Vertrag über Auftragsverarbeitung (AVV)

zwischen

registrierte Schule

– nachfolgend „Verantwortlicher“ genannt –

und

Digitale Drehtür, Am Weidedamm 20, 28215 Bremen

– nachfolgend „Auftragsverarbeiter“ genannt

und gemeinsam als „Vertragsparteien“ bezeichnet – wird Folgendes vereinbart:

§ 1 Zweck

Die Digitale Drehtür stellt auf der Online-Plattform „Digitale Drehtür Campus“ Lernangebote für alle Schülerinnen und Schüler zur Verfügung. Die Inhalte werden von Schülerinnen und Schülern ergänzend zum Regelunterricht bearbeitet. Es handelt sich um Live-Formate (Videokonferenz) oder Selbstlernformate. Die erhobenen personenbezogenen Daten werden genutzt, um die Lernplattform selbst als auch die Lernangebote (weiter-) zu entwickeln, zu gestalten, durchzuführen, zu planen und auszuwerten. Die ausführlichen Zweckbestimmungen der Digitalen Drehtür werden in Anhang 1 aufgeführt.

§ 2 Gegenstand und Dauer des Auftrags

Der Auftragsverarbeiter führt die im Anhang 1 aufgeführten Datenverarbeitungen durch. Darin werden Gegenstand, Art und Dauer der Verarbeitung, Kategorien verarbeiteter Daten und betroffener Personen sowie die Löschfristen beschrieben.

§ 3 Weisungen der Verantwortlichen

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur für in Anhang 1 aufgeführte Zwecke bzw. nur auf Grund dokumentierter Weisungen des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine erteilte Weisung gegen geltende Datenschutzbestimmungen der Union oder eines Mitgliedstaats verstößt.

(3) Eine Verarbeitung der überlassenen personenbezogenen Daten durch den Auftragsverarbeiter für andere, insbesondere für eigene Zwecke ist unzulässig.

§ 4 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft mindestens die im Anhang 5 aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Die Maßnahmen haben ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus tragen die Vertragsparteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen, den Zwecken der Verarbeitung und der Datenkategorien (insbesondere nach Art. 9

Abs. 1 bzw. Art. 10 DSGVO) sowie den unterschiedlichen Eintrittswahrscheinlichkeiten und der Schwere des Risikos für die betroffenen Personen gebührend Rechnung.

(2) Die in Anhang 5 aufgeführten technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Diese sind durch den Auftragsverarbeiter anzupassen, wenn das bei Vertragsschluss festgelegte Sicherheitsniveau nicht mehr gewährleistet werden kann. Durch die Anpassung muss mindestens das Schutzniveau der bisherigen Maßnahmen erreicht werden. Soweit nichts anderes bestimmt ist, teilt der Auftragsverarbeiter die Anpassungen dem Verantwortlichen unaufgefordert mit.

§ 5 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(3) Soweit gesetzlich vorgeschrieben, bestellt der Auftragsverarbeiter einen Beauftragten für den Datenschutz und teilt dessen Kontaktdaten im Anhang 1 mit. Der Auftragsverarbeiter informiert unverzüglich und unaufgefordert über den Wechsel des Datenschutzbeauftragten.

(4) Der Auftragsverarbeiter erbringt die Auftragsverarbeitung im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedstaat der Europäischen Union oder innerhalb des Europäischen Wirtschaftsraums. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf stets der vorherigen dokumentierten Zustimmung des Verantwortlichen und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind.

§ 6 Unterstützungspflichten des Auftragsverarbeiters

(1) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragsverarbeiter bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden und bei Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jede Geltendmachung von Rechten durch die von den Datenverarbeitungen betroffenen Personen.

(2) Eine Unterstützung sichert der Auftragsverarbeiter bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten zu sowie bei der Einhaltung der Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind.

(3) Ferner unterstützt der Auftragsverarbeiter mit geeigneten technischen und organisatorischen Maßnahmen, damit der Verantwortliche seine bestehenden Pflichten gegenüber der betroffenen Person erfüllen kann.

§ 7 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragsverarbeiter darf Unterauftragsverarbeiter, die nicht in Anhang 2 benannt sind, nur beauftragen, wenn der Verantwortliche in die Beauftragung vorher schriftlich eingewilligt hat. Der Auftragsverarbeiter stellt die Informationen, die der Verantwortliche benötigt, um über die Genehmigung zu entscheiden, rechtzeitig, mindestens jedoch drei Wochen vor der Beauftragung des betreffenden Unterauftragsverarbeiters, zur Verfügung. Die Inanspruchnahme der in Anhang 2 zum Zeitpunkt der Vertragsunterzeichnung aufgeführten Unterauftragsverarbeiter gilt als genehmigt, sofern die in § 6 Abs. 2 dieses Vertrages genannten Voraussetzungen umgesetzt werden.

(2) Ein Zugriff auf personenbezogene Daten durch den Unterauftragsverarbeiter darf erst erfolgen, wenn der Auftragsverarbeiter durch einen schriftlichen Vertrag, der auch in einem elektronischen Format abgeschlossen werden kann, mit dem Unterauftragsverarbeiter sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber dem Unterauftragsverarbeiter gelten. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen eine Kopie des Vertrags und etwaiger späterer Änderungen zur Verfügung. Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen vollumfänglich dafür, dass der Unterauftragsverarbeiter seinen vertraglichen Pflichten nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen über vertragliche Pflichtverletzungen des Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter stellt bei einer Unterbeauftragung, die eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhaltet, die Einhaltung der Regelungen der Artikel 44 ff. DSGVO sicher, indem – sofern erforderlich – geeignete Garantien gemäß Artikel 46 DSGVO getroffen werden.

