

Auftragsverarbeitungsvertrag

zwischen

als Verantwortlicher (nachfolgend „**Verantwortlicher**“),

und

Scobees GmbH, Neusser Str. 5-7, 50670 Köln

als Auftragsverarbeiter (nachfolgend „**Auftragsverarbeiter**“,
Verantwortlicher und Auftragsverarbeiter gemeinsam die „**Parteien**“)

Fassung für Hessen in der Version zum 01.06.2025

Präambel

Der Verantwortliche hat den Auftragsverarbeiter im bereits geschlossenen Vertrag (nachfolgend „Hauptvertrag“) zu den dort genannten Leistungen beauftragt. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten im Rahmen der Bereitstellung des Lernsystems Scobees. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien den nachfolgenden Auftragsverarbeitungsvertrag (nachfolgend die „Vereinbarung“), dessen Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist.

Der Vertrag wurde in der o.g. Fassung inhaltlich im Rahmen einer Folgeabschätzung mit dem Bereich Datenschutz des Kooperationsverbundes Süd der Staatlichen Schulämter in Hessen abgestimmt, so dass alle Zwecke dieser Cloud-Online-Anwendung und Subunternehmer des Anbieters im Bezug zu den Landesvorschriften vollständig aufgeführt wurden. Dies bedeutet keine Bestätigung der Datenschutzkonformität. Wenn Zwecke und Subunternehmer sich ändern, erlischt der Vertrag und muss neu abgestimmt werden.

§ 0

Der Auftragsverarbeitungsvertrag ist in der Fassung für Hessen abgestimmt mit dem Bereich: Datenschutz im Verbund Süd der Staatlichen Schulämter Wiesbaden, Rüsselsheim, Darmstadt und Heppenheim.

§ 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

„**Betroffener**“) 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 personenbezogene 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, biometrische 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, der 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 Vertragsgegenstand

(1) Das Lernsystem Scobees ist ein digitales Tool für Schulen, das individualisiertes und selbstgesteuertes Lernen unterstützt, mit dem in einem digitalen Lerntagebuch der Lernstand und Lernerfolg der Lernenden dokumentiert wird. Das Scobees-Lernsystem bietet separate Bereiche für Lehrkräfte, Lernende und optional für Erziehungsberechtigte, in denen Lehrkräfte Lernmaterialien bereitstellen und

bewerten, Lernende darauf zugreifen und ihre Aufgaben einreichen können, und Erziehungsberechtigte freigegebene Inhalte einsehen dürfen.

Pädagogische Lernangebote zu den Schwerpunkten Deutsch, Mathematik, Englisch für die Sekundarstufe I und die Jahrgangsstufe 4 der Grundschulen. Das Scobees Lernsystem besteht aus folgenden Modulen:

Das Scobees-Lernsystem besteht aus den folgenden Modulen:

1. **Bereich für Lehrkräfte:** Lehrkräfte können hier Lernmaterialien hochladen und ggf. freigeben, die Abgaben der Lernende bewerten und persönliches Feedback geben.
2. **Bereich für Lernende:** Lernende haben Zugriff auf die bereitgestellten Lernmaterialien und können ihre bearbeiteten Aufgaben einreichen.
3. **Bereich für Erziehungsberechtigte (optional):** Erziehungsberechtigte können hier die von den Lehrkräften freigegebenen Inhalte einsehen.

Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten, die der Auftragsverarbeiter für den Verantwortlichen ausschließlich im Auftrag und nach Weisung des Verantwortlichen verarbeitet. Umfang und Zweck der Datenverarbeitung durch den Auftragsverarbeiter ergeben sich aus dem Hauptvertrag und etwaigen zugehörigen Leistungsbeschreibungen. Dem Verantwortlichen 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 Hauptvertrags vor.

(3) Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei denen der Auftragsverarbeiter und seine Beschäftigten oder durch den Auftragsverarbeiter Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Verantwortlichen stammen oder für den Verantwortlichen erhoben wurden.

(4) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüber hinausgehende Verpflichtungen oder Kündigungsrechte ergeben.

