Vereinbarung über die Verarbeitung von Daten im Auftrag gemäß Art. 28 DSGVO

Diese Vereinbarung zur Verarbeitung von Daten im Auftrag regelt die Datenverarbeitung im Auftrag des Auftraggebers durch den Verein CompetenceCenter Duale Hochschulstudien - StudiumPlus e.V., Charlotte-Bamberg-Straße 3, 35578 Wetzlar als Auftragnehmer. Sie ist Teil des Hauptvertrages über die Zurverfügungstellung von Dienstleistungen an den, in der jeweiligen Vereinbarung genannten Auftraggeber.

1. Allgemeines

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers 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.

(2) Sofern in diesem Vertrag der Begriff „Datenverarbeitung“ oder „Verarbeitung“ (von Daten) benutzt wird, wird die Definition der „Verarbeitung“ i.S.d. Art. 4 Nr. 2 DSGVO zugrunde gelegt.

2. Gegenstand des Auftrags

Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind in **Anlage 1** zu diesem Vertrag festgelegt.

3. Rechte und Pflichten des Auftraggebers

(1) Der Auftraggeber ist Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO für die Verarbeitung von Daten im Auftrag durch den Auftragnehmer. Dem Auftragnehmer steht nach Ziff. 4 Abs. 5 das Recht zu, den Auftraggeber darauf hinzuweisen, wenn eine seiner Meinung nach rechtlich unzulässige Datenverarbeitung Gegenstand des Auftrags und/oder einer Weisung ist.

(2) Der Auftraggeber ist als Verantwortlicher für die Wahrung der Betroffenenrechte verantwortlich. Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn Betroffene ihre Betroffenenrechte gegenüber dem Auftragnehmer geltend machen.

(3) Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen über Art, Umfang und Verfahren der Datenverarbeitung gegenüber dem Auftragnehmer zu erteilen. Weisungen können in Textform (z.B. E-Mail) erfolgen.

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

(5) Der Auftraggeber kann weisungsberechtigte Personen benennen. Sofern weisungsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsberechtigten Personen beim Auftraggeber ändern, wird der Auftraggeber dies dem Auftragnehmer in Textform mitteilen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten durch den Auftragnehmer feststellt.

(7) Für den Fall, dass eine Informationspflicht gegenüber Dritten nach Art. 33, 34 DSGVO oder einer sonstigen, für den Auftraggeber geltenden gesetzlichen Meldepflicht besteht, ist der Auftraggeber für deren Einhaltung verantwortlich.

4. Allgemeine Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und/oder unter Einhaltung der ggf. vom Auftraggeber erteilten ergänzenden Weisungen. Ausgenommen hiervon sind gesetzliche Regelungen, die den Auftragnehmer ggf. zu einer anderweitigen Verarbeitung verpflichten. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Zweck, Art und Umfang der Datenverarbeitung richten sich ansonsten ausschließlich nach diesem Vertrag und/oder den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung von Daten ist dem Auftragnehmer untersagt, es sei denn, dass der Auftraggeber dieser schriftlich zugestimmt hat.

(2) Die Datenverarbeitung findet nach Maßgabe der folgenden Bestimmungen statt.

☑* Der Auftragnehmer verpflichtet sich, die Datenverarbeitung im Auftrag nur in Mitgliedsstaaten der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) durchzuführen.

☐* 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 Drittländern

- ☐* 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. 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. 40 DS-GVO);
- ☐* wird hergestellt durch einen genehmigten Zertifizierungsmechanismus (Art. 46 Abs. 2 lit. f i.V.m. 42 DS-GVO).
- ☐* wird hergestellt durch sonstige Maßnahmen (Art. 46 Abs 2 lit. a, Abs. 3 lit. a und b DS-GVO):

(*Zutreffendes ankreuzen/anhaken)

(3) Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsmäßige Abwicklung aller vereinbarten Maßnahmen zu.

(4) Der Auftragnehmer ist verpflichtet, sein Unternehmen und seine Betriebsabläufe so zu gestalten, dass die Daten, die er im Auftrag des Auftraggebers verarbeitet, im jeweils erforderlichen Maß gesichert und vor der unbefugten Kenntnisnahme Dritter geschützt sind. Der Auftragnehmer wird Änderungen in der Organisation der Datenverarbeitung im Auftrag, die für die Sicherheit der Daten erheblich sind, vorab mit dem Auftraggeber abstimmen.