(4) Der Auftragsverarbeiter verpflichtet sich in den Fällen, in denen er einen Unterauftragsverarbeiter in Anspruch nimmt und in denen die Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der DSGVO beinhalten, mit dem Unterauftragsverarbeiter Standardvertragsklauseln nach Art. 46 DSGVO zu schließen, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

(5) Im Falle des § 6 Abs. 4 führt der Auftragsverarbeiter eine Prüfung nach den Klauseln 14 und 15 der Standardvertragsklauseln durch und stellt diese dem Verantwortlichen unaufgefordert zur Verfügung. Kommen Auftragsverarbeiter oder Verantwortlicher zu dem Ergebnis, dass weitere Maßnahmen getroffen werden müssen, um ein angemessenes Schutzniveau zu erreichen, sind diese Maßnahmen vom Auftragsverarbeiter bzw. vom Unterauftragsverarbeiter zu ergreifen. Der Unterauftragsverarbeiter darf erst dann in die Datenverarbeitung eingebunden werden, wenn ein angemessenes Schutzniveau sichergestellt ist.

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten oder sich unmittelbar aus der DSGVO ergebenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diesen Vertrag fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen im Sinne des Art. 28 Abs. 5 DSGVO des Auftragsverarbeiters berücksichtigen.

(2) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können gegebenenfalls auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden mit angemessener Vorankündigung

und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragsverarbeiters sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchgeführt.

(3) Die Vertragsparteien stellen den zuständigen Aufsichtsbehörden die in diesem Vertrag genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

§ 9 Mitzuteilende Verstöße

(1) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Verantwortlichen mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Verantwortlichen. Gleiches gilt, wenn der Auftragsverarbeiter feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Dem Auftragsverarbeiter ist bekannt, dass der Verantwortliche verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird Verletzungen an den Verantwortlichen unverzüglich melden und hierbei zumindest folgende Informationen mitteilen:

- Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,
- Name und Kontaktdaten von Kontaktpersonen für weitere Informationen,
- Beschreibung der wahrscheinlichen Folgen der Verletzung sowie
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

§ 10 Beendigung des Auftrags

(1) Mit Beendigung der Auftragsverarbeitung hat der Auftragsverarbeiter alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht, dies gilt auch für etwaige Sicherungskopien nach Maßgabe der getroffenen technischen und organisatorischen Maßnahmen. Die Löschung hat der Auftragsverarbeiter dem Verantwortlichen in Textform anzuzeigen.

(2) Der Verantwortliche kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragsverarbeiter einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Verantwortlichen aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

(3) Der Auftragsverarbeiter kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Verantwortliche auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragsverarbeiter den Verantwortlichen darüber in Kenntnis gesetzt hat.

§ 11 Beitritt zum Vertrag

Diesem Vertrag können mit Zustimmung aller Parteien über eine Beitrittserklärung jederzeit weitere Parteien als Verantwortliche oder als Auftragsverarbeiter beitreten. Zusätzlich zur Beitrittserklärung sind – soweit erforderlich – die Anhänge 1 bis 3 auszufüllen. Ab dem Zeitpunkt des Beitritts gelten die beitretenden Parteien als Vertragsparteien dieses Vertrags mit den entsprechend ihrer Bezeichnung bestehenden Rechten und Pflichten.

§ 12 Schlussbestimmungen

(1) Sollte das Eigentum des Verantwortlichen bei dem Auftragsverarbeiter durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Verantwortlichen ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(3) Im Falle eines Widerspruchs zwischen diesen Vertragsklauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

_____ _____

Ort, Datum Auftragsverarbeiter

_____

Schulische/r Datenschutzbeauftragte/r

_____

Schulleitung

Anhang 1

Auflistung der beauftragten Dienstleistungen und Kontaktdaten der Datenschutzbeauftragten

Gegenstand der Verarbeitung	Nutzung der Lernplattform 'Digitale Drehtür Campus' durch Lehrkräfte und Schülerinnen sowie Schüler.
Art und Zweck der Verarbeitung	Die Digitale Drehtür verarbeitet personenbezogene Daten, insofern diese zur Funktionalität der Lernplattform beiträgt. Folgend möchten wir den Zweck und die Funktionsweise der Plattform näher erläutern: ● Um den Digitalen Drehtür Campus nutzen zu können, muss eine Anmeldung durch die Schule erfolgen. Dafür müssen personenbezogene Daten an uns übermittelt werden (Name, Vorname, Mailadresse etc.). ● Eine registrierte Partnerschule erhält einen individuellen Registrierungslink, der mit den teilnehmenden Schülern und Schülerinnen geteilt wird. Dieser Registrierungslink enthält den Namen und den Ort der Schule. Über diesen Link kommen die Schüler und Schülerinnen sowie die Lehrkräfte auf eine Maske, in der sie ein Login festsetzen (Mailadresse und Passwort). Im Anschluss wird eine Bestätigungsmail mit einem Link versendet, der zu einer Registrierungsmaske führt. In diese Maske müssen die erforderlichen Daten (Name, Geburtstag, Klassenstufe, Geschlecht etc.) eingegeben werden. ● Nach erfolgreicher Registrierung können die Teilnehmenden auf die Lernplattform zugreifen und sich zu den Lernangeboten anmelden. Die Lernangebote bestehen aus Live-Kursen, Selbstlernkursen und hybriden Kursen (Live- und Selbstlernanteil). ● Die Teilnahme an Live-Kursen wird über die Videokonferenzplattform 'BigBlueButton' realisiert. Die Schüler und Schülerinnen treffen sich mit einem Kursleitenden und bearbeiten gemeinsam ein Thema. Haben die Teilnehmenden an einem Live-Kurs erfolgreich teilgenommen, können sie über eine Mail eine Teilnahmebescheinigung anfordern. Diese wird per Mail zugesendet. Vor Beginn des Kurses erhalten die Kursleiter eine verschlüsselte Datei mit der Anmeldeliste, damit diese kontrollieren können, dass wirklich nur die Lernenden anwesend sind. ● Die Selbstlernkurse bestehen aus interaktiven H5P-Elementen und Einbindungen von Links, Videos, Bildern oder ganzen Kursinhalten Dritter. ● Zukünftig sollen die Teilnahmebescheinigung durch "Kompetenzzertifikate" von 'Open Badges' ersetzt und in die Plattform integriert werden. Jedem Kurs werden Kompetenzen zugeordnet, die mit Abschluss der Kurse von den Lernenden erworben werden. Diese werden auf dem Campus dem Schüler und der Schülerin angezeigt.