(5) Wenn Scobees Funktionen oder Zwecke in dem Lernsystem ergänzt, die über diesen Vertrag hinausgehen, wird dies von Scobees an den Bereich Datenschutz im

Kooperationsverbund Süd vgl. §0 gemeldet. Ziel ist es im Rahmen der Folgeabschätzung einen neuen Vertrag abzuschließen. Sobald dies geschehen ist, erscheint der Vertrag in einer neuen Fassung.

§ 3 Weisungsrecht

(1) Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Verantwortlichen erheben, verarbeiten oder nutzen. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag festgelegt und können vom Verantwortlichen danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Verantwortliche ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung, Löschung und Sperrung von Daten.

(3) Alle erteilten Weisungen sind vom Verantwortlichen zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt.

(4) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung, so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 4 Löschfristen

(1) Die Löschung der Lernergebnis- und Bewertungsdaten findet am 01.09. jedes Jahres statt.

(2) Ferner werden personenbezogene Daten nach Weisung oder am Vertragsende gemäß § 12 gelöscht.

§ 5 Arten der verarbeiteten Daten, Kreis der Betroffenen, Drittland

(1) Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragsverarbeiter Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten.

(2) Der Kreis der von der Datenverarbeitung Betroffenen ist in **Anlage 1** dargestellt.

(3) Personenbezogene Daten werden grundsätzlich nicht in ein Drittland (außerhalb des EWR) übermittelt. Eine Übermittlung personenbezogener Daten in ein Drittland bedarf die ausdrückliche Zustimmung des Verantwortlichen und muss die Voraussetzungen der Art. 44 ff. DSGVO erfüllen.

§ 6 Schutzmaßnahmen des Auftragsverarbeiters

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

(2) Der Auftragsverarbeiter wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er hat die in **Anlage 2** genannten technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Verantwortlichen gem. Art. 32 DSGVO getroffen, die der Verantwortliche als angemessen anerkennt. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

(3) Den bei der Datenverarbeitung durch den Auftragsverarbeiter beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Der Auftragsverarbeiter wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (nachfolgend "**Mitarbeiter**"), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28

Abs. 3 lit. b DSGVO) und mit der gebotenen Sorgfalt die Einhaltung dieser Verpflichtung sicherstellen.

(4) Der Auftragsverarbeiter hat einen Datenschutzbeauftragten benannt. Der Datenschutzbeauftragte des Auftragsverarbeiters ist heyData GmbH, Schützenstr. 5, 10117 Berlin, datenschutz@heydata.eu, www.heydata.eu.

§ 7 Informationspflichten des Auftragsverarbeiters

(1) Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragsverarbeiters, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragsverarbeiter den Verantwortlichen unverzüglich informieren. Dasselbe gilt für Prüfungen des Auftragsverarbeiters 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 dem Auftragsverarbeiter ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen;
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.

(2) Der Auftragsverarbeiter trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der Betroffenen, informiert hierüber den Verantwortlichen und ersucht um weitere Weisungen.

(3) Der Auftragsverarbeiter ist darüber hinaus verpflichtet, dem Verantwortlichen jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz 1 betroffen sind.

(4) Über wesentliche Änderung der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragsverarbeiter den Verantwortlichen zu unterrichten.

§ 8 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche kann sich vor der Aufnahme der Datenverarbeitung und sodann jährlich von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Hierfür kann er z. B. Auskünfte des Auftragsverarbeiters einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen oder durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragsverarbeiter steht. Der Verantwortliche wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

(2) Der Auftragsverarbeiter verpflichtet sich, dem Verantwortlichen auf dessen 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 des Auftragsverarbeiters erforderlich sind.