(5) Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung nach seiner Auffassung gegen gesetzliche Regelungen verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Sofern der Auftragnehmer darlegen kann, dass eine Verarbeitung nach Weisung des Auftraggebers zu einer Haftung des Auftragnehmers nach Art. 82 DSGVO führen kann, steht dem Auftragnehmer das Recht frei, die weitere Verarbeitung insoweit bis zu einer Klärung der Haftung zwischen den Parteien auszusetzen.

(6) Die Verarbeitung von Daten im Auftrag des Auftraggebers außerhalb von Betriebsstätten des Auftragnehmers oder Subunternehmern ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform zulässig. Eine Verarbeitung von Daten für den Auftraggeber in Privatwohnungen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform im Einzelfall zulässig.

(7) Der Auftragnehmer wird die Daten, die er im Auftrag für den Auftraggeber verarbeitet, getrennt von anderen Daten verarbeiten. Eine physische Trennung ist nicht zwingend erforderlich.

(8) Der Auftragnehmer kann dem Auftraggeber die Person(en) benennen, die zum Empfang von Weisungen des Auftraggebers berechtigt sind. Sofern weisungsempfangsberechtigte Personen benannt werden sollen, werden diese in der **Anlage 1** benannt. Für den Fall, dass sich die weisungsempfangsberechtigten Personen beim Auftragnehmer ändern, wird der Auftragnehmer dies dem Auftraggeber in Textform mitteilen.

5. Datenschutzbeauftragter des Auftragnehmers

Der Auftragnehmer bestätigt, dass er einen Datenschutzbeauftragten nach Art. 37 DSGVO benannt hat. Der Auftragnehmer trägt Sorge dafür, dass der Datenschutzbeauftragte über die erforderliche Qualifikation und das erforderliche Fachwissen verfügt.

Name und Anschrift des Datenschutzbeauftragten:
Der Datenschutzbeauftragte des Auftragnehmers, gem. Art. 37 DSGVO ist:
Herr Rechtsanwalt Frank Eckerkunst
c/o ITWerk Giessen GmbH
Siemensstrasse 7
35394 Gießen
Deutschland
Tel.: +49 641 96993-0
E-Mail: eckerkunst@itwerk-giessen.de
Website: www.itwerk-giessen.de

6. Meldepflichten des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, dem Auftraggeber jeden Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen und/oder die erteilten Weisungen des Auftraggebers, der im Zuge der Verarbeitung von Daten durch ihn oder andere mit der Verarbeitung beschäftigten Personen erfolgt ist, unverzüglich mitzuteilen. Gleiches gilt für jede Verletzung des Schutzes personenbezogener Daten, die der Auftragnehmer im Auftrag des Auftraggebers verarbeitet.

(2) Ferner wird der Auftragnehmer den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde nach Art. 58 DSGVO gegenüber dem Auftragnehmer tätig wird und dies auch eine Kontrolle der Verarbeitung, die der Auftragnehmer im Auftrag des Auftraggebers erbringt, betreffen kann.

(3) Dem Auftragnehmer ist bekannt, dass für den Auftraggeber eine Meldepflicht nach Art. 33, 34 DSGVO bestehen kann, die eine Meldung an die Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden vorsieht. Der Auftragnehmer wird den Auftraggeber bei der Umsetzung der Meldepflichten unterstützen. Der Auftragnehmer wird dem Auftraggeber insbesondere jeden unbefugten Zugriff auf personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, unverzüglich, spätestens aber binnen 48 Stunden ab Kenntnis des Zugriffs mitteilen. Die Meldung des Auftragnehmers an den Auftraggeber 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 Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

7. Mitwirkungspflichten des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nach Art. 12-23 DSGVO. Es gelten die Regelungen von Ziff. 11 dieses Vertrages.

(2) Der Auftragnehmer wirkt an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten durch den Auftraggeber mit. Er hat dem Auftraggeber die insoweit jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

(3) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten.

8. Kontrollbefugnisse

(1) Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz und/oder die Einhaltung der zwischen den Parteien getroffenen vertraglichen Regelungen und/oder die Einhaltung der Weisungen des Auftraggebers durch den Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren.