	● Zur optimalen Nutzung der Plattform müssen die personenbezogenen Daten verwaltet und überprüft werden. ● Zur Evaluation oder zu Forschungszwecken können Daten in pseudonymisierter oder anonymisierter Form verarbeitet werden. ● Zum Zwecke der Einsicht über die Aktivitäten und Überprüfung können Lehrkräfte über ein Dashboard die personenbezogenen Daten der Lernenden ihrer Schule einsehen.
Art der personenbezogenen Daten	● Vor- und Nachnamen ● Mailadresse ● Geburtsdatum ● Geschlecht ● Bundesland des Wohnortes ● Schulname, ● Klassenstufe, ● ggf. Bilddaten (falls ein Bild hochgeladen wird)
Kategorien betroffener Personen	● Lehrkräfte ● Schüler:/innen ● Kursleitende ● Mitarbeitende aus Landesinstituten, Universitäten und Ministerien
Dauer der Verarbeitung	Entspricht der Dauer des Hauptvertrages (Registrierung zur/ Abmeldung von der Digitalen Drehtür).

Datenschutzbeauftragte/r des Auftragsverarbeiters	Datenschutz nord GmbH, Konsul-Smidt-Straße 88, 28217 Bremen

Anhang 2

Löschfristen

Datenart	Verwendungszweck	Löschfrist
Kontaktdaten der Schule	Kommunikation	● 6 Monate nach Vertragsende ● Nach der Abmeldung von der Digitalen Drehtür
Registrierungsdaten (bei Inaktivität)	Kommunikation, Nutzung der Plattform, Forschung, Evaluation	7 Monate
Registrierungsdaten	Kommunikation, Nutzung der Plattform, Forschung, Evaluation	Mit der Löschung des Kontos vom Digitalen Drehtür Campus
Rechnungsdaten	Rechnungen verschicken, Kommunikation	10 Jahre
Arbeitserzeugnisse der Lernenden		● Immer zum Stichtag 31.07. / Ende des Schuljahres (Umsetzung ab 2026) ● Mit der Löschung des Kontos von dem Digitalen Drehtür Campus
Login-Daten (Registrierung nicht zu Ende geführt)	Kommunikation und Nutzung der Plattform	6 Monate

Anhang 3

Liste der beauftragten Unterauftragnehmer einschließlich der Verarbeitungsstandorte

UNTERAUFTRAGNEHMER	VERARBEITUNGS-STANDORT	BESCHREIBUNG DER VERARBEITUNG
Kiron Digital Learning Solutions GmbH	Impact Hub Berlin, Rollbergstraße 28 A, 12053 Berlin	● Betreiber der Plattform, auf die der 'Digitale Drehtür Campus' läuft. Die Wartung und Entwicklung der Plattform wird seitens Kiron umgesetzt. ● Es werden die Daten der Menschen verarbeitet, die sich auf der Plattform registrieren. ● Kiron nutzt für die Server den Dienst "SysEleven" (siehe Anlage 3). Die Zertifizierung für den BSI-Grundschutz steht kurz vor dem Abschluss.
IONOS SE	Eigendorfer Str. 57, 56410 Montabaur,	● Versenden und Empfangen von E-Mails (bspw. bei Problemen, Einladungen etc.). ● Hosting der Webseite „Digitale Drehtür": Daten werden zur korrekten Darstellung und Funktion der Webseite verarbeitet. Zudem können sich interessierte Schulen, Schüler und Kursleitungen per Kontaktformular an uns wenden. Dort geben sie die jeweils erforderlichen Daten an (bspw. Name, E-Mail). ● Newsletterversand: Nach einer Anmeldung mit einem Double-Opt-In-Verfahren wird die Mailadresse als Zieladresse von Newsletter verarbeitet.
Invokable GmbH	Kratzberger Str. 9, 42855 Remscheid,	● Nutzung des Videokonferenzsystem „BigBlueButton" für Live-Kurse und Live-Meetings bspw. für Projekte. ● Die Lernenden klicken auf den hinterlegten Link auf der Plattform und werden dann zum entsprechenden Videokonferenzraum weitergeleitet. ● Es werden der Name, Audiodateien, Videodaten (Webcam-Bild, Screenshare) und Chat-Nachrichten verarbeitet. Die Speicherung der Daten ist temporär und wird nach Ende der Konferenz gelöscht.
Enuvo GmbH	Huobstrasse 10, 8808 Pfäffikon SZ, Schweiz	● Mit dem Tool 'Umfrageonline' werden Umfragen generiert, damit die Lernenden bspw. Feedback zu den Live-Kursen geben können. Auch können damit allgemein Umfragen mit Lernende, Lehrkräfte oder Kursleitende durchgeführt werden. ● Die Daten, die verarbeitet werden, werden größtenteils vom Auftragnehmer bestimmt (grundsätzlich sind die Umfragen anonym).
Stackfield GmbH	Maximilianplatz 17, 80333 München	● Stackfield ist ein Tool zur Arbeitsorganisation. ● Dort werden personenbezogene Daten gespeichert und verwaltet, um die Arbeit im Team zu ermöglichen. ○ Schülerdaten (bspw. Aufbewahrung von Teilnahmebescheinigungen), ○ Daten von Schulen bzw. Ansprechpersonen der Schulen (Mailadresse; Vor- und Nachname etc.).