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

§ 9 Einsatz von Dienstleistern

- (1) Die vertraglich vereinbarten Leistungen werden unter Einschaltung der in **Anlage 3** genannten Dienstleister (nachfolgend **„Unterauftragsverarbeiter“**) durchgeführt. Der Verantwortliche erteilt dem Auftragsverarbeiter seine allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 S. 1 DSGVO, im Rahmen seiner vertraglichen Verpflichtungen weitere Unterauftragsverarbeiter zu beauftragen oder bereits beauftragte zu ersetzen.
- (2) Der Auftragsverarbeiter wird den Verantwortlichen vor jeder beabsichtigten Änderung in Bezug auf die Hinzuziehung oder die Ersetzung eines Unterauftragsverarbeiters informieren. Der Verantwortliche muss jedem neuen Unterauftragsverarbeiter zustimmen.
- (3) Der Auftragsverarbeiter hat bei der Einschaltung von Unterauftragsverarbeitern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten.
- (4) Ein Unterauftragsverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragsverarbeiter 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 der Auftragsverarbeiter für den Verantwortlichen erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen zustimmungspflichtige Unterauftragsverhältnisse dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Verantwortlichen genutzt werden.
- (5) Eine Weitergabe personenbezogener Daten in ein Drittland (außerhalb des EWR) ist ausgeschlossen.

§ 10 Anfragen und Rechte Betroffener

- (1) Der Auftragsverarbeiter unterstützt den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art. 12–22 sowie 32 bis 36 DSGVO.
- (2) Macht ein Betroffener Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich seiner Daten, unmittelbar gegenüber dem Auftragsverarbeiter

geltend, so reagiert dieser nicht selbstständig, sondern verweist den Betroffenen an den Verantwortlichen und wartet dessen Weisungen ab.

§ 11 Haftung

(1) Die Parteien haften nach Maßgabe des Art. 82 DSGVO für Schäden, die einer betroffenen Person durch eine Verletzung der Datenschutz-Grundverordnung entstehen.

§ 12 Beendigung des Hauptvertrags

(1) Der Auftragsverarbeiter wird dem Verantwortlichen nach Beendigung des Hauptvertrags alle ihm überlassenen Unterlagen, Daten und Datenträger zurückgeben oder – auf Wunsch des Verantwortlichen, sofern nicht nach dem Unionsrecht oder anderem anwendbaren nationalen Recht eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragsverarbeiter. Der Auftragsverarbeiter hat den dokumentierten Nachweis der ordnungsgemäßen Löschung auf Anfrage zu führen.

(2) Der Verantwortliche hat das Recht, die vollständige und vertragsgerechte Rückgabe oder Löschung der Daten beim Auftragsverarbeiter in geeigneter Weise zu kontrollieren.

(3) Der Auftragsverarbeiter ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragsverarbeiter über personenbezogene Daten verfügt, die ihm vom Verantwortlichen zugeleitet wurden oder die er für diesen erhoben hat.

§ 13 Schlussbestimmungen

(1) Soweit der Auftragsverarbeiter Unterstützungshandlungen nach dieser Vereinbarung nicht ausdrücklich kostenlos durchführt, kann er dem Verantwortlichen dafür eine angemessene Gebühr in Rechnung stellen, es sei denn,

eigene Handlungen oder Unterlassungen des Auftragsverarbeiters haben diese Unterstützung unmittelbar erforderlich gemacht.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. 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.

Verantwortlicher

Name: _____

Position: _____

Datum: _____

Unterschrift: _____

Unterschrift des schulischen Datenschutzbeauftragten

Name: _____

Position: _____

Datum: _____

Unterschrift: _____

AuftragsverarbeiterName: Ann-Christin DoerflePosition: Co-FounderDatum: 01.06.2025Unterschrift: Annie Doerfle

Anlagen

Anlage 1 – Beschreibung der Verarbeitung

Verarbeitungstätigkeit	Kategorien von personenbezogenen Daten	Kategorie n von betroffene n Personen	Verarbeitungszweck e
Accounterstellung und -verifizierung (Module: Lehrkräfte, Erziehungsberechtigte)	Vor- und Nachname, E-Mail-Adresse, Passwort	Lehrkräfte, Erziehungsberechtigte	Identifizierung und Verifizierung der Benutzer
Accounterstellung und -verifizierung (Modul: Lernende)	Name oder Pseudonym, Passwort	Lernende	Identifizierung und Verifizierung der Benutzer
Erstellung und Änderung von Lerneinheiten (Modul: Lehrkräfte)	Datum und Art der Aktivität, Name der Lehrkraft	Lehrkräfte	Nachverfolgung und Anzeige von erstellten/veränderten Lerneinheiten