(2) Der Auftragnehmer ist dem Auftraggeber gegenüber zur Auskunftserteilung verpflichtet, soweit dies zur Durchführung der Kontrolle i.S.d. Absatzes 1 erforderlich ist.

(3) Der Auftraggeber kann eine Einsichtnahme in die vom Auftragnehmer für den Auftraggeber verarbeiteten Daten sowie in die verwendeten Datenverarbeitungssysteme und -programme verlangen.

(4) Der Auftraggeber kann nach vorheriger Anmeldung mit angemessener Frist die Kontrolle im Sinne des Absatzes 1 in der Betriebsstätte des Auftragnehmers zu den jeweils üblichen Geschäftszeiten vornehmen. Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

(5) Der Auftragnehmer ist verpflichtet, im Falle von Maßnahmen der Aufsichtsbehörde gegenüber dem Auftraggeber i.S.d. Art. 58 DSGVO, insbesondere im Hinblick auf Auskunfts- und Kontrollpflichten die erforderlichen Auskünfte an den Auftraggeber zu erteilen und der jeweils zuständigen Aufsichtsbehörde eine Vor-Ort-Kontrolle zu ermöglichen. Der Auftraggeber ist über entsprechende geplante Maßnahmen vom Auftragnehmer zu informieren.

9. 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, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

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

a) ☐* Eine Unterbeauftragung ist unzulässig.

b) ☑* Der Auftraggeber stimmt der Beauftragung der nachfolgend aufgeführten Unterauftragnehmer **(Anlage 2)** zu unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO:

Unterauftragnehmer	Anschrift/Land	Leistung
Wissenschaftliches Zentrum Duales Hochschulstudium (**ZDH**)	Charlotte-Bamberg-Straße 3 D - 35578 Wetzlar	Laut Anlage 2

DATEV eG	Paumgartnerstr. 6 – 14 D - 90429 Nürnberg	Laut Anlage 2

c) ☑* Die Auslagerung auf Unterauftragnehmer oder

☐* der Wechsel des bestehenden Unterauftragnehmers

sind zulässig, soweit:

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DSGVO zugrunde gelegt wird.

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

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen nach Ziffer 4 des Vertrages sicher. Gleiches gilt, wenn Dienstleister im Sinne von Ziffer 9 Abs. 1 Satz 2 eingesetzt werden sollen.

(5) Eine weitere Auslagerung durch den Unterauftragnehmer

☐* ist nicht gestattet;

☑* bedarf der ausdrücklichen Zustimmung des Hauptauftraggebers (mind. Textform);

☐* bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform).

(*Zutreffendes ankreuzen/anhaken)

Sämtliche vertraglichen Regelungen in der Vertragskette sind auch den weiteren Unterauftragnehmern aufzuerlegen.

10. Vertraulichkeitsverpflichtung

(1) Der Auftragnehmer ist bei der Verarbeitung von Daten für den Auftraggeber zur Wahrung der Vertraulichkeit über Daten, die er im Zusammenhang mit dem Auftrag erhält bzw. zur Kenntnis erlangt, verpflichtet. Der Auftragnehmer verpflichtet sich, die gleichen Geheimnisschutzregeln zu beachten, wie sie dem Auftraggeber obliegen. Der Auftraggeber ist verpflichtet, dem Auftragnehmer etwaige besondere Geheimnisschutzregeln mitzuteilen.

(2) Der Auftragnehmer sichert zu, dass ihm die jeweils geltenden datenschutzrechtlichen Vorschriften bekannt sind und er mit der Anwendung dieser vertraut ist. Der Auftragnehmer sichert ferner zu, dass er seine Beschäftigten mit den für sie maßgeblichen

Bestimmungen des Datenschutzes vertraut macht und zur Vertraulichkeit verpflichtet hat. Der Auftragnehmer sichert ferner zu, dass er insbesondere die bei der Durchführung der Arbeiten tätigen Beschäftigten zur Vertraulichkeit verpflichtet hat und diese über die Weisungen des Auftraggebers informiert hat.

(3) Die Verpflichtung der Beschäftigten nach Absatz 2 sind dem Auftraggeber auf Anfrage nachzuweisen.