Anhang 4

Liste der Subdienstleister

SUBDIENSTLEISTER	VERARBEITUNGS-STANDORT	BESCHREIBUNG DER VERARBEITUNG
Philipps-Universität Marburg (betrifft nur hessische Schüler)	Biegenstraße 10, 35037 Marburg	• Die Forschenden stellen Live-Kurse, Selbstlernkurse oder hybride Kurse zu bestimmten Themen ihres Fachbereichs zur Verfügung. Darüber hinaus hat die Universität Marburg noch ein Empfehlungstool gebaut, welches den Lernenden nach Beantwortung von Fragen, Empfehlungen für ihre Kurse gibt. Um die folgenden Forschungsvorhaben umzusetzen: • Evaluation des Empfehlungstools • Evaluation der selbst erstellten Kurse erhalten die Forschenden Daten in pseudonymisierter Form über einen Datenexport und ein Dashboard (siehe Anhang 5).
Justus-Liebig-Universität Gießen (betrifft nur hessische Schüler)	Ludwigstraße 23, 35390 Gießen	• Die Forschenden stellen Live-Kurse, Selbstlernkurse oder hybride Kurse zu bestimmten Themen ihres Fachbereichs zur Verfügung. Um die folgenden Forschungsvorhaben umzusetzen: • Evaluation der selbst erstellten Kurse nach Fachbereichen erhalten die Forschenden Daten in pseudonymisierter Form über einen Datenexport und ein Dashboard (siehe Anhang 5).

Anhang 5

Technisch-organisatorische Maßnahmen zur IT--Sicherheit

A. Maßnahmen zur Sicherstellung der Vertraulichkeit und Integrität

1.	Zutrittskontrolle Serverräume (Kiron Digital Learning Solutions GmbH)
1.0	Werden personenbezogene Daten der Auftraggeberin auf Servern gespeichert, die von Ihnen oder etwaigen Dienstleistern betrieben werden? ☒ ja ☐ nein
	Wenn 1.0 nein: In diesem Fall müssen die weiteren Fragen zu A1 nicht beantwortet werden, sondern sogleich die Fragen ab A2. Auch die Fragen zu B1 und B2 entfallen.
1.1	Standort des Serverraums / Rechenzentrums (RZ). Rechenzentren in Berlin, Frankfurt am Main, Hamburg und Düsseldorf
1.2	Sind die personenbezogenen Daten auf mehr als einen Serverstandort bzw. Rechenzentrum verteilt (bspw. Backup-Server, Nutzung von Cloud-Dienstleistungen)? ☒ ja ☐ nein
1.3	*Falls 1.2 ja:* Machen Sie bitte die entsprechenden Standortangaben auch zu weiteren Servern. Die von Kiron genutzten Lösungen von SysEleven (Serverstandort: Frankfurt a.M. und Berlin) sind eigenständig betriebene Public-Cloud-Services. Diese erfüllen höchste Sicherheitsstandards: · Sie sind ISO 27001-zertifiziert sowie C5 Typ 1 testiert. · Die Zertifizierung nach dem BSI IT-Grundschutz steht kurz vor dem Abschluss. · Georedundanz kann durch mehrere Rechenzentrumsstandorte innerhalb Deutschlands gewährleistet werden. Es liegt jedoch in der Verantwortung von Kiron, diese Möglichkeit aktiv zu nutzen und in die eigene Sicherheitsstrategie zu integrieren.
1.4	Gelten die folgenden Angaben zu Zutrittskontroll-Maßnahmen für alle im Einsatz befindlichen Rechenzentrum- bzw. Serverstandorte? ☒ ja ☐ nein
1.5	*Falls 1.4 nein:* Beantworten Sie bitte die Fragen 1.6 bis 1.21 und B für weitere Rechenzentrum- bzw. Serverstandorte.
1.6	Hat der Serverraum Fenster? ☐ ja ☒ nein
1.7	*Wenn 1.6 ja:* Wie sind die Fenster vor Einbruch geschützt? ☐ vergittert ☐ alarmgesichert ☐ abschließbar ☐ gar nicht ☐ Sonstiges: <Andere Sicherungsmaßnahmen benennen>
1.8	Ist der Serverraum mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☒ ja ☐ nein
1.9	*Wenn 1.8 ja:* Wer wird informiert, wenn die EMA auslöst (Mehrfachantworten möglich)? ☒ beauftragter Wachdienst ☐ Administrator ☐ Leiter IT ☐ andere Stelle: <[Stelle], die informiert wird, bspw. Geschäftsführung>
1.10	Ist der Serverraum videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☒ ja, mit Bildaufzeichnung ☐ nein
1.11	*Wenn 1.10 ja, mit Bildaufzeichnung:* Wie lange werden die Bilddaten gespeichert? Frankfurt am Main: 72 Std volle Aufnahmen; 90 Tage Bewegungserkennung

