezug genommenen Vereinbarungen konkret beschrieben, ist die Art der Verarbeitung der personenbezogenen Daten in **Anlage 1** zu diesem Vertrag festgelegt.

3.3 Ort der Datenverarbeitung

3.3.1

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.

3.3.2

Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des AG und darf nur erfolgen, wenn die besonderen Voraussetzungen zu einem angemessenen Schutzniveau gemäß Art. 44 ff. EU-DSGVO erfüllt sind.

3.3.3 entfällt

~~Bei beabsichtigtem Drittlandtransfer:~~

Das angemessene Schutzniveau in Art. _____ ist festgestellt durch

- ☐ ~~einen Angemessenheitsbeschluss der Kommission gemäß Art. 45 Abs. 3 EU-DSGVO;~~
- ☐ ~~wird hergestellt durch verbindliche interne Datenschutzvorschriften gemäß Art. 46 Abs. 2 lit. b i.V.m. Art. 47 EU-DSGVO;~~
- ☐ ~~wird hergestellt durch Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 lit. c und d EU-DSGV;~~
- ☐ ~~wird hergestellt durch genehmigte Verhaltensregeln gemäß Art. 46 Abs. 2 lit. e i.V.m. Art. 40 EU-DSGVO;~~
- ☐ ~~wird hergestellt durch einen genehmigten Zertifizierungsmechanismus gemäß Art. 46 Abs. 2 lit. f i.V.m. Art. 42 EU-DSGVO;~~
- ☐ ~~wird hergestellt durch sonstige Maßnahmen gemäß Art. 46 Abs. 2 lit. a, Abs. 3 litt. a und b EU-DSGVO: _____~~

4 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers (AG)

4.1 Allgemein

4.1.1

Der AG ist Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den AN. Der AG ist damit allein verantwortlich für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO.

Dem AN steht nach Zif. 5.8 dieses Vertrages das Recht zu, den AG darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

4.1.2

Der AG informiert den AN unverzüglich und vollständig, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten feststellt.

4.2 Weisungsbefugnisse

4.2.1

Weisungen werden anfänglich durch den Auftrag festgelegt und können vom AG danach in schriftlicher Form durch einzelne Weisungen über Art, Umfang und Verfahren der Datenverarbeitung geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen per einfacher E-Mail und Telefon (fernmündlich) bestätigt der AG unverzüglich in schriftlicher oder ausreichend gesicherter elektronischer Form.

4.2.2

Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers beim Auftragnehmer entstehen, bleiben unberührt.

4.2.3

Weisungsbefugte Personen des AG und Weisungsempfänger des AN werden in **Anlage 2** zu diesem Vertrag benannt.

4.3 Betroffenenrechte und Informationspflichten

4.3.1

Der AG ist als Verantwortlicher für die Wahrung der Betroffenenrechte nach Art. 12 bis 22 DSGVO verantwortlich. Der AN wird den AG unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem AN geltend machen. Für den AN gelten insoweit die Pflichten gemäß Zif. 5.4 dieses Vertrages.

4.3.2

Für den Fall, dass eine Melde- und Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder eine sonstige, für den AG geltende gesetzliche Meldepflicht besteht, ist der AG für deren Einhaltung verantwortlich. Für den AN gelten insoweit die Pflichten gemäß Zif. 5.3 dieses Vertrages.

4.4 Kontrollrechte und -pflichten

4.4.1

Der AG ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim AN getroffenen technischen und organisatorischen Maßnahmen gemäß Zif. 5.2 dieses Vertrages sowie von der Einhaltung der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

4.4.2

Hierfür kann er entweder Selbstauskünfte des Auftragnehmers einholen, sich ein Testat eines Sachverständigen vorlegen lassen, oder nach vorheriger Abstimmung eine eigenständige Prüfung vor Ort durchführen.

5 Rechte und Pflichten des Auftragnehmers (AN)

5.1 Allgemein

5.1.1

Der AN und jede dem AN unterstellte Person, die Zugang zu personenbezogenen Daten hat, verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen

und nach Weisungen des AG, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem er als Auftragsverarbeiter unterliegt, verpflichtet ist (z. B. Ermittlungen von Strafverfolgungsbehörden); in einem solchen Fall teilt der AN dem AG diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

5.1.2

Der AN hat die Auftragsverarbeitung so durchzuführen, dass sie im Einklang mit den Anforderungen der DSGVO steht und den Schutz der Rechte der betroffenen Personen gewährleistet.