11. Wahrung von Betroffenenrechten

(1) Der Auftraggeber ist für die Wahrung der Betroffenenrechte allein verantwortlich. Der Auftragnehmer ist verpflichtet, den Auftraggeber bei seiner Pflicht, Anträge von Betroffenen nach Art. 12-23 DSGVO zu bearbeiten, zu unterstützen. Der Auftragnehmer hat dabei insbesondere Sorge dafür zu tragen, dass die insoweit erforderlichen Informationen unverzüglich an den Auftraggeber erteilt werden, damit dieser insbesondere seinen Pflichten aus Art. 12 Abs. 3 DSGVO nachkommen kann.

(2) Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten - insbesondere auf Auskunft, Berichtigung, Sperrung oder Löschung - durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen.

(3) Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch Mitwirkungsleistungen im Zusammenhang mit Geltendmachung von Betroffenenrechten gegenüber dem Auftraggeber beim Auftragnehmer entstehen, bleiben unberührt.

12. Geheimhaltungspflichten

(1) 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.

(2) 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.

13. Vergütung

Die Vergütung des Auftragnehmers wird gesondert vereinbart und ist Teil des Hauptvertrages.

14. Technische und organisatorische Maßnahmen zur Datensicherheit

(1) Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

(2) Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist als **Anlage 3** zu diesem Vertrag beigefügt. Die Par-

teien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Wesentliche Änderungen, die die Integrität, Vertraulichkeit oder Verfügbarkeit der personenbezogenen Daten beeinträchtigen können, wird der Auftragnehmer im Voraus mit dem Auftraggeber abstimmen. Maßnahmen, die lediglich geringfügige technische oder organisatorische Änderungen mit sich bringen und die Integrität, Vertraulichkeit und Verfügbarkeit der personenbezogenen Daten nicht negativ beeinträchtigen, können vom Auftragnehmer ohne Abstimmung mit dem Auftraggeber umgesetzt werden. Der Auftraggeber kann jederzeit eine aktuelle Fassung der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

(3) Der Auftragnehmer wird die von ihm getroffenen technischen und organisatorischen Maßnahmen regelmäßig und auch anlassbezogen auf ihre Wirksamkeit kontrollieren. Für den Fall, dass es Optimierungs- und/oder Änderungsbedarf gibt, wird der Auftragnehmer den Auftraggeber informieren.

15. Dauer des Auftrags

(1) Dauer

☑* Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit der Leistungsvereinbarung (Hauptvertrag) oder,

falls keine Leistungsvereinbarung zur Dauer besteht,

☐* 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 3 Monaten zum Jahresende gekündigt werden. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

(*Zutreffendes ankreuzen/anhaken)

(2) Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer den Zutritt des Auftraggebers oder der zuständigen Aufsichtsbehörde vertragswidrig verweigert.

16. Beendigung

(1) Nach Beendigung des Vertrages hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, Daten und erstellten Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers an diesen zurückzugeben oder zu löschen. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt. Für Datenträger gilt, dass diese im Falle einer vom Auftraggeber gewünschten Löschung zu vernichten sind, wobei mindestens die Sicherheitsstufe 3 der DIN 66399 einzuhalten ist; die Vernichtung ist dem Auftraggeber unter Hinweis auf die Sicherheitsstufe gemäß DIN 66399 nachzuweisen.

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

17. Zurückbehaltungsrecht

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

18. Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

(2) Für Nebenabreden ist die Schriftform erforderlich.

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

(4) Es gilt deutsches Recht. Gerichtsstand ist der Sitz des Auftraggebers, soweit sich nicht aus dem zugrundeliegenden Hauptvertrag ein anderer Gerichtsstand ergibt.

Anlage 1 - Gegenstand der Verarbeitung

1. Gegenstand und Zweck der Verarbeitung

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

- Der Auftragnehmer verarbeitet im Rahmen des Auftrags personenbezogene Daten des Auftraggebers zum Zwecke der studentischen Betreuung von Mitarbeitern/Studenten des Auftraggebers

Der Auftrag des Auftraggebers an den Auftragnehmer umfasst folgende Arbeiten und/oder Leistungen:

☑* Bereitstellung von Lernplattformen einschließlich Hard- und Software für Beschäftigte des Auftraggebers während des theoretischen Teils des dualen Studiums

☐* Sonstiges…….