1.12	Wie viele Personen haben Zutritt zum Serverraum und welche Funktionen haben diese inne? Anzahl der Personen: ca. 10 Funktion im Unternehmen: Zuständig für RZ Betrieb
1.13	Ist der Serverraum mit einem elektronischen Schließsystem versehen? ☒ ja ☐ nein, mit mechanischem Schloss
1.14	*Wenn 1.13 ja:* Welche Zutrittstechnik kommt zum Einsatz? ☒ RFID ☒ PIN ☐ Biometrie ☐ Sonstiges: <andere Zutrittstechnik>
1.15	*Wenn 1.13 ja:* Werden die Zutrittsrechte personifiziert vergeben? ☒ ja ☐ nein
1.16	*Wenn 1.13 ja:* Werden die Zutritte zum Raum im Zutrittssystem protokolliert? ☒ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche Zutritte ☐ ja, aber nur erfolglose Zutrittsversuche ☐ nein, das Schloss wird nur freigegeben oder nicht
1.17	*Wenn 1.16 ja:* Wie lange werden die Zutrittsdaten ungefähr gespeichert? Frankfurt am Main: 90 Tage Berlin: Zutrittsdaten zu den Serverräumen können über komplette Vertragslaufzeit abgerufen werden. Nach Beendigung des Vertragsverhältnisses werden die Daten noch 1 Jahr aufbewahrt.
1.18	*Wenn 1.13 nein:* Wie viele Schlüssel zum Serverraum existieren, wo werden diese aufbewahrt, wer gibt die Schlüssel aus? ☐ Anzahl Schlüssel: <Anzahl>. ☐ Aufbewahrungsort: <Ort> ☐ Ausgabestelle: <Stelle>
1.19	Aus welchem Material besteht die Zugangstür zum Serverraum? ☒ Stahl/Metall ☐ sonstiges Material
1.20	Wird der Serverraum neben seiner eigentlichen Funktion noch für andere Zwecke genutzt? ☐ ja ☒ nein
1.21	*Wenn 1.20 ja:* Was wird in dem Serverraum noch aufbewahrt? ☐ Telefonanlage ☐ Lagerung Büromaterial ☐ Lagerung Akten ☐ Archiv ☐ Lagerung von IT-Ausstattung ☐ Sonstiges: <Sonstiges>
2.	ZUTRITTSKONTROLLMASSNAHMEN ZU BÜRORÄUMEN
2.1	Standort der Clientarbeitsplätze, von denen auf personenbezogene Daten zugegriffen wird: Landesinstitut Schule Bremen, Am Weidedamm 20, 28215 Bremen, Raum C 06 & von dem jeweiligen zu Hause des Mitarbeiters, falls Home-Office vereinbart.
2.2	Existiert ein Pförtnerdienst bzw. ständig besetzter Empfangsbereich zum Gebäude bzw. zu Ihren Büros? ☐ ja ☒ nein
2.3	Wird ein Besucherbuch geführt? ☐ ja ☒ nein
2.4	Ist das Gebäude oder sind die Büroräume mittels einer Einbruchmeldeanlage (EMA) alarmgesichert? ☒ ja ☐ nein
2.5	*Wenn 2.4 ja:* Wer wird informiert, wenn die EMA auslöst? ☐ beauftragter Wachdienst ☒ Administrator ☐ Leiter IT ☐ Sonstiges: <Stelle>
2.6	Werden das Bürogebäude bzw. seine Zugänge videoüberwacht? ☐ ja, ohne Bildaufzeichnung ☐ ja, mit Bildaufzeichnung ☒ nein

2.7	*Wenn 2.6 ja (mit Bildaufzeichnung):* Wie lange werden die Bilddaten gespeichert? <Speicherdauer in Tagen> Tage
2.8	Ist das Gebäude bzw. sind die Büroräume mit einem elektronischen Schließsystem versehen? ☐ ja, Gebäude und Büroräume sind elektronisch verschlossen ☐ ja, aber nur das Gebäude, nicht der Eingang zu den Büros bzw. zur Büroetage ☐ ja, aber nur der Eingang zu den Büros bzw. zur Büroetage, nicht das Gebäude insgesamt ☒ nein
2.9	*Wenn 2.8 ja:* Welche Zutrittstechnik kommt zum Einsatz? ☐ RFID ☐ PIN ☐ Biometrie ☐ Sonstiges: <Zutrittstechnik>
2.10	*Wenn 2.8 ja:* Werden die Zutrittsrechte personifiziert vergeben? ☐ ja ☐ nein
2.11	*Wenn 2.8 ja:* Werden die Zutritte im Zutrittssystem protokolliert? ☐ ja, sowohl erfolgreiche als auch erfolglose Zutrittsversuche ☐ ja, aber nur erfolgreiche Zutritte ☐ ja, aber nur erfolglose Zutrittsversuche ☐ nein, das Schloss wird nur freigegeben oder nicht
2.12	*Wenn 2.11 ja:* Wie lange werden diese Protokolldaten aufbewahrt? <Aufbewahrungsdauer> Tage
2.13	*Wenn 2.11 ja:* Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich
2.14	Existiert ein mechanisches Schloss für die Gebäude bzw. die Büroräume? ☒ ja ☐ nein
2.15	*Wenn 2.14 ja:* Wird die Schlüsselausgabe protokolliert, wer gibt die Schlüssel aus? ☒ ja, Ausgabestelle: Zentrale Dienste Leitung Gebäude- und Umweltmanagement, Innerer Dienst ☐ nein
2.16	Gibt es offizielle Zutrittsregelungen für betriebsfremde Personen (bspw. Besucher) zu den Büroräumen? ☒ nein ☐ ja, betriebsfremde Personen werden am Eingang bzw. Empfang vom Ansprechpartner abgeholt und dürfen sich im Gebäude nur begleitet bewegen.
3.	ZUGANGS- UND ZUGRIFFSKONTROLLMASSNAHMEN
3.1	Existiert ein Prozess zur Vergabe von Benutzerkennungen und Zugriffsberechtigungen bei der Neueinstellung und beim Ausscheiden von Mitarbeitern bzw. bei organisatorischen Veränderungen? ☒ definierter Freigabeprozess ☐ kein definierter Freigabeprozess, auf Zuruf ☐ Sonstige Vergabeweise: <Verfahren>
3.2	Werden die Vergabe bzw. Änderungen von Zugriffsberechtigungen protokolliert? ☒ ja ☐ nein
3.3	Authentisieren sich die Mitarbeiter über eine individuelle Kennung gegenüber dem zentralen Verzeichnisdienst? ☒ ja ☐ nein
3.4	Existieren verbindliche Passwortparameter im Unternehmen? ☒ ja ☐ nein