5.1.3

Der AN sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

5.1.4

Der AN sichert zu, dass die für den AG verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Die Datenträger und die Datenbestände, die vom AG stammen bzw. für den AG genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

5.1.5

Der AN verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des AG nicht erstellt.

5.1.6

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechnete Interessen des Auftragnehmers dem nicht entgegenstehen. Dies gilt auch über die Beendigung des Vertrages hinaus.

5.2 Technisch-organisatorische Maßnahmen des AN

5.2.1

Der AN trifft alle gemäß Art. 32 i.V.m. Art 28 Abs. 3 lit. c) DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme und Dienste zu gewährleisten und kontrolliert diese regelmäßig.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

5.2.2

Die Einzelheiten zu den technischen und organisatorischen Maßnahmen sind vom AN zu dokumentieren und vor Beginn der Verarbeitung, insbesondere vor der konkreten Auftragsdurchführung, dem AG zur Prüfung zu übergeben.

Bei Akzeptanz durch den AG werden die dokumentierten Maßnahmen Grundlage des Auftrags und Bestandteil dieses Vertrages in **Anlage 3**. Soweit die Prüfung des AG einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

5.2.3

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem AN gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren und dem AG mitzuteilen.

5.2.4

Die getroffenen technischen und organisatorischen Maßnahmen sind gegenüber dem AG im Rahmen seiner Kontrollbefugnisse gemäß Zif. 4.4 dieses Vertrages jederzeit nachzuweisen.

5.2.5

Der AN stellt dem AG auf dessen Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für diese Auftragsverarbeitung zur Verfügung.

5.3 Mitteilungspflichten bei Störungen der Verarbeitung, bei Verletzungen des Schutzes personenbezogener Daten und Tätigwerden der Aufsichtsbehörde

5.3.1

Der AN teilt dem AG unverzüglich - spätestens aber binnen 48 Stunden ab Kenntnis - Störungen, Verstöße des AN oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit.

5.3.2

Dies gilt vor allem im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des AG nach Art. 33 und Art. 34 DSGVO, die binnen 72 Stunden nach Bekanntwerden wahrzunehmen ist. Der AN sichert zu, den AG erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen.

5.3.3

Die Meldung des AN an den AG muss insbesondere folgende Informationen beinhalten:

- 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;

- eine Beschreibung der von dem AN ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

5.3.4

Meldungen nach Art. 33 oder 34 DSGVO für den AG an die Aufsichtsbehörden oder Betroffenen darf der AN nur nach vorheriger ausdrücklicher Weisung durch den AG gemäß Zif. 4.2. dieses Vertrages durchführen.

5.3.5

Ferner wird der AN den AG unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem AN tätig wird und dies auch eine Kontrolle der Verarbeitung, die der AN im Auftrag des AG erbringt, betreffen kann.

5.4 Mitwirkungspflichten bei der Wahrung von Betroffenenrechten, Erstellung von Verzeichnissen über Verarbeitungstätigkeiten und Datenschutz-Folgeabschätzungen

5.4.1

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den AG, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten nach Art. 30 DSGVO sowie bei erforderlichen Datenschutz-Folgeabschätzungen des AG nach Art. 35 DSGVO hat der AN im notwendigen Umfang mitzuwirken und den AG soweit möglich angemessen zu unterstützen.

5.4.2

Der AN hat dazu jeweils unverzüglich an folgende Stelle des AG –
ZDI, Abteilung SAP

(Kontaktdaten der verantwortlichen Organisationseinheit der FernUniversität in Hagen)

– weiterzuleiten:

- alle ihm verfügbaren, erforderlichen Informationen zu Erfüllung der vorgenannten Pflichten des AG
- gegenüber ihm selbst geltend gemachte Betroffenenrechte

5.4.3

Soweit eine Mitwirkung des AN für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Einschränkung, Sperrung oder Löschung - durch den AG erforderlich ist, wird der AN die jeweils erforderlichen Maßnahmen nach Weisung des AG treffen.

5.4.4

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der AN nur nach vorheriger Weisung oder Zustimmung durch den AG gemäß Zif. 4.2 dieses Vertrages erteilen.

5.5 Wahrung der Vertraulichkeit

5.5.1

Der AN bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Er verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem AG obliegen:

-

(z. B. Bankgeheimnis, Fernmeldegeheimnis, Sozialgeheimnis, Berufsgeheimnisse nach § 203 StGB etc.)