Erfassung und Anzeige von Lernfortschritten (Modul: Lernende)	Abschluss von Aufgaben und Teilaufgaben	Lernende	Erfassung und Anzeige des quantitativen Lernfortschritts, Löschung spätestens jährlich am 01.09. jedes Jahres
Hochladen und Speichern von Lernergebnissen und Selbstreflektionen (Modul: Lernende)	Lernergebnisse, Selbstreflektionen (Einschätzungen, Kommentare), Stimmung, Verhalten, Lernmaterialien	Lernende	Bereitstellung von Informationen für Lehrkräfte, Nachverfolgung des Lernerfolgs, Selbstbewertung, Löschung spätestens jährlich am 01.09. jedes Jahres
Feedback und Notizenerstellung (Modul: Lehrkräfte)	Feedback auf Lernergebnisse und Selbstreflektionen der Lernenden, Notizen, Kompetenzenbewertung, Stimmungsbewertung	Lehrkräfte, Lernende	Bereitstellung von Feedback für Lernende, Speicherung im Lerntagebuch, Beurteilung der Kompetenzen und Stimmungen der Lernenden; Löschung spätestens am 01.09. jedes Jahres

Verwaltung von Benutzerkonten und Einladung von Kollegen (Modul: Lehrkräfte)	Benutzername, Passwort, Name der Lehrkraft	Lehrkräfte	Verwaltung und Organisation der Lernumgebung, Zusammenarbeit mit Kollegen
Zugriff auf Lerninformationen des Kindes (Modul: Erziehungsberechtigte)	Lernfortschritt, Lernthemen, Benutzername, Passwort	Erziehungsberechtigte, Lernende	Beobachtung und Unterstützung des Lernprozesses des Kindes
Server-Logdaten (Module: Lernende, Lehrkräfte, Erziehungsberechtigte)	IP-Adresse, Datum und Uhrzeit der Anfrage, Inhalt der Anforderung (konkrete Seite), Zugriffsstatus/HTTP-Statuscode, jeweils übertragene Datenmenge, Website, von der die Anforderung kommt, Browser, Betriebssystem und dessen Oberfläche, Sprache und Version der Browsersoftware.	Alle Benutzer (Lehrkräfte, Lernende, Erziehungsberechtigte)	Gewährleistung eines reibungslosen Verbindungsaufbaus der Website, Gewährleistung einer komfortablen Nutzung unserer Website, Auswertung der Systemsicherheit und -stabilität sowie zu weiteren administrativen Zwecken

Bearbeitung von Support-Anfragen (Modul: je nach Support-Anfrage)	Die in der Supportanfrage angegebenen personenbezogene Daten.	Alle Benutzer (Lehrkräfte, Lernende, Erziehungsberechtigte)	Bearbeitung von Support-Anfragen und Behebung von Problemen.
---	---	--	--

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragsverarbeiters

1. Einleitung

Dieses Dokument fasst die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 Abs. 1 DSGVO zusammen. Das sind Maßnahmen, mit denen der Auftragsverarbeiter personenbezogene Daten schützt. Das Dokument hat den Zweck, den Verantwortlichen bei der Erfüllung seiner Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu unterstützen.

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

2.1. Zutrittskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zutritt zu den Datenverarbeitungsanlagen haben:

- Alarmanlage
- Automatisches Zugangskontrollsystem

- Lichtschranken / Bewegungsmelder
- Manuelles Schließsystem (z.B. Schlüssel)
- Schließsystem mit Codesperre
- Sicherheitsschlösser
- Videoüberwachung der Zugänge
- Klingelanlage mit Kamera
- Personenkontrolle beim Pförtner oder Empfang
- Protokollierung der Besucher (z.B. Besucherbuch)
- Schlüsselregelung / Schlüsselbuch
- Sorgfältige Auswahl von Sicherheitspersonal
- Tragepflicht von Mitarbeiter- und Gästerausweisen
- Sorgfältige Auswahl des Reinigungspersonals
- Anweisung an Mitarbeiter, nicht in öffentlich zugänglichen Räumlichkeiten (z.B. Cafés) zu arbeiten
- Arbeit im Home Office: Unbefugte haben kein Zutritt zur Wohnstätte der Mitarbeiter

