

Vertrag zur Auftragsverarbeitung, Art. 28 DSGVO anlässlich VR-Bildung 4.0

zwischen

als Verantwortlicher (hier bezeichnet als „Bank“)

und

Genossenschaftsverband - Verband der Regionen e.V., Wilhelm-Haas-Platz, 63263 Neu-Isenburg,

als Auftragsverarbeiter (hier bezeichnet als „Akademie“)

Präambel

Die Bank möchte die Akademie mit den in § 3 genannten Leistungen beauftragen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

§ 1 Begriffsbestimmungen

(1) Verantwortlicher ist gem. Art. 4 Abs. 7 DSGVO die Stelle, die allein oder gemeinsam mit anderen Verantwortlichen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(2) Auftragsverarbeiter ist gem. Art. 4 Abs. 8 DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(3) Personenbezogene Daten sind gem. Art. 4 Abs. 1 DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.



(4) Besonders schutzbedürftige personenbezogene Daten sind personenbezogenen Daten gem. Art. 9 DSGVO, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit von Betroffenen hervorgehen, personenbezogene Daten gem. Art. 10 DSGVO über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen sowie genetische Daten gem. Art. 4 Abs. 13 DSGVO, biometrischen Daten gem. Art. 4 Abs. 14 DSGVO, Gesundheitsdaten gem. Art. 4 Abs. 15 DSGVO sowie Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

(5) Verarbeitung ist gem. Art. 4 Abs. 2 DSGVO jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(6) Aufsichtsbehörde ist gem. Art. 4 Abs. 21 DSGVO eine von einem Mitgliedstaat gem. Art. 51 DSGVO eingerichtete unabhängige staatliche Stelle.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Aufsichtsbehörde für die Bank ist der jeweilige Landesdatenschutzbeauftragte.

(2) Zuständige Aufsichtsbehörde für die Akademie ist der Hessische Beauftragte für Datenschutz und Informationsfreiheit, Postfach 3163, 65021 Wiesbaden.

(3) Die Bank und die Akademie und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

(1) Die Akademie erbringt für die Bank Leistungen im Bereich Betrieb von web-basierten Lernplattformen mit Lerntagebüchern, Videos, Foren, Wikis, Webinaren, Seminaren, Workshops, Coachings, Workshops, e-testings und Lernprogrammen auf Grundlage des Nutzungsvertrages VR-Bildung. Dabei erhält die Akademie Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung der Bank. Umfang und Zweck der Datenverarbeitung durch die Akademie ergeben sich aus dem Nutzungsvertrag VR-Bildung sowie des Bildungsvertrages zwischen zu schulendem Mitarbeiter und der Akademie. Der Bank obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen der vorliegenden Vereinbarung gehen im Zweifel den Regelungen des Nutzungsvertrag VR-Bildung vor.



(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Nutzungsvertrag VR-Bildung und Bildungsvertrag in Zusammenhang stehen und bei der die Akademie und ihre Beschäftigten oder durch die von der Akademie Beauftragten mit personenbezogenen Daten in Berührung kommen, die von der Bank stammen oder für die Bank erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Haupt- bzw. Bildungsvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

§ 4 Weisungsrecht

(1) Die Akademie darf Daten nur im Rahmen des Nutzungsvertrages VR-Bildung und gemäß den Weisungen der Bank erheben, verarbeiten oder nutzen; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird die Akademie durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt sie der Bank diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen der Bank werden anfänglich durch diesen Vertrag festgelegt und können von der Bank danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Die Bank ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus Anlage 5. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl von der Bank als auch vom Akademie zu dokumentieren. Weisungen, die über die vertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist die Akademie der Ansicht, dass eine Weisung der Bank gegen datenschutzrechtliche Bestimmungen verstößt, hat sie die Bank unverzüglich darauf hinzuweisen. Die Akademie ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch die Bank bestätigt oder geändert wird. Die Akademie darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 5 Art der verarbeiteten Daten, Kreis der Betroffenen

(1) Im Rahmen der Durchführung des Schulungsvertrags erhält die Akademie Zugriff auf die in Anlage 1 näher spezifizierten personenbezogenen Daten. Diese Daten umfassen die in Anlage 1 aufgeführten und als solche gekennzeichneten besonderen Kategorien personenbezogener Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in Anlage 2 dargestellt.



§ 6 Schutzmaßnahmen der Akademie

(1) Die Akademie ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich der Bank erlangten Informationen nicht an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Die Akademie wird in ihrem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Sie trifft alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten der Bank bzw. deren Mitarbeiter gem. Art. 32 DSGVO, insbesondere mindestens die in Anlage 3 aufgeführten Maßnahmen der

- a) Zutrittskontrolle
- b) Zugangskontrolle
- c) Zugriffskontrolle
- d) Weitergabekontrolle
- e) Eingabekontrolle
- f) Auftragskontrolle
- g) Verfügbarkeitskontrolle
- h) Trennungskontrolle.

Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt der Akademie vorbehalten, wobei sie sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Die Akademie veröffentlicht die Kontaktdaten des Datenschutzbeauftragten auf ihrer Internetseite und teilt sie der Aufsichtsbehörde mit (datenschutz@genossenschaftsverband.de). Veröffentlichung und Mitteilung weist die Akademie auf Anforderung der Bank in geeigneter Weise nach.

(4) Den bei der Datenverarbeitung durch die Akademie beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Die Akademie wird alle Personen, die von ihr mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und der Akademie bestehen bleiben. Der Bank sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.



§ 7 Informationspflichten der Akademie

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen der Akademie, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch die Akademie, bei ihr im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird die Akademie die Bank unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen der Akademie durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält zumindest folgende Informationen:

- a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze;
- b) eine Beschreibung der von der Akademie ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(2) Die Akademie trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber die Bank und ersucht um weitere Weisungen.

(3) Die Akademie ist darüber hinaus verpflichtet, der Bank jederzeit Auskünfte zu erteilen, soweit deren Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Sollten die Daten der Bank bei der Akademie durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat die Akademie die Bank unverzüglich darüber zu informieren, sofern ihr dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Die Akademie wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich bei der Bank als „Verantwortlichem“ im Sinne der DSGVO liegen.

(5) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 hat die Akademie die Bank unverzüglich zu unterrichten.

(6) Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten für den Datenschutz ist der Bank unverzüglich mitzuteilen.

(7) Die Akademie und gegebenenfalls ihr Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag der Bank durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Das Verzeichnis ist der Bank auf Anforderung zur Verfügung zu stellen.

(8) An der Erstellung des Verfahrensverzeichnisses durch die Bank hat die Akademie im angemessenen Umfang mitzuwirken. Sie hat der Bank die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.



§ 8 Kontrollrechte der Bank

(1) Die Bank überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen der Akademie. Hierfür kann sie z. B. Auskünfte der Akademie einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen der Akademie nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zur Akademie steht. Die Bank wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe der Akademie dabei nicht unverhältnismäßig stören. Sollte sich eine Kontrolle als mutwillig herausstellen, hat die Bank deren Kosten zu tragen.

(2) Die Akademie verpflichtet sich, der Bank auf deren mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen der Akademie erforderlich sind.

(3) Die Bank dokumentiert das Kontrollergebnis und teilt es der Akademie mit. Bei Fehlern oder Unregelmäßigkeiten, die die Bank insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat sie die Akademie unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt die Bank der Akademie die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Die Akademie stellt der Bank auf deren Wunsch ein umfassendes und aktuelles Datenschutz- und Sicherheitskonzept für die Auftragsverarbeitung sowie über zugriffsberechtigte Personen zur Verfügung.

(5) Die Akademie weist der Bank die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

§ 9 Einsatz von Subunternehmern

(1) Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in Anlage 4 genannten Subunternehmer durchgeführt. Die Akademie ist im Rahmen ihrer vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt, soweit sie die Bank hiervon vorab in Kenntnis setzt und diese der Beauftragung des Subunternehmers vorab schriftlich zugestimmt hat. Die Akademie ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Die Akademie hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass die Bank ihre Rechte aus dieser Vereinbarung (insbesondere ihre Prüf- und Kontrollrechte) direkt gegenüber den Subunternehmern wahrnehmen kann. Die Bank erklärt ihr Einverständnis zur Einschaltung von Subunternehmern, wenn diese bereits in der genossenschaftlichen Finanzgruppe oder für andere deutsche Kreditinstitute in Kernbankbereichen nachhaltig als Auftragsverarbeiter tätig sind. Die



Akademie wird der Bank auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(2) Die Bank erklärt ihr Einverständnis zur Einschaltung der VR Bildung GbR des Bildungsverbundes, bestehend aus 1. Akademie Deutscher Genossenschaften e.V., Schloss Montabaur, 56410 Montabaur, 2. Baden-Württembergischer Genossenschaftsverband e.V., Heilbronner Straße 41, 70191 Stuttgart, 3. ABG GmbH, Leising 16, 92339 Beilngries, 4. Genossenschaftsverband - Verband der Regionen e.V., Wilhelm-Haas-Platz, 63263 Neu-Isenburg, 5. Genossenschaftsverband Weser-Ems e.V., Raiffeisenstraße 26, 26122 Oldenburg.

(3) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn die Akademie Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die die Akademie für die Bank erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Subunternehmerverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für die Bank genutzt werden.

§ 10 Anfragen und Rechte Betroffener,

(1) Die Akademie unterstützt die Bank nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 und 36 DSGVO.