5.5.2

Der AN überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb. Er setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die bei der Verarbeitung personenbezogener Daten auf Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 S. 2 lit. b EU-DSGVO) und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden.

5.5.3

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte darf der AN nur nach vorheriger Weisung oder Zustimmung durch den AG gemäß Zif. 4.2 dieses Vertrages erteilen.

5.5.4

Die Vereinbarungen zur Vertraulichkeit bestehen auch nach Beendigung des Vertrages fort.

5.6 Datenschutzbeauftragter des Auftragnehmers

5.6.1

Der AN bestätigt, dass er eine/n Datenschutzbeauftragte/n nach Art. 37 DSGVO benannt hat. Der AN trägt Sorge dafür, dass die/der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

5.6.2

Beim AN ist als Beauftragte(r) für den Datenschutz Herr/Frau

<<>>

(Vorname, Name, Organisationseinheit, Telefon)

bestellt. Ein Wechsel der/des Datenschutzbeauftragten ist dem AG unverzüglich mitzuteilen.

5.6.3

Die Pflicht zur Benennung eines Datenschutzbeauftragten kann im Ermessen des AG entfallen, wenn der AN nachweisen kann, dass er gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen und der AN nachweisen kann, dass betriebliche Regelungen bestehen, die eine Verarbeitung personenbezogener Daten unter Einhaltung der

gesetzlichen Vorschriften, der Regelungen dieses Vertrages sowie etwaiger weiterer Weisungen des AG gewährleisten.

5.7 Kontrollbefugnis der Aufsichtsbehörde

Der AN unterwirft sich im Rahmen der Auftragsdurchführung der Kontrolle der zuständigen Aufsichtsbehörde gemäß Art. 51 DSGVO (hier: der/dem Landesbeauftragten für Datenschutz und Informationsfreiheit NRW).

5.8 Beanstandung von Weisungen des AG

Der AN hat den AG unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung gemäß Zif 4.2 dieses Vertrages verstoße gegen Datenschutzvorschriften. Der AN ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den AG bestätigt oder geändert wird.

5.9 Kontrollbefugnisse des AG

Der AN erklärt sich damit einverstanden, dass der AG - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom AG beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort.

Der AN sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

6 Unterauftragsverhältnisse

6.1 Unterauftragsverhältnisse – Definitionen

Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

Nicht hierzu gehören Nebenleistungen, die der AN z. B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Benutzerservice in Anspruch nimmt. Der AN ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des AG auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

Die Wartung und Pflege von IT-System oder Applikationen stellt ein zustimmungspflichtiges Unterauftragsverhältnis und Auftragsverarbeitung i. S. d. Art. 28 DSGVO dar, wenn die Wartung und Prüfung solche IT-Systeme betrifft, die auch im Zusammenhang mit der Erbringung von Leistungen für den AG genutzt werden und bei der Wartung auf personenbezogenen Daten zugegriffen werden kann, die im Auftrag des AG verarbeitet werden.

6.2 Zustimmungserfordernis des AG für Unterauftragsverhältnisse

Der AN darf Unterauftragnehmer (UAN, weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des AG beauftragen. Diese werden in **Anlage 4** dokumentiert.

Die Zustimmung ist so rechtzeitig einzuholen, dass dem AG bis zur geplanten Beauftragung eine angemessene Zeit zur Überprüfung bleibt. Liegt ein wichtiger datenschutzrechtlicher Grund des AG vor, die Zustimmung zu verweigern, und ist eine einvernehmliche Lösung zwischen den Parteien nicht zu erzielen, wird dem AG ein Sonderkündigungsrecht eingeräumt.

Oder

- ☐ Eine Unterbeauftragung ist unzulässig.

Ggf.

- ☐ Der AG stimmt der Beauftragung der in **Anlage 4** dieses Vertrages festgelegten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2 und 4 EU-DSGVO zu.

6.3 Eignung der Unterauftragnehmer (UAN)

Der AN hat den Unterauftragnehmer unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auszuwählen. Die relevanten Prüfunterlagen dazu sind dem AG auf Anfrage zur Verfügung zu stellen.

6.4 Übertragung von Rechten und Pflichten auf UAN

Der AN hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen AG und AN auch gegenüber Unterauftragnehmern gelten. Dies ist dem AG erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen nachzuweisen. Der AN haftet gegenüber dem AG dafür, dass der Unterauftragnehmer insbesondere den Datenschutzpflichten nachkommt, die dem AN mit diesem Vertrag auferlegt wurden.