2.2. Zugangskontrolle

Folgende implementierte Maßnahmen verhindern, dass Unbefugte Zugang zu den Datenverarbeitungssystemen haben:

- Authentifikation mit Benutzer und Passwort
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls
- Einsatz von VPN-Technologie bei Remote-Zugriffen
- Verwendung von Gehäuseverriegelungen
- Verschlüsselung von Datenträgern
- Verwaltung von Benutzerberechtigungen
- Erstellen von Benutzerprofilen
- Zentrale Passwortregeln
- Nutzung von 2-Faktor-Authentifizierung
- Personenkontrolle beim Pförtner oder Empfang
- Protokollierung der Besucher (z.B. Besucherbuch)
- Schlüsselregelung / Schlüsselbuch

- Allgemeine Unternehmens-Richtlinie zum Datenschutz oder zur Sicherheit
- Unternehmens-Richtlinie für sichere Passwörter
- Unternehmens-Richtlinie "Löschen/Vernichten"
- Unternehmens-Richtlinie "Cleandesk"
- Unternehmens-Richtlinie zur Verwendung mobiler Geräte
- Allgemeine Anweisung, bei Verlassen des Arbeitsplatzes Desktop manuell zu sperren

2.3. Zugriffskontrolle

Folgende implementierte Maßnahmen stellen sicher, dass Unbefugte keinen Zugriff auf personenbezogene Daten haben:

- Einsatz von Aktenvernichtern (mit cross cut-Funktion)
- Physische Löschung von Datenträgern vor deren Wiederverwendung
- Protokollierung der Vernichtung von Daten
- Protokollierung von Zugriffen auf Anwendungen (insbesondere bei der Eingabe, Änderung und Löschung von Daten)
- Einsatz eines Berechtigungskonzepts
- Anzahl der Administratoren ist so klein wie möglich gehalten

- Sichere Aufbewahrung von Datenträgern
- Verwaltung der Benutzerrechte durch Systemadministratoren
- Verwendung einer Bildschirmfolie als Sichtschutz
- Anweisung an Mitarbeiter, dass nur unbedingt erforderliche Daten ausgedruckt werden
- Anweisung an Mitarbeiter, dass Daten nur nach Rücksprache gelöscht werden

2.4. Trennungskontrolle

Folgende Maßnahmen stellen sicher, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden:

- Physisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Trennung von Produktiv- und Testsystem
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts
- Festlegung von Datenbankrechten

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

3.1. Weitergabekontrolle

Es ist sichergestellt, dass personenbezogene Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und überprüft werden kann, welche Personen oder Stellen personenbezogene Daten erhalten haben. Zur Sicherstellung sind folgende Maßnahmen implementiert:

- Einrichtungen von VPN-Tunneln
- WLAN-Verschlüsselung (WPA2 mit starkem Passwort)
- Bereitstellung von Daten über verschlüsselte Verbindungen: TTLS und HTTPS
- Nutzung von Signaturverfahren
- Uploadverbot dienstlicher Daten auf unternehmensfremde Server

3.2. Eingabekontrolle

Durch folgende Maßnahmen ist sichergestellt, dass geprüft werden kann, wer personenbezogene Daten zu welcher Zeit in Datenverarbeitungsanlagen verarbeitet hat:

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle oder automatische Kontrolle der Protokolle
- Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

- Anweisung an Mitarbeiter, nur nach Rücksprache Daten zu löschen

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

Durch folgende Maßnahmen ist sichergestellt, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt und für den Auftraggeber stets verfügbar sind:

- Feuerlöschgeräte in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Klimaanlage in Serverräumen
- Unterbrechungsfreie Stromversorgung (USV)
- RAID-System / Festplattenspiegelung
- Videoüberwachung in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Regelmäßige Backups
- Erstellung eines Backup- & Recoverykonzepts
- Kontrolle des Sicherungsvorgangs
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Hosting (jedenfalls der wichtigsten Daten) mit einem professionellen Hoster

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

5.1. Datenschutz-Management

Folgende Maßnahmen sollen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Verwendung der heyData-Plattform zum Datenschutz-Management
- Bestellung des Datenschutzbeauftragten heyData
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeiter im Datenschutz
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO)

5.2. Incident-Response-Management

Folgende Maßnahmen sollen gewährleisten, dass im Fall von Datenschutzverstößen Meldeprozesse ausgelöst werden:

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)

- Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- Einbindung des Datenschutzbeauftragten in Sicherheitsvorfälle und Datenpannen
- Einsatz von Anti-Viren-Software
- Einsatz von Firewalls

5.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Die folgenden implementierten Maßnahmen tragen den Voraussetzungen der Prinzipien "Privacy by design" und "Privacy by default" Rechnung:

- Schulung der Mitarbeiter im "Privacy by design" und "Privacy by default"
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

5.4. Auftragskontrolle

Durch folgende Maßnahmen ist sichergestellt, dass, dass personenbezogene Daten nur entsprechend der Weisungen verarbeitet werden können:

- Schriftliche Weisungen an den Auftragnehmer oder Weisungen in Textform (z.B. durch Auftragsverarbeitungsvertrag)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen

- Bestätigung von Auftragnehmern, dass sie ihre eigenen Mitarbeiter auf das Datengeheimnis verpflichten (typischerweise im Auftragsverarbeitungsvertrag)
- Sorgfältige Auswahl von Auftragnehmern (insbesondere hinsichtlich Datensicherheit)
- Laufende Überprüfung von Auftragnehmern und ihren Tätigkeiten
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, z.B. durch Anfrage entsprechender Bestätigungen

Anlage 3 – Aktuelle Unterauftragsverarbeiter und Subunterauftragsverarbeiter

	<u>Funktion</u>	<u>Serverstandort & Zertifikat</u>
virtion GmbH, Südring 11, 33647 Bielefeld	Hosting, IT-Sicherheit und Infrastruktur	DE ISO 27001 nach BSI IT-Grundschutz Standard
proIO GmbH Kleyerstraße 79-89 60326 Frankfurt am Main	Support/Housing von Rechenzentrums-Infrastruktur	
Telekom Deutschland GmbH Landgrabenweg 151 53227 Bonn	Hosting von Rechenzentrums- Infrastruktur	DE ISO 27001 nach BSI IT-Grundschutz Standard
Concat AG Berliner Ring 127-129 64625 Bensheim	Support/Rechenzentrums- Infrastruktur	
Quentn.com GmbH, Friedrich-Ebert-Straße 51, 14469 Potsdam	Versand Transaktionsmails Transportverschlüsselung mittels TTLS	

Hetzner Online GmbH Industriestraße 25, 91710 Gunzenhausen, Deutschland	Hosting der Quentn Server, Ersatz defekter Hardware, Aufspielen des Grundsystems, Installationsarbeiten	DE ISO 27001 nach BSI IT-Grundschutz Standard
Amazon Web Services EMEA SARL 38 Avenue, John F. Kennedy, L-1855 Neudorf-Weimershof, Luxembourg	Content Delivery Network, Web Application Firewall, Nameserver und Domain- Zertifikate	EU ISO 27001 nach BSI IT-Grundschutz Standard
Treestack GmbH, Lüderichstr. 2-4, 51105, Köln	Fehlerbehebung	
Zammad GmbH, Marienstraße 18, 10117 Berlin	Helpdesk-System	
Hetzner Online GmbH, Industriestraße 25, D- 91710 Gunzenhausen	Hosting	DE ISO 27001 nach BSI IT-Grundschutz Standard

Es werden keine weiteren Unterauftragsverarbeiter durch den Auftragsverarbeiter oder Unterauftragsverarbeiter eingesetzt.