(2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber der Akademie geltend, so reagiert diese nicht selbstständig, sondern verweist den Betroffenen unverzüglich an die Bank und wartet deren Weisungen ab.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die ein Betroffener wegen einer nach dem Datenschutzrecht unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zur Akademie alleine die Bank gegenüber dem Betroffenen verantwortlich.

(2) Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.



§ 12 Außerordentliches Kündigungsrecht

Die Bank kann den Schulungsvertrag fristlos ganz oder teilweise kündigen, wenn die Akademie ihre Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO vorsätzlich oder grob fahrlässig verletzt oder eine Weisung der Bank nicht ausführen kann oder will. Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt die Bank der Akademie eine angemessene Frist, innerhalb welcher die Akademie den Verstoß abstellen kann.

§ 13 Beendigung des Nutzungsvertrages VR-Bildung

(1) Die Akademie wird der Bank nach Beendigung des Nutzungsvertrages VR-Bildung oder jederzeit auf deren Anforderung alle ihr überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch der Bank, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen bei der Akademie. Die Akademie hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen. Zu entsorgende Unterlagen sind mit einem Aktenvernichter nach DIN 32757-1 zu vernichten. Zu entsorgende Datenträger sind nach DIN 66399 zu vernichten.

(2) Die Bank hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten bei der Akademie in geeigneter Weise zu kontrollieren.

(3) Die Akademie ist verpflichtet, auch über das Ende des Schulungsvertrags hinaus die ihr im Zusammenhang mit dem Schulungsvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Schulungsvertrags hinaus solange gültig, wie die Akademie über personenbezogene Daten verfügt, die ihr von der Bank zugeleitet wurden oder die sie für diesen erhoben hat.

§ 14 Schlussbestimmungen

(1) Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch die Akademie i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

(3) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.



(4) Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist am Sitz der Akademie.

Anlagen:

Anlage 1 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

Anlage 3 – Technische und organisatorische Maßnahmen der Akademie

Anlage 4 – Genehmigte Subunternehmer nebst deren technischen und organisatorischen Maßnahmen

Anlage 5 – Weisungsberechtigte Personen

....., den Neu-Isenburg, den 04.11.2020

..... i. V.

i. V.

(Unterschrift Bank)

Eppo Franke

Udo Urner

Anlagen



Anlage 1 – Beschreibung der besonders schutzbedürftigen Daten/Datenkategorien

- Vor- und Zuname
- Benutzername
- E Mail-Adresse
- Arbeitgeber
- Lernstatistik
- Rolle (Kursteilnehmer, Bildungsmanager, Tutor, Administrator)

Anlage 2 – Beschreibung der Betroffenen/Betroffenengruppen

- Kunden (Arbeitgeber)
- Mitarbeiter

Anlage 3 – Technische und organisatorische Maßnahmen der Akademie

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

- Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen:

- mechanische oder elektronische Schließsysteme
- elektrische Türöffner
- Alarmanlagen
- Videoanlagen

- Zugangskontrolle

Keine unbefugte Systembenutzung:

- (sichere) Kennwörter
- automatische Sperrmechanismen
- Verschlüsselung von Datenträgern

- Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems:

- Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte
- Protokollierung von Zugriffen



- Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden:

- Mandantenfähigkeit

- Pseudonymisierung (Artikel 32 Abs. 1 lit. a DSGVO; Artikel 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:

- Personenbezogene Daten können pseudonymisiert verarbeitet werden, sofern dies verhältnismäßig ist

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

- Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport:

- Verschlüsselung
- Virtual Private Networks (VPN)
- elektronische Signatur

- Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

- Protokollierung

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

- Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

- Backup-Konzepte
- unterbrechungsfreie Stromversorgung (USV)
- Virenschutz
- Firewall
- Meldewege und Notfallpläne

- Rasche Wiederherstellbarkeit (Artikel 32 Abs. 1 lit. c DSGVO).

- Für wichtige IT-Systeme werden ausreichend Ressourcen zur Verfügung gestellt

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

- Datenschutz-Management;
- Auftragskontrolle



Keine Auftragsdatenverarbeitung im Sinne von Artikel 28 DSGVO ohne entsprechende Weisung des Auftraggebers

- Eindeutige Vertragsgestaltung
- formalisiertes Auftragsmanagement
- strenge Auswahl des Dienstleisters
- Vorabüberzeugungspflicht
- Nachkontrollen.

Anlage 4 – Genehmigte Subunternehmer

Die nachfolgenden Unternehmen sind genehmigte Subunternehmer im Sinne des § 9:

- 1.) Genossenschaftsverband - Verband der Regionen e.V.
- 2.) Fiducia & GAD IT AG
- 3.) PERBILITY GmbH
- 4) IMC AG
- 5) Peras GmbH
- 6) Noris Network GmbH

Anlage 5 – Weisungsberechtigte Personen

Weisungsberechtigte Personen der Bank: _____

Weisungsempfänger bei der Akademie sind die Herren Eppo Franke, Stefan Diehm, Thorsten Heitmann.