Auftragsverarbeitungsvertrag

„PROWISE LEARN“

1. Die Bildungseinrichtung/Schule _____
unter der Anschrift _____,
nachstehend „**Verantwortliche**“ genannt,

und

2. Der **PROWISE GMBH**, eine nach deutschem Recht gegründete Gesellschaft, mit eingetragenem Sitz unter der Anschrift Richmodstr. 6, 50667 Köln, Deutschland, nachstehend „**Auftragsverarbeiter**“ genannt ,

nachstehend zusammen auch als: die "Parteien" bezeichnet,

DIE PARTEIEN VEREINBAREN HIERMIT FOLGENDES:

1. Subject matter of this Data Processing Agreement

1.1 Dieser Datenverarbeitungsvertrag gilt ausschließlich für die Verarbeitung personenbezogener Daten, die im Rahmen des Vertrags zwischen den Parteien über die webbasierte Dienstleistung Prowise Learn ("**Dienstleistungen**") (nachstehend der "**Dienstleistungsvertrag**") unter das EU-Datenschutzrecht fallen.

1.2 Der Begriff **„Datenschutzrecht**“ steht für Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr („**Datenschutz-Grundverordnung**“) und andere geltendem Datenschutzbestimmungen der EU oder eines Mitgliedsstaates verstößt. Begriffe wie **„Verarbeitung**“, „**Personenbezogene Daten**“, „**Verantwortlicher**“ und „**Auftragsverarbeiter**“ haben die Bedeutung, die ihnen gemäß Art. 4 Datenschutz-Grundverordnung zugeschrieben werden.

1.3 Sofern der Auftragsverarbeiter im Rahmen des Dienstleistungsvertrags personenbezogene Daten im Sinne der Datenschutz-Grundverordnung im Auftrag des Verantwortlichen verarbeitet, gelten die Bestimmungen dieses Auftragsdverarbeitungsvertrages.

1.4 Die Parteien haben einen Dienstleistungsvertrag geschlossen, um vom Know-how des Auftragsverarbeiters über die Sicherung und Verarbeitung der personenbezogenen Daten zu den in Anlage 2 aufgeführten Zwecken zu profitieren. Es ist dem Auftragsverarbeiter gestattet, die Mittel, die

er zur Umsetzung dieser Zwecke im Rahmen der Anforderungen des Datenverarbeitungsvertrags für notwendig hält, nach eigenem Ermessen auszuwählen und zu nutzen.

2. Art, Umfang und Zweck der vorgesehenen Verarbeitung der personenbezogenen Daten

2.1 Der Verantwortliche legt den Rahmen, die Zwecke und das Verfahren für den Zugriff auf die personenbezogenen Daten bzw. für die Verarbeitung der personenbezogenen Daten durch den Auftragsverarbeiter fest. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten ausschließlich gemäß den schriftlichen Weisung des Verantwortlichen.

2.2 Eine Übersicht über die Kategorien personenbezogener Daten, die Kategorien der Datensubjekte betroffenen Personen und die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, ist in Anlage 2 enthalten.

3. Pflichten des Auftragsverarbeiter

3.1 Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten auf dokumentierte Weisungen des Verantwortlichen ausschließlich so, dass – und insofern – dies für die Ausführung der Dienstleistungen angemessen ist, es sei denn, es bestehen gesetzliche Verpflichtungen, zu deren Einhaltung der Auftragsverarbeiter verpflichtet ist. In einem solchen Fall informiert der Auftragsverarbeiter den Verantwortlichen vor der Verarbeitung über eine solche gesetzliche Verpflichtung, es sei denn, die Weitergabe dieser Information an den Verantwortlichen ist laut Gesetz ausdrücklich untersagt. Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten unter keinen Umständen auf eine Weise, die gegen die schriftlichen Weisungen des Verantwortlichen verstößt. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn eine Anweisung seiner ihrer Meinung nach gegen das EU-Datenschutzrecht oder andere Datenschutzbestimmungen der EU oder eines Mitgliedsstaates verstößt.

3.2 Unbeschadet aller bestehenden vertraglichen Vereinbarungen zwischen den Parteien behandelt der Auftragsverarbeiter alle personenbezogenen Daten streng vertraulich und informiert alle seine Mitarbeiter, Vertreter und/oder genehmigten Unterauftragsverarbeiter, die mit der Verarbeitung der personenbezogenen Daten befasst sind, über den vertraulichen Charakter der personenbezogenen Daten. Der Auftragsverarbeiter stellt sicher, dass alle diese Personen oder Parteien eine entsprechende Geheimhaltungserklärung unterzeichnet haben, anderweitig zur Geheimhaltung verpflichtet sind der Geheimhaltungsverpflichtung aus einer gesetzlichen Bestimmung unterliegen.