2. Kategorien betroffener Person

Kreis der von der Datenverarbeitung betroffenen Personen:

☑* Mitgliederdaten

☑* Beschäftigtendaten

☑* Ansprechpartner

☑* Mitarbeiter

☑* Sonstige: alle verfügbaren personenbezogenen Daten

(*Zutreffendes ankreuzen/anhaken)

3. Art(en) der personenbezogenen Daten

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

☑* Bestandsdaten

☑* Personenstammdaten

☑* Kommunikationsdaten (z.B. Telefon, E-Mail)

☑ * Leistungs- und Beurteilungsdaten

☑* Abrechnungs- und Zahlungsdaten

☑* Sonstiges: Weitere Daten, die dem Auftragnehmer vom Auftraggeber für die Durchführung seiner Leistungen zur Verfügung gestellt werden bzw. die im Rahmen der Durchführung der Leistungen des Auftragnehmers vom Auftragnehmer für den Auftraggeber erhoben werden

(* Zutreffendes ankreuzen/anhaken)

Anlage 2 - Unterauftragnehmer

Der *Auftragnehmer* nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).

Dabei handelt es sich um nachfolgende(s) Unterauftragnehmer:

Firma Unterauftragnehmer	Anschrift/Land	Leistungen
Wissenschaftliches Zentrum Duales Hochschulstudium (**ZDH)**	Charlotte-Bamberg-Straße 3, 35578 Wetzlar	Siehe Anlage 1 - Gegenstand des Auftrages
Datev eG	Paumgartnerstr. 6-14, 90429 Nürnberg	Buchhaltung

Anlage 3

Allgemeine Dokumentation

Technische und organisatorische Maßnahmen für Verantwortliche (Art. 30 Abs. 1 lit. g EU-DSGVO)

Der Verein CompetenceCenter Duale Hochschulstudien - StudiumPlus e.V. als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO bestätigt Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen zu haben Art. 32 Abs. 1 DSGVO, § 64 BDSG.
Die getätigten Datenschutzmaßnahmen haben das Ziel der Sicherstellung der Verfügbarkeit der Daten, Integrität, Vertraulichkeit, Nichtverkettbarkeit durch Zweckbestimmung, Transparenz durch Prüffähigkeit und Intervenierbarkeit durch Ankerpunkte. Es werden Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten durchgeführt, welche ein aktuelles Schutzniveau gewährleisten. Ebenso haben unsere Maßnahmen zur Datensicherheit das Ziel einer dauerhaften, hohen Belastbarkeit unserer Systeme und Dienste hinsichtlich der damit verbundenen Datenverarbeitung. Wir stellen die Fähigkeit sicher, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Ferner verwenden wir ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung. Überdies unternehmen der Verantwortliche Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet. Die Geschäftsprozesse von orientieren sich an den Vorgaben des Art. 32 DSGVO.

Dies sind folgende:

1. **Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b, 1. Alt. DSGVO)**

a) Zutrittskontrolle

Unbefugten wird durch folgende Maßnahmen der Zutritt sowie der Zugang zu den Datenverarbei- tungsanlagen verwehrt, mit denen personenbezogene Daten verarbeitet oder gesichert werden:

Die Räumlichkeiten des Vereins befinden sich in mehrgeschossigen Gebäudekomplexen in 35578 Wetzlar, Ch.-Bamberg-Str. 3. Das Zugangs-Management und die Verwaltung der ausgegebenen Schlüssel obliegt dem Verantwortlichen.