3.5	Passwort-Zeichenlänge: mind. 12 Zeichen Muss das Passwort Sonderzeichen enthalten? ☒ ja ☐ nein Mindest-Gültigkeitsdauer in Tagen: 30
3.6	Zwingt das IT-System den Nutzer zur Einhaltung der oben genannten Passwort-Vorgaben? ☐ ja ☒ nein
3.7	Wird der Bildschirm bei Inaktivität des Benutzers gesperrt? Ja Wenn ja, nach wieviel Minuten? 5 Minuten
3.8	Welche Maßnahmen ergreifen Sie bei Verlust, Vergessen oder Ausspähen eines Passworts? ☒ Administrator vergibt neues Initialpasswort ☐ keine
3.9	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen? ☒ ja ☐ nein
3.10	*Wenn 3.9 ja:* Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht wurde? ☒ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☐ Die Zugänge bleiben für ‹Dauer der Sperre› Minuten gesperrt.
3.11	Wie erfolgt die Authentisierung bei Fernzugängen? Authentisierung mit ☐ Token ☒ VPN-Zertifikat ☐ Passwort
3.12	Gibt es eine Begrenzung von erfolglosen Anmeldeversuchen bei Fernzugängen? ☐ ja, ‹Anzahl Anmeldeversuche› Versuche ☒ nein
3.13	*Wenn 3.12 ja:* Wie lange bleiben Zugänge gesperrt, wenn die maximale Zahl erfolgloser Anmeldeversuche erreicht worden ist? ☐ Die Zugänge bleiben bis zur manuellen Aufhebung der Sperre gesperrt ☐ Die Zugänge bleiben für ‹Dauer in Minuten› Minuten gesperrt.
3.14	Wird der Fernzugang nach einer gewissen Zeit der Inaktivität automatisch getrennt? ☐ ja, nach ‹Dauer in Minuten› Minuten ☒ nein
3.15	Werden die Systeme, auf denen personenbezogene Daten verarbeitet werden, über eine Firewall abgesichert? ☒ ja ☐ nein
3.16	*Wenn 3.15 ja:* Wird die Firewall regelmäßig upgedatet? ☒ ja ☐ nein
3.17	*Wenn 3.15 ja:* Wer administriert Ihre Firewall? ☐ eigene IT ☒ Externer Dienstleister
3.18	*Wenn ein externer Dienstleister zum Einsatz kommt:* Kann sich dieser ohne Aufsicht durch Ihre IT auf die Firewall aufschalten? ☒ ja ☐ nein, die Aufschaltung ist nur im Vier-Augen-Prinzip mit einem Mitarbeiter der eigenen IT möglich.
4.	MASSNAHMEN ZUR SICHERUNG VON PAPIER-UNTERLAGEN, MOBILEN DATENTRÄGERN UND MOBILEN ENDGERÄTEN
4.1	Wie werden nicht mehr benötigte Papier-Unterlagen mit personenbezogenen Daten (bspw. Ausdrucke, Akten, Schriftwechsel) entsorgt? ☐ Altpapier / Restmüll ☒ Es stehen hierfür Schredder zur Verfügung, deren Nutzung angewiesen ist ☐ Es sind verschlossene Datentonnen aufgestellt, die von einem Entsorgungsdienstleister zur datenschutzkonformen Vernichtung abgeholt werden ☐ Sonstiges: ‹Art der Entsorgung›

4.2	Wie werden nicht mehr benötigte Datenträger (z.B. USB-Sticks, Festplatten), auf denen personenbezogene Daten gespeichert sind, entsorgt? ☐ Physische Zerstörung durch eigene IT ☐ Physische Zerstörung durch externen Dienstleister ☒ Löschen der Daten ☐ Löschen der Daten durch <Anzahl> Überschreibungen ☐ Sonstiges: <Art der Entsorgung>
4.3	Dürfen im Unternehmen mobile Datenträger verwendet werden (z.B. USB-Sticks) ☒ ja ☐ nein
4.4	Dürfen die Mitarbeiter private Datenträger (z.B. USB-Sticks) verwenden? ☐ generell ja ☐ ja, aber nur nach Genehmigung und Überprüfung des Speichermediums durch die IT ☒ nein, alle benötigten Speichermedien werden vom Unternehmen gestellt
4.5	Werden personenbezogene Daten auf mobilen Endgeräten verschlüsselt? ☐ Verschlüsselung der Festplatte ☒ Verschlüsselung einzelner Verzeichnisse ☐ keine Maßnahmen
4.6	Verarbeiten Mitarbeiter personenbezogene Daten auch auf eigenen privaten Geräten (bring your own device)? ☒ ja ☐ nein
5.	MASSNAHMEN ZUR SICHEREN DATENÜBERTRAGUNG
5.1	Erfolgt der Transfer personenbezogener Daten durchgängig verschlüsselt? ☐ gar nicht ☐ nein, Datenübertragung erfolgt per MPLS ☐ nur vereinzelt ☐ per verschlüsselter Datei als Mailanhang ☐ per PGP oder S/MIME ☐ per verschlüsseltem Datenträger ☐ per VPN ☒ per https/TLS ☐ per SFTP ☐ Sonstiges: <Art der Verschlüsselung>
5.2	Wer verwaltet die Schlüssel bzw. die Zertifikate? ☒ Anwender selbst ☐ eigene IT ☐ Externer Dienstleister
5.3	Werden die Übertragungsvorgänge protokolliert? ☐ ja ☒ nein
5.4	*Wenn 5.3 ja:* Wie lange werden diese Protokolldaten aufbewahrt? <Dauer in Tagen> Tage
5.5	*Wenn 5.3 ja:* Werden die Protokolle regelmäßig ausgewertet? ☐ ja ☐ nein, eine Auswertung wäre aber im Bedarfsfall möglich

B. Maßnahmen zur Sicherstellung der Verfügbarkeit

1.	SERVERAUM (Kiron Digital Learning Solutions GmbH)
1.1	Verfügt der Serverraum über eine feuerfeste bzw. feuerhemmende Zugangstür? ☒ ja ☐ nein
1.2	Ist der Serverraum mit Rauchmeldern ausgestattet? ☒ja ☐ nein
1.3	Ist der Serverraum an eine Brandmeldezentrale angeschlossen? ☒ ja ☐ nein