6.5 Kontrollbefugnisse von AG und Aufsichtsbehörden bei UAN

Der AN ist insbesondere verpflichtet, durch vertragliche Regelungen sicherzustellen, dass die Kontrollbefugnisse des AG und von Aufsichtsbehörden auch gegenüber dem Unterauftragnehmer gelten. Es ist zudem vertraglich zu regeln, dass der Unterauftragnehmer diese Kontrollmaßnahmen und etwaige Vor-Ort-Kontrollen zu dulden hat.

6.6 Datenschutzbeauftragte bei UAN

Für den Fall, dass kein Datenschutzbeauftragter beim Unterauftragnehmer benannt worden ist, hat der Auftragnehmer den Auftraggeber hierauf hinzuweisen und Informationen dazu beizubringen, aus denen sich ergibt, dass der Unterauftragnehmer gesetzlich nicht verpflichtet ist, einen Datenschutzbeauftragten zu benennen.

6.7 Trennung der Aufgaben von AN und UAN

In dem Vertrag mit dem Unterauftragnehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des AN und des Unterauftragnehmers deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern.

6.8 Prüfungs- und Inspektionsberechtigung des AG bei UAN

Insbesondere muss der AG berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragnehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

6.9 Beginn der Unterbeauftragung erst nach vertraglicher Regelung

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

7 Geheimhaltung

7.1 Geheimhaltungspflicht

Beide Parteien verpflichten sich, alle Informationen, die sie im Zusammenhang mit der Durchführung dieses Vertrages erhalten, zeitlich unbegrenzt vertraulich zu behandeln und nur zur Durchführung des Vertrages zu verwenden. Keine Partei ist berechtigt, diese Informationen ganz oder teilweise zu anderen als den soeben genannten Zwecken zu nutzen oder diese Information Dritten zugänglich zu machen.

7.2 Begrenzung der Geheimhaltung

Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

7.3 Fortgeltung der Geheimhaltung nach Vertragsende

Die Vereinbarungen zur Geheimhaltung bestehen auch nach Beendigung des Vertrages fort.

8 Beendigung des Vertrages

8.1 Rückgabe und/oder Löschung von Daten

Nach Beendigung des Vertrages hat der AN sämtliche in seinen Besitz sowie an Subunternehmen gelangte Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des AG an diesen zurückzugeben oder zu in datenschutzkonformer Weise zu löschen. Hierzu

gehören auch Test- und Ausschussmaterial. Die Löschung ist in geeigneter Weise zu dokumentieren und dem AG zu bestätigen.

8.2 Aufbewahrungspflichten bleiben unberührt

Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

8.3 Vernichtung von Datenträgern

Für Datenträger gilt, dass diese im Falle einer vom AG gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der Norm ISO/IEC 21964 (siehe auch ehem. DIN 66399) einzuhalten ist; die Vernichtung ist dem AG unter Hinweis auf diese Sicherheitsstufe nachzuweisen.

8.4 Kontrollrecht des AG bei Rückgabe und/oder Löschung von Daten

Der AG hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim AN zu kontrollieren. Dies kann auch durch eine Inaugenscheinnahme der Datenverarbeitungsanlagen in der Betriebsstätte des AN erfolgen. Die Vor-Ort-Kontrolle soll mit angemessener Frist durch den AG angekündigt werden.

9 Haftung

Auf Art. 82 DSGVO wird verwiesen.

10 Sonstiges

10.1 Ausschluss der Einrede des Zurückbehaltungsrechts

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den AN i. S. d. § 273 BGB hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen wird.

10.2 Informationspflicht des AN bei Gefährdung der Daten des AG

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des AG beim AN durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren, durch Forderungen von Polizei, Ermittlungsbehörden oder richterlichen Beschluss) oder durch sonstige Ereignisse gefährdet werden, so hat der AN den AG unverzüglich zu verständigen. Der AN wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

11 Schlussbestimmungen

11.1 Schriftformerfordernis bei Nebenabreden

Für Nebenabreden ist die Schriftform erforderlich.

11.2 Rechtsgültigkeit trotz unwirksamer Teile des Vertrags

Sollten einzelne Teile dieses Vertrages unwirksam sein, so berührt dies die Wirksamkeit der übrigen Regelungen des Vertrages nicht.

11.3 Rechtsgeltung, Gerichtsort

Es gilt deutsches Recht. Sofern nicht anders vereinbart, ist der Gerichtsstand Hagen.