- Personenidentifikation, Zentrale Zutrittsregelung für Büroräume (Schließsystem mit Chipkarten/Transponder sowie Schlüsselregelung / Schlüsselbuch), für die Ausgabe gibt einen Prozess (Protokollierung), ein Verlust ist unverzüglich melden, außerdem gibt es einen Prozess beim Ausscheiden eines Mitarbeiters, der auch die Rückgabe regelt
- Räume verfügen über Schließsystem
- Eingangstüren verfügen über einen Knauf an der Außenseite
- Absicherung der Gebäudeschächte
- Lagerung von vertraulichen Dokumenten ausschließlich unter Verschluss in abschließbaren, Schränken
- Anmeldung für Besucher
- Sorgfältige Auswahl von Reinigungspersonal

a) Zugangskontrolle

Unbefugte werden durch folgende Maßnahmen an der Benutzung der Datenverarbeitungssysteme gehindert:

- Anmeldung an IT-Systemen mit vorheriger Authentifizierung, dies erfolgt durch persönlichen und individuellen User-Log-In mittels Benutzernamen und Passwortschutz
- Erstellung von Benutzerprofilen mit einem Benutzerstammsatz pro User
- IP-beschränkter Zugriff auf Server
- BIOS Schutz mittels separatem Passwort
- Zentrale Passwortvergabe
- Richtlinien „Sicheres Passwort", „Löschen und Vernichten" sowie „CleanDesk" und „manuelle Desktopsperre"
- Einsatz von Anti-Viren Software auf Servern und Clients sowie mobilen Geräten
- Einsatz von Firewall
- Einsatz von VPN-Technologie bei Remote Zugriffen
- Einsatz von IDS (Intrusion-Detection-Systeme)
- Verschlüsselung von Datenträgern, Notebook, Tablets und Smartphones
- Gehäuseverriegelung

b) Zugriffskontrolle

- Einsatz eines Berechtigungskonzeptes
- Erstellung und Verwaltung von Benutzerprofilen und Benutzerberechtigungen durch IT-Administration nach vorheriger schriftlicher Anweisung der Geschäftsführung
- Berechtigungskonzept (Lese- bzw. Lese-Schreibzugriff) für digitale Zugriffsmöglichkeiten,
  eine Berechtigung zur Nutzung eines IT Systems oder Applikation wird nach dem 4-Augen Prinzip erteilt. Eine Berechtigung erfolgt nur in dem Umfang, die für den Mitarbeiter erforderlich ist, damit dieser seine arbeitsvertraglichen Verpflichtungen erfüllen kann
- Erteilte Berechtigungen und deren Entzug werden protokolliert
- Periodische Überprüfungen der eingeräumten Berechtigungen in relevanten Teilbereichen, im Falle von Aufgabenwechseln von Mitarbeitern erfolgt eine entsprechende Korrektur der Berechtigungen bei der IT-Administration
- Im Falle des Ausscheidens von Mitarbeitern wird die IT-Administration unverzüglich über anstehende Veränderungen informiert, damit entsprechende Berechtigungen entzogen werden können, der Entzug muss spätestens binnen 24 Stunden nach dem Ausscheiden eines Mitarbeiters durchgeführt worden sein
- Beschränkung der Anzahl Administratoren unter Berücksichtigung von Krankheits- und Vertretungsregelungen auf das Notwendigste
- Regelmäßige Überprüfung der Benutzerrollen
- Deaktivierung der Benutzerkonten bei Ausscheiden oder Wechsel des Mitarbeiters durch Administrator
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Protokollierung von Zugriffen auf Anwendungen (Eingabe, Änderung und Löschung von Daten) sowie der Vernichtung von Daten und Datenträgern durch mechanische Zerstörung
- Einsatz von Aktenvernichtern sowie zertifizierten Dienstleistern zur Aktenvernichtung (DIN 32757)
- Sichere Aufbewahrung von Datenträgern

c) Pseudonymisierung

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

- Eine Pseudonymisierung erfolgt nach den entsprechenden Voraussetzungen der vom Verantwortlichen eingesetzten Verarbeitungen, insbesondere der Software, die eine Pseudonymisierung vorsehen.
- Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder nach Ablauf der gesetzlichen Aufbewahrungs- und Löschfrist möglichst zu anonymisieren/ pseudonymisieren

d) Trennungskontrolle

Die im Verein getroffenen Maßnahmen der Trennungskontrolle gewährleisten darüber hinaus, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten ebenfalls getrennt verarbeitet werden. Die nachfolgend aufgeführten Maßnahmen sind zur Erreichung dieses Zwecks in die Geschäftsabläufe implementiert:

- Einsatz mandantenfähiger Software mit logischer Mandantentrennung
- Entwicklungs- und Testsysteme werden nicht betrieben
- Physikalische Trennung von Systemen, Datenbanken, Datenträgern
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- Datensätze sind mit Zweckattributen versehen

1. Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b, 2. Alt. DSGVO)

Die im Verein getroffenen Maßnahmen der Integrität gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Darüber hinaus wird sichergestellt, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Diese Prozesse werden durch die nachfolgend aufgeführten Maßnahmen unterstützt:

a) Eingabekontrolle

- differenzierte und aufgabenbezogene Berechtigungen gemäß Berechtigungskonzept mit Benutzerprofilen
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
- Aufzeichnung von Logfiles
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen, jederzeitige Nachvollziehbarkeit, welcher Benutzer Daten eingegeben, geändert oder gelöscht hat durch Protokollierung
- Übersicht mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
- Manuelle oder automatisierte Kontrolle der Protokolle
- Aufbewahrung der Formulare/Unterlagen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Klare Übertragung von Zuständigkeiten für Löschungen

b) Weitergabekontrolle

Die im Verein getroffenen Maßnahmen gewährleisten eine hinreichende Weitergabekontrolle. Personenbezogene Daten werden bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt, ohne dass dies überprüft, festgestellt und unterbunden werden kann. Über die gesetzlich vorgesehenen Ausnahmefälle hinaus werden keinerlei Daten an Dritte weitergegeben. Folgende Maßnahmen sind dabei vorgesehen:

- Dokumentation der Datenempfänger sowie der Dauer der Überlassung bzw. Löschfristen
- Übersicht regelmäßiger Abruf- und Übermittlungsvorgänge
- Einsatz von VPN
- Bereitstellung verschlüsselter Verbindungen (sftp, https)
- Nutzung von Signaturverfahren (teilweise)
- Dokumentation der Empfänger von Daten und Zeitspannen der geplanten Überlassung

c) Auftragskontrolle

Die im Verein getroffenen Maßnahmen gewährleisten ebenfalls ein hohes Schutzniveau im Bereich Auftragskontrolle. Gegenwärtig finden keine Auftragsverarbeitungen statt. Sofern eine Auftragsverarbeitung stattfindet, erfolgen die nachstehend getroffenen Maßnahmen:

- Schriftlicher Vertrag zur Auftragsverarbeitung gem. Art 28 DS-GVO mit Regelungen zu den Rechten und Pflichten des Auftragnehmers und Auftraggebers bzw. EU Standardvertragsklauseln
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten, insbesondere hinsichtlich Datensicherheit und Datenschutz sowie vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation sowie bei längerer Zusammenarbeit laufende Überprüfung des Auftragnehmers und des Schutzniveaus

- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Vereinbarung wirksamer Kontrollrechte
- Regelung zum Einsatz weiterer Subunternehmer des Auftragnehmers
- Existenz von Regelungen zur Datenvernichtung und Löschung

2. Gewährleistung der Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b, 3. Alt. DSGVO)

Die im Verein getroffenen Maßnahmen zur Verfügbarkeitskontrolle gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust sowie Systeme gegen Unfälle und Eindringlinge durch folgende Maßnahmen geschützt sind:

- Regelmäßiges Backup-Verfahren, Kontrolle des Sicherungsvorgangs
- Parallelbetrieb von Festplatten (RAID-Verfahren)
- Getrennte Partitionen für Betriebssysteme und Daten
- Unterbrechungsfreite Notstromversorgung (USV)
- Schutzsteckdosenleisten im Serverraum
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Notfallplan mit Kontaktdaten externer Dienstleister sowie regelmäßige Überprüfung
- Regelmäßige Systemwartung
- Feuerlöschgeräte am Serverraum, Feuer- und Rauchmeldeanalgen im Gebäude
- Klimaanlage in Serverräumen
- Aufbewahrung der Datensicherung an einem sicheren ausgelagerten sicheren Ort
- Datensicherheitskonzept (Backup & Recovery Plan) und regelmäßiger Check

3. Die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall kann durch folgende Maßnahmen rasch wiederhergestellt werden - Wiederherstellung der Verfügbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Die im Verein getroffenen Maßnahmen Herstellung zur Wiederherstellung der Verfügbarkeit der personenbezogenen Daten bei einem physischen oder technischen Zwischenfall gewährleisten eine Wiederherstellung der relevanten Systeme innerhalb von spätestens 48 Stunden. Folgende Maßnahmen wurden getroffen:

- Datensicherheitskonzept (Backup & Recovery Plan)
- Doppelsicherung der Sicherungskopien
- Interne / externe Aufbewahrung von Datensicherungen
- Datenwiederherstellung nach Notfallplan
- Durchführung regelmäßiger Stress- und Performancetests, um die Systeme nach dem Stand der Technik aufrechtzuerhalten

4. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit. d, Art. 25 Abs. 1 DSGVO)

Der Verein als Verantwortlicher hat die Verantwortung für den Datenschutz durch Leitlinien übernommen.

Es wurde ein externer Datenschutzbeauftragter benannt.

Darüber hinaus gibt eine Richtlinie für Mitarbeiter im Umgang mit personenbezogenen Daten. Die Umsetzung und Sensibilisierung erfolgt durch regelmäßige Schulungen, in denen die Mitarbeiter zum vertraulichen Umgang mit personenbezogenen Daten verpflichtet werden. Die Mitarbeiter werden geschult und zur Vertraulichkeit sowie auf das Datengeheimnis verpflichtet. Es erfolgt eine regelmäßige Sensibilisierung.

Es wurde ein Incident-Response-Management System implementiert. Dieses beinhaltet neben dem Einsatz von IDS den Einsatz von Virenscanner, Firewall und Spamfilter sowie deren regelmäßige Aktualisierung auch dokumentierte Prozesse zur Erkennung, Umgang und Meldung von Sicherheitsvorfällen/ Datenpannen, auch im Hinblick auf Meldepflichten gegenüber Aufsichtsbehörden sowie zur Nachbearbeitung.

Sofern Datenschutzverletzungen erkannt werden, ist unverzüglich der Datenschutzbeauftragte zu konsultieren, damit nach Prüfung und Feststellung eines meldepflichtigen Vorgangs gemäß Art. 33 DSGVO die Aufsichtsbehörde innerhalb von 72 Stunden oder, wenn gesetzlich erforderlich, der Betroffene informiert werden kann.

Der Datenschutzbeauftragte ist in jedem Fall vorab zu konsultieren, sofern ein Prozess aufgesetzt wird, der eine Datenschutzfolgenabschätzung gemäß Art. 35 DSGVO zur Folge hat.

Ebenso ist der Datenschutzbeauftragte zentraler Ansprechpartner für die Anfragen von Betroffenen, die nach Eingang unverzüglich, spätestens innerhalb von 48 Stunden an diesen weiterzuleiten sind, um eine fristgerechte Beantwortung gemäß Art. 12 Abs. 3 DSGVO zu gewährleisten.

Im Rahmen des Datenschutz-Audits durch den benannten Datenschutzbeauftragten erfolgen neben der Nachbereitung der datenschutzrechtlichen Bestandsaufnahme fortlaufende Maßnahmen zur Sicherstellung der datenschutzrechtlichen Vorgaben. Darüber hinaus findet eine jährliche Bewertung und Evaluierung durch den Datenschutzbeauftragten statt. Ebenso wird mindestens jährlich eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen durchgeführt.

Im Verein erfolgt der Einsatz von Standardsoftware. Maßnahmen nach Art. 25 DSGVO („privacy by design“, „privacy by default“) sind möglich, wenn die Anbieter/Softwarehersteller im Zuge ihrer jeweiligen Anpassungen / Updates eine Implementierung derartiger Verarbeitungen vorsehen werden. Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

Es wurde ein Datenschutzmanagement- (DSMS) und ein Informationssicherheitsmanangementsystem (ISMS) implementiert und im Datenschutzhandbuch hinterlegt.

Zentrale Dokumentation aller Leitlinien, Richtlinien, Verfahrensweisen, Regelungen und Prozesse zum Datenschutz im Datenschutzhandbuch mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (Intranet).

Der Verein als Verantwortlicher kommt seinen Informationspflichten nach Art. 13 und 14 DSGVO nach.

Es wurde ein Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30, Abs. 1 und 2 DSGGVO erstellt.

Einsatz eines Datenschutz-Management Systems beim externen Datenschutzbeauftragten.