4. Technisch-organisatorische Maßnahmen

4.1 Unter Berücksichtigung des technischen Stands, der Kosten der Umsetzung sowie der Art, des Umfangs, des Kontextes und der Zwecke der Verarbeitung sowie der Risiken der unterschiedlichen Wahrscheinlichkeiten und Auswirkungen auf die Rechte und Pflichten natürlicher Personen und unbeschadet aller sonstigen Sicherheitsstandards, die zwischen den Parteien vereinbart werden, ergreifen der Verantwortliche und der Auftragsverarbeiter angemessene technische und organisatorische Maßnahmen, um zu gewährleisten, dass die Verarbeitung personenbezogener Daten

auf einem angemessenen Niveau gesichert wird. Die Maßnahmen, mit denen sich alle Parteien einverstanden erklären, sind in Anlage 3 aufgeführt.

4.2 Der Auftragsverarbeiter sorgt dafür, dass angemessene schriftliche Sicherheitsrichtlinien für die Verarbeitung personenbezogener Daten gelten, die als Mindestmaß die in Artikel 4.1 genannten Maßnahmen umfassen.

4.3 Die Parteien bestätigen, dass sich die Sicherheitsanforderungen ständig ändern und dass eine effektive Sicherheit die regelmäßige Evaluierung und Verbesserungen veralteter Sicherheitsmaßnahmen erfordert. Der Auftragsverarbeiter bewertet daher fortlaufend die aktuellen Sicherheitsmaßnahmen im Sinne von des Artikel 4 dieses Vertrages und verschärft, ergänzt und verbessert diese Sicherheitsmaßnahmen, um die Einhaltung der Anforderungen aus Artikel 4 dieses Vertrages aufrechtzuerhalten. Die Parteien verhandeln in Treu und Glauben über die Kosten – sofern welche anfallen – zur Umsetzung wesentlicher Änderungen aufgrund spezifischer Sicherheitsanforderungen, die laut geltendem Datenschutzrecht erforderlich sind oder von den für den Datenschutz zuständigen Behörden im jeweiligen Gerichtsbezirk vorgeschrieben werden.

4.4 Sofern der Dienstleistungsvertrag angepasst werden muss, um eine Anweisung des Verantwortlichen an den Auftragsverarbeiter zur Verbesserung von Sicherheitsmaßnahmen, die aufgrund von Änderungen im des geltenden Datenschutzrechts notwendig ist, zu entsprechen, verhandeln die Parteien in Treu und Glauben über eine entsprechende Anpassung des Dienstleistungsvertrags.

5. Kontrollrechte des Auftragsverarbeiter

5.1 Nach Aufforderung durch den Verantwortlichen muss der Auftragsverarbeiter die Maßnahmen vorführen, die er aufgrund Artikels 4.1 ergriffen hat, und muss derm Verantwortlichen gestatten, diese Maßnahmen im Rahmen eines Audits zu prüfen und zu testen. Ein Audit kann nur stattfinden, nachdem der Verantwortliche vergleichbare Auditberichte, die dem Auftragsverarbeiter zugänglich sind, angefordert und bewertet hat, und nachvollziehbare Argumente liefert, die ein Audit durch den Verantwortlichen rechtfertigen. Ein solches Audit ist gerechtfertigt, wenn vergleichbare Auditberichte, die für den Auftragsverarbeiter zugänglich sind, keine oder unzureichende Informationen über die Einhaltung dieses Datenverarbeitungsvertrags durch den Auftragsverarbeiter bieten.

5.2 Der Auftragnehmer hat das Recht, einen vom Auftraggeber zur Kontrolle benannten Dritten abzulehnen, wenn dieser Dritte nach Einschätzung des Auftragnehmers nicht hinreichend qualifiziert ist oder es sich um einen Wettbewerber des Auftragnehmers handelt. Sofern der Auftragnehmer einen Dritten aus den vorstehenden Gründen ablehnt, ist der Auftraggeber verpflichtet, einen anderen Dritten für die Prüfung zu benennen oder kann alternativ die Kontrolle selbst durchführen.