1.4	Ist der Serverraum mit Löschsystemen ausgestattet (Mehrfachantworten möglich)? ☒ ja, CO2 Löscher ☒ ja, Halon-/Argon-Löschanlage ☐ Sonstiges: ‹Art des Löschsystems›
1.5	Woraus bestehen die Außenwände des Serverraumes? ☒ Massivwand (bspw. Beton, Mauer) ☐ Leichtbauweise ☐ Brandschutzwand (bspw. F90)
1.6	Ist der Serverraum klimatisiert? ☒ja ☐ nein
1.7	Verfügt der Serverraum über eine unterbrechungsfreie Stromversorgung (USV)? ☒ ja ☐ nein
1.8	Wird die Stromversorgung des Serverraums zusätzlich über ein Dieselaggregat abgesichert? ☒ ja ☐ nein
1.9	Werden die Funktionalitäten unter 1.2, 1.3, 1.4, 1.6, 1.7 und 1.8 – sofern vorhanden – regelmäßig getestet? ☒ ja ☐ nein
2.	BACKUP- UND NOTFALL-KONZEPT, VIRENSCHUTZ (Kiron Digital Learning Solutions GmbH)
2.1	Existiert ein Backupkonzept? ☒ ja ☐ nein
2.2	Wird die Funktionalität der Backup-Wiederherstellung regelmäßig getestet? ☒ ja ☐ nein
2.3	In welchem Rhythmus werden Backups von Systemen angefertigt, auf denen personenbezogene Daten gespeichert werden? ☐ Echtzeitspiegelung ☐ täglich ☐ ein bis dreimal pro Woche ☒ Sonstiges: 7 tägliche, 4 wöchentliche und 3 monatliche
2.4	Auf was für Sicherungsmedien werden die Backups gespeichert? ☒ Zweiter redundanter Server ☐ Sicherungsbänder ☐ Festplatten ☐ Sonstiges: ‹Art des Backups›
2.5	Wo werden die Backups aufbewahrt? ☒ Zweiter redundanter Server steht an einem anderen Ort ☐ Safe, feuerfest, datenträger- und dokumentensicher ☐ einfacher Safe ☐ Bankschließfach ☐ abgeschlossener Aktenschrank/Schreibtisch ☐ im Serverraum ☐ Privathaushalt ☐ Sonstiges: ‹Art der Aufbewahrung›
2.6	*Zu 2.5:* Im Falle eines Transports der Backups: Wie wird dieser durchgeführt? ☒ Mitnahme durch einen Mitarbeitenden der IT-Abteilung, Geschäftsführung, Sekretariat ☐ Abholung durch Dritte (bspw. Bankmitarbeitende, Wachunternehmen) ☐ Sonstiges: ‹Art des Backups›
2.7	Sind die Backups verschlüsselt? ☐ ja ☒ nein
2.8	Befindet sich der Aufbewahrungsort der Backups in einem, vom primären Server aus betrachtet, getrennten Brandabschnitt bzw. Gebäudeteil? ☒ ja ☐ nein
2.9	Existiert ein dokumentierter Prozess zum Software- bzw. Patchmanagement? ☒ ja ☐ nein ☐ Prozess existiert, ist jedoch nicht dokumentiert

2.10	*Wenn 2.9 ja:* Wer ist für das Software- bzw. Patchmanagement verantwortlich? ☐ Anwender selbst ☐ eigene IT ☒ Externer Dienstleister
2.11	Existiert ein Notfallkonzept (bspw. Notfallmaßnahmen bei Hardwaredefekten, Brand oder Totalverlust)? ☒ ja ☐ nein
2.12	Sind die IT-Systeme technisch vor Datenverlusten bzw. unbefugten Datenzugriffen geschützt? ☒ ja. Es wird eine "kubernete Infrastruktur" verwendet. Zu den Sicherheitsvorkehrungen gehören: ● Image Signing zur Sicherstellung der Unveränderbarkeit (Immutability) der verwendeten Container Images ● CVE-Scans der verwendeten Images (zur Build Zeit sowie automatisiert täglich) ● Secret Scans zur Prevention von Secret Leaks ● Trennung der Systeme durch VPCs (Virtual Private Clouds), kein Zugriff auf die Systeme von außerhalb des Clusters möglich ● Absicherung des eingehenden Public Traffics durch einen Reverse Proxy (Ingress NGINX) inkl. OWASP Firewall und – je nach Komponente – aktivierter „OWASP Top 10 Rules" und Rate Limits ● Einsatz von Observability Tools zur Echtzeit Überwachung der Systeme und Anomalie Detection ☐ nein
2.13	*Wenn 2.12 ja:* Wer ist für den aktuellen Virenschutz, Anti-Spyware und Spamfilter verantwortlich? ☐ Anwender selbst ☐ eigene IT ☒ Externer Dienstleister
3.	NETZANBINDUNG
3.1	Verfügt das Unternehmen über eine redundante Internetanbindung? ☒ ja ☐ nein
3.2	Sind die einzelnen Standorte des Unternehmens redundant miteinander verbunden? ☒ ja ☐ nein
3.3	Wer ist für die Netzanbindung des Unternehmens verantwortlich? ☐ eigene IT ☒ Externer Dienstleister

C. Pseudonymisierung / Verschlüsselung

1.	Einsatz von Pseudonymisierung (Kiron Digital Learning Solutions GmbH)
1.1	Werden verarbeitete personenbezogene Daten pseudonymisiert? ☒ ja, und zwar folgende: ● User-ID (gehasht) ● Schulname (ID wird vergeben und angezeigt) ● Geburtsdatum (Auf das Geburtsjahr reduziert) ☐ nein