_____, den _____, _____, den _____
Ort Datum Ort Datum

- Auftraggeber - - Auftragnehmer -

Anlage 1 zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

Ergänzung zu Zif. 3 des Vertrages

1. *Art der Daten*

Aufgrund der Komplexität der in einer integrierten Systemumgebung wie SAP vorhandenen zahlreichen Daten und Objekte und der Aufgabenstellung können keine einzelnen Datenfelder mit Umfang, Art und Zweck der Erhebung, Verarbeitung oder Nutzung festgelegt werden.

Somit sind alle Daten und Datenarten, die in den SAP Systemen verarbeitet werden betroffen.

2. *Kategorien betroffener Personen*

Betroffene Personen sind alle Beschäftigten und Studierenden der FernUniversität, sowie auch externe Personen, dessen Daten aufgrund gesetzlicher Bestimmungen erhoben, verarbeitet und genutzt werden.

3. *Art der Verarbeitung der personenbezogenen Daten*

Einblick auf Datenobjekte im Rahmen der Beratungsleistung entsprechend der Leistungsbeschreibung im Beisein von Beschäftigten der FernUniversität oder auch eigenständige Zugriffe auf Datenobjekte durch das zur Verfügung stellen von (administrativen) Benutzerkennungen für das SAP System sowohl vor Ort in der FernUniversität, als auch aus der Ferne durch geeignete Verbindungen.

Anlage 2

zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

Weisungsberechtigte und Weisungsempfänger gemäß Zif. 4.2.3. des Vertrages

Art der Kommunikation bei Weisungen

Weisungsberechtigte Personen des Auftraggebers sind:

1. Dominik Eversberg, Leitung Abteilung SAP
2. Sarah Merker, Abteilung SAP, Universitätsstraße 27, sarah.merker@fernuni-hagen.de

Weisungsempfänger beim Auftragnehmer sind:

1. <<>>
2. <<>>

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Weisung zu nutzende Kommunikationskanäle:

Für Weisung zu nutzende Kommunikationskanäle:

1. Seitens AG (Weisungsberechtigt):

Anschrift:

FernUniversität in Hagen
ZDI – KompetenzCenter Business Applications
Universitätsstr. 27
58097 Hagen

E-Mail:

sarah.merker@fernuni-hagen.de

2. Seitens AN (Weisungsempfänger):

Anschrift:

<<>>

E-Mail:

<<>>

Telefonnummer:

<<>>

Anlage 3

zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

Technisch-organisatorische Maßnahmen gemäß Zif.5.2.2. des Vertrages

Darstellung der technischen und organisatorischen Maßnahmen (TOM) durch den AN.

Die zu treffenden Maßnahmen müssen geeignet sein, folgendes zu gewährleisten

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

▪ Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

TOM des AN: ...

▪ Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperremechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;

TOM des AN: ...

▪ Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

TOM des AN: ...

▪ Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

TOM des AN: ...

2. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

TOM des AN: ...

3. Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Unter Verschlüsselung versteht man Verfahren und Algorithmen, die Daten und Dateien (Text, Bild, Audio, Video, etc.) oder auch Netzwerkverbindungen mittels digitaler bzw. elektronischer Codes oder Schlüssel inhaltlich in eine nicht einfach lesbare, betrachtbare oder auslesbare Form umwandeln. Diesen Vorgang bezeichnet man als Verschlüsseln. Gleichzeitig wird dafür gesorgt, dass nur mit dem Wissen eines Schlüssels die geheimen (verschlüsselten) Daten wieder entschlüsselt, also lesbar und betrachtbar und somit wieder verarbeitet werden können.

TOM des AN: ...

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

- Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

TOM des AN: ...

- Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

TOM des AN: ...

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

- Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne; Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO); Ausreichende informationstechnische Kapazität, z.B. redundante Anwendungssysteme und Serverstruktur, oder Loadbalancing bei webbasierten Anwendungen.

TOM des AN: ...

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

- Datenschutz-Management;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
- Auftragskontrolle

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen, gesicherte Kommunikationswege der Weisungen, .

TOM des AN: ...