5.3 Für Audits durch den Verantwortlichen gelten die folgenden Bedingungen:

a. Der Audittermin wird nach Rücksprache mit dem Auftragsverarbeiter mindestens vierzehn (14) Tage im Voraus geplant und schriftlich festgelegt. Es darf höchstens ein Audit pro Jahr stattfinden (außer das Audit erfolgt im Anschluss an eine Verletzung des Schutzes personenbezogener Daten).

b. Der Auditor verpflichtet sich gegenüber dem Auftragsverarbeiter zur Geheimhaltung.

c. Der Auditor hat keinen Zugang zu Daten, die nicht von derm Verantwortlichen stammen.

d. Der Verantwortliche gewährleistet, dass weder die Geschäftstätigkeiten noch die Daten- und Netzwerksysteme des Auftragsverarbeiters durch das Audit beeinträchtigt oder beschädigt werden.

e. Der Verantwortliche trägt sämtliche Kosten und übernimmt die Verantwortung und Haftung für das Audit.

f. Der Verantwortliche erhält ausschließlich den Bericht des Auditors, behandelt die Auditergebnisse streng vertraulich und verwendet sie lediglich zu den spezifischen Zwecken, die für Audits in diesem Artikel festgelegt sind.

g. Auf Wunsch des Auftragsverarbeiters stellt der Verantwortliche diesem dieser eine Kopie des Auditberichts zur Verfügung.

5.4 Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

6. Datenübermittlung

6.1 Der Auftragsverarbeiter benachrichtigt den Verantwortlichen unverzüglich über jegliche (geplanten) dauerhaften oder vorübergehenden Übertragungen personenbezogener Daten in Länder außerhalb des Europäischen Wirtschaftsraumes ohne ein angemessenes Datenschutzniveau und nimmt eine solche (geplante) Übertragung nur mit Zustimmung des Verantwortlichen vor, der diese Zustimmung nach eigenem Ermessen verweigern kann. Anlage 4 enthält eine Liste der Übertragungen, für die der Verantwortliche bei Abschluss dieses Datenverarbeitungsvertrags seine ihre Zustimmung erteilt.

6.2 Sofern der Verantwortliche und der Auftragsverarbeiter sich auf einen spezifischen vertraglich vereinbarten Mechanismus für die Vereinheitlichung internationaler Datenübertragungen verlassen, der anschließend verändert, widerrufen oder von einem zuständigen Gericht für ungültig erklärt wird, vereinbaren der Verantwortliche und der Auftragsverarbeiter in Treu und Glauben, die Übertragung unverzüglich zu beenden oder eine geeignete Alternative zu finden, mit der die Übertragung rechtmäßig bewirkt werden kann.

7. Informationspflicht und Verletzung des Schutzes personenbezogener Daten

7.1 Wenn der Auftragsverarbeiter von einem Zwischenfall erfährt, der einen Verletzung des Schutzes personenbezogener Daten darstellt, der die Verarbeitung der personenbezogenen Daten, die Gegenstand des Dienstleistungsvertrags sind, beeinflusst, muss er den Verantwortlichen unverzüglich über den Zwischenfall benachrichtigen, jederzeit mit dem Verantwortlichen zusammenarbeiten und die Anweisungen des Verantwortlichen im Zusammenhang mit solchen Zwischenfällen befolgen, um es dem Verantwortlichen zu ermöglichen, den Zwischenfall umfassend zu untersuchen, eine angemessene Reaktion zu finden und geeignete weitere Maßnahmen im Zusammenhang mit dem Zwischenfall zu ergreifen.

7.2 Der Auftragsverarbeiter muss jederzeit über schriftlich festgelegte Verfahren verfügen, die es ihm ermöglichen, den Verantwortlichen unverzüglich über einen Zwischenfall, der einen Verletzung des

Schutzes personenbezogener Daten darstellt, zu informieren. Wenn es ein Zwischenfall nach vernünftigem Ermessen erforderlich macht, dass der die Auftragsverarbeiter nach geltendem Datenschutzrecht über einen Verstoß informiert, muss der Auftragsverarbeiter seine schriftlich festgelegten Verfahren so umsetzen, dass er in der Lage ist, den Verantwortlichen zu benachrichtigen, nachdem er von einem solchen Zwischenfall erfahren hat.