1.2	Zwecke der Verarbeitung der pseudonymisierten Daten: ● Zur Planung, Entwicklung, Gestaltung, Durchführung und Auswertung der online bereitgestellten Informations-/Beratungs- und Lernangebote und -veranstaltungen sowie von Austauschformaten, ● Zur Erstellung, Bereitstellung und Weiterentwicklung von onlinebasierten Lernmaterialien, ● Zur Bereitstellung von individuellen Lernempfehlungen sowie Rückmeldungen zu lernrelevanten Kompetenzen und Präferenzen an die Schülerinnen und Schüler und deren Lehrkräfte, ● Zur Erfassung von Lernfortschritten ● Zur digitalen Kommunikation zwischen Lernenden und Kursleitenden/ Lehrenden/ Gastreferentinnen und Gastreferenten/ Projektmitarbeiterinnen und Projektmitarbeitern, ● Zur Information von und Kommunikation mit Erziehungsberechtigten ● Zur Lernstandskontrolle bzw. zur Erfassung von Lernfortschritten und der Erteilung fachlicher Rückmeldungen, ● Zu Schulungszwecken der Mitarbeiterinnen und Mitarbeiter, ● Evaluation und wissenschaftlichen Begleitung der Digitalen Drehtür sowie einzelner Angebote hieraus und der (Nach-)Nutzung zu wissenschaftlichen Zwecken.
2.	EINSATZ VON VERSCHLÜSSELUNG **(Kiron Digital Learning Solutions GmbH)**
2.1	Werden verarbeitete personenbezogene Daten über die bereits beschriebenen Maßnahmen hinaus verschlüsselt? ☒ ja, und zwar: Alle. ☐ nein
	Wenn 2.1 nein: In diesem Fall müssen die weiteren Fragen zu C2 nicht beantwortet werden, sondern sogleich die Fragen ab D1.
2.2	Welche Arten der Verschlüsselung werden eingesetzt (Mehrfachantworten möglich)? Bei Mehrfachantworten beschreiben Sie bitte im Feld „Sonstige“, welche Art der Verschlüsselung für welche Daten eingesetzt wird. ☒ Ende-zu-Ende-Verschlüsselung ☒ Transportverschlüsselung ☒ Data-at-Rest-Verschlüsselung ☐ Sonstige: <Art der Verschlüsselung>
2.3	Welche kryptographischen Algorithmen werden zur Verschlüsselung oder für verschlüsselungsartige Maßnahmen (z.B. Hashen von Passwörtern) eingesetzt? ☒ AES ☒ SHA-256 ☒ RSA-2048 oder höher ☐ Sonstige: <Algorithmus>
2.4	Wer hat Zugriff auf die verschlüsselten Daten? Mitarbeitende aus den Abteilungen: Need-to-know-Prinzip Insgesamt haben wenige Mitarbeitende Zugriff auf die verschlüsselten Daten

D. Sonstige Maßnahmen

1.	Belastbarkeit (Kiron Digital Learning Solutions GmbH)
	Es existieren Maßnahmen, die die Fähigkeit gewährleisten, die Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. ☒ ja, ausreichende Kapazitäten sind vorhanden ☐ nein
2.	WIEDERHERSTELLBARKEIT **(Kiron Digital Learning Solutions GmbH)**
	Existieren Notfall- oder Recovery-Konzepte und Maßnahmen über B.2.11 hinaus, die die Fähigkeit gewährleisten, die Verfügbarkeit der personenbezogenen Daten und den

	Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen? ☒ ja, die regelmäßig durchgeführten Backups ermöglichen die vollständige Wiederherstellung einzelner Komponenten sowie – bei Bedarf – der kompletten Infrastruktur. Backups werden proaktiv überwacht und im Falle von fehlgeschlagenen Backups im Observability erkannt und über Alerts an die verantwortlichen Personen gemeldet. Es bestehen Desaster Recovery Pläne, mit denen einzelne Komponenten sowie die gesamte Infrastruktur innerhalb von wenigen Minuten wieder hergestellt werden kann. Sollte es einen Ausfall der SysEleven Compute-Infrastruktur geben, so kann die komplette Software über einen Restore der Backups auf einem anderen Provider (z.B. Azure, AWS, Google, etc.) neu gestartet werden. Es werden regelmäßig Tests zur Sicherstellung der Backup Funktionen durchgeführt („Red Cards"), um im tatsächlichen Fehlerfall schnell reagieren zu können. ☐ nein
3.	VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG DER GETROFFENEN MASSNAHMEN **(Kiron Digital Learning Solutions GmbH)**
3.1	Existiert ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung? ☒ ja, es wird ein funktionierendes ISMS betrieben ☐ nein
3.2	*Wenn 3.1 ja:* In welchen Abständen finden die Überprüfungen statt? Zeitraum: Permanent
3.3	*Wenn 3.1 ja:* Werden die Ergebnisse der Prüfungen dokumentiert? ☒ ja ☐ nein
3.4	Gibt es Zertifizierungen mit Bezug zu den technisch-organisatorischen Maßnahmen und wenn ja, welche? ☐ ja, <Art der Zertifizierung/en> ☒ nein

E. Externe Verlinkungen und Einbettungen

1.	VERLINKUNGEN ZU EXTERNEN Dritten
	Externe Verlinkungen auf der vom Auftragsverarbeiter betriebenen Webseite werden regelmäßig hinsichtlich ihrer Vertrauenswürdigkeit geprüft. Es wird sichergestellt, dass keine ungewollte Weitergabe personenbezogener Daten durch automatische Verbindungen zu Drittanbietern erfolgt. Externe Links sind entsprechend gekennzeichnet.
2.	Prüfung
	Der Auftragsverarbeiter weist die Ersteller und Erstellerinnen von Kursen an, dass Seiten, die per Link eingebunden oder eingebettet werden sollen, vorab nach Maßgabe interner Kriterien geprüft werden müssen. Die Einbettung von Videos erfolgt im erweiterten Datenschutzmodus; die Anschaffung einer Lizenz ist in Planung.
3.	Maßnahmen
	Damit die Lernenden die externe Verlinkung erkennen, ist diese durch einen Disclaimer gekennzeichnet: "Wenn du auf diesen Link klickst, verlässt du den Digitalen Drehtür Campus. Dort kann es sein, dass persönliche Daten wie deine IP-Adresse gesammelt werden. Darauf haben wir keinen Einfluss. Bitte schau dir die Datenschutzinfos der anderen Seite an."
4.	Verlinkungen als Beispiel
	• IQ-Test: Wie schlau bist du? - [GEOLINO] • Herzmuschel

- Austernfischer – Nationalpark Wattenmeer