Anlage 4
zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

Unterauftragnehmer gemäß Zif. 6.2. dieses Vertrages

Unterauftragnehmer	Anschrift /Land	Ansprechpartner	Leistung (Kategorien der verarbeiteten Daten des AG und Art der Datenverarbeitung)

Anlage 5

zum Vertrag zur Auftragsverarbeitung gemäß Art. 28 EU-DSGVO

Auftragsverarbeitung anlässlich von (Fern)Wartung und Beratungen durch Externe gemäß Zif. 1 Alt. 2 dieses Vertrages

Folgende vom Zentrum für Digitalisierung und IT (ZDI) der Fernuniversität in Hagen (Fernuniversität oder AG) definierte Maßnahmen sind mindestens einzuhalten. Abweichungen und Anpassungen an spezielle Gegebenheiten der jeweiligen IT-Systeme sind möglich bei gleichbleibendem Sicherheitsniveau und Dokumentation.

Im Rahmen der beauftragten und zu leistenden Arbeiten hat der AN folgende Rahmenbedingungen bei Zugriff auf das Netzwerk, die IT-Systeme und Anwendungen des AG zu beachten:

- Der AN erhält für Arbeiten an den IT-Systemen und Anwendungen eine eigene personalisierte Benutzerkennung eingerichtet. Das dazugehörige Passwort ist regelmäßig zu ändern (spätestens alle 60 Tage). Hierbei sind die Kennwortrichtlinien des AG/des ZDI zu beachten und einzuhalten. Jeder Mitarbeitende des AN erhält eine eigene personalisierte Benutzerkennung für seine Aufgaben zugewiesen. Der AN nutzt die ihm für seine Arbeiten überlassene personalisierte Benutzerkennung ausschließlich für sich selbst und gibt diese nicht an Dritte weiter.
- Sind für Arbeiten an den IT-Systemen und Anwendungen des AG spezielle Berechtigungen oder Rollen notwendig, so sind diese über den für den AN zuständigen Ansprechpartner des AG einzufordern.
- Nutzt der AN für die Ausübung seiner Tätigkeiten eigene technische Geräte stellt er sicher, dass hiervon keinerlei Gefahren auf die Netzinfrastruktur, IT-Systeme und Anwendungen des AG übergehen können.
- Veränderungen an den IT-Systemen und Anwendungen, insbesondere Konfigurationsänderungen, sind seitens des AN mit den jeweils zuständigen Personen des AG abzustimmen und nach dem durch den AG spezifizierten Dokumentationsstandard zu dokumentieren.

Insbesondere beim Fernzugriff auf das Netzwerk und die IT-Systeme des AG gelten die zusätzlichen Bedingungen:

- Das eigene Netz muss mittels einer Firewall gegen unberechtigte Zugriffsversuche von außen geschützt sein.
- Der Fernzugriff von außerhalb auf das Netzwerk des AG erfolgt ausschließlich über eine VPN-Verbindung. Die Einrichtung der VPN-Verbindung erfolgt in Absprache mit dem Rechenzentrum (ZDI) des AG. Notwendige Konfigurationen an Firewall und Netzwerkkomponenten für den Zugriff auf Subnetze sind zuvor über den zuständigen Ansprechpartner des AG einzufordern und zu legitimieren.

- Ist für den Aufbau eines Fernzugriffs auf IT-Systeme oder Anwendungen spezielle zusätzliche Software notwendig, ist diese ausschließlich nur nach Legitimation durch das Rechenzentrum (ZDI) des AG einzusetzen.
- Es findet eine lückenlose Protokollierung aller Zugriffsversuche durch den AG statt, so dass erkennbar ist, wer im Rahmen der Fernwartung wann auf welche Art und Weise auf welche Daten zugegriffen hat.
- Der für die Fernwartung genutzte Rechner in den Räumlichkeiten des AN ist gegen den Zugriff Unberechtigter geschützt.
- Der Fernzugriff sollte generell nur innerhalb der üblichen Arbeitszeiten des AG durchgeführt werden. Ein Fernzugriff außerhalb dieser Zeiten ist durch den AN mit dem zuständigen Ansprechpartner des AG abzustimmen und zu legitimieren und zu dokumentieren. Der Zugriff ist nach erfolgter Tätigkeit zu beenden und die Verbindung zu schließen.
- Aufzeichnungen (z. B. Screenrecording, Screenshots o. Ä.) oder Logging von Aktivitäten auf den Systemen des AG bedürfen der expliziten Zustimmung des zuständigen Ansprechpartners des AG.
- Dateiübertragungen aus dem Bereich des AG hinaus über den Fernwartungszugang hin zu Drittsystemen oder den Systemen des AN bedürfen der expliziten Zustimmung durch den AG.