7.3 Alle Benachrichtigungen an den Verantwortlichen im Sinne dieses Artikels 7 sind an den Mitarbeiter desVerantwortlichen zu richten, dessen Kontaktdaten in Anlage 1 zu diesem Datenverarbeitungsvertrag genannt sind, und müssen Folgendes enthalten:

a. eine Beschreibung der Art des Zwischenfalls, einschließlich – sofern möglich – der Kategorien und der ungefähren Anzahl der betroffenen Datensubjekte Personen sowie der Kategorien und der ungefähren Anzahl der betroffenen Datensätze mit personenbezogenen Daten,

b. Namen und Kontaktdaten des Datenschutzbeauftragten des Verantwortlichen oder einer anderen Kontaktperson, die weitere Informationen bereitstellen kann,

c. eine Beschreibung der wahrscheinlichen Konsequenzen des Zwischenfalls, und

d. eine Beschreibung der ergriffenen Maßnahmen oder der Maßnahmen, die dem Auftragsverarbeiter zur Behandlung des Zwischenfalls vorgeschlagen werden, einschließlich, sofern zutreffend, der Maßnahmen zur Vermeidung möglicher nachteiliger Auswirkungen.

8. Verträge mit Unterauftragsverarbeitern

8.1 Der Verantwortliche gestattet es dem Auftragsverarbeiter, für servicebezogene Tätigkeiten gemäß Anlage 2 Unterauftragsverarbeiter an den Länderstandorten zu beschäftigen. Der Auftragsverarbeiter informiert den Verantwortlichen über alle neuen oder ersetzten Unterauftragsverarbeiter. Der Verantwortliche ist berechtigt, dieser Hinzufügung oder Ersetzung aus triftigen Gründen schriftlich innerhalb von 30 Tagen nach Bekanntgabe des Auftragsverarbeiter zu widersprechen. Wenn der Auftragsverarbeiter trotz des Widerspruchs des Verantwortliche weiterhin beabsichtigt, einen neuen Unterauftragsverarbeiter zu ersetzen oder zu beauftragen, ist der Verantwortliche berechtigt, die Dienstleistungsvertrag innerhalb von 30 Tagen nach Mitteilung des Auftragsverarbeiter mit sofortiger Wirkung zu kündigen. Die Kündigung muss schriftlich erfolgen.

8.2 Ungeachtet irgendeiner Genehmigung des Verantwortlichen im Sinne des vorstehenden Absatzes haftet der Auftragsverarbeiter weiterhin vollumfänglich gegenüber dem Verantwortlichen für alle Datenschutzrechtsverletzungen durch ihre Unterauftragsverarbeiter.

8.3 Die Zustimmung des Verantwortlichen im Sinne von Artikel 8.1 ändert nichts an dem Umstand, dass die Zustimmung im Sinne von Artikel 6 für die Beschäftigung von Unterauftragsverarbeitern in einem Land außerhalb des Europäischen Wirtschaftsraumes ohne ein angemessenes Datenschutzniveau erforderlich ist.

8.4 Der Auftragsverarbeiter gewährleistet, dass der Unterauftragsverarbeiter an dieselben Datenschutzverpflichtungen im Sinne dieses Datenverarbeitungsvertrags wie der Auftragsverarbeiter selbst im Sinne dieses Datenverarbeitungsvertrags gebunden ist, überwacht deren Einhaltung und muss seine Unterauftragsverarbeiter insbesondere dazu verpflichten, angemessene technische und

organisatorische Maßnahmen zu ergreifen, die so auszugestalten sind, dass die Verarbeitung den Anforderungen des Datenschutzrechts genügt.

9. Rückgabe oder Löschung von personenbezogenen Daten

9.1 Nach Ende Beendigung dieses Datenverarbeitungsvertrags werden die personenbezogenen Daten für einen Zeitraum von 12 Monaten weiterverarbeitet. Nach Ablauf dieser 12 Monate werden diese personenbezogenen Daten gelöscht oder anonymisiert.

9.2 Ungeachtet des Artikels 9.1 muss der Auftragsverarbeiter jedoch Auf schriftliche Anfrage des Verantwortlichen alle personenbezogenen Daten entweder löschen, löschen oder an den Datenverarbeiter zurückgeben und vorhandene Kopien auf schriftliche Anfrage des Datenverarbeiters löschen, vernichten oder an den Verantwortlichen zurückgeben und alle bestehenden Kopien vernichten oder zurückgeben.

10. Unterstützung des Verantwortlichen

10.1 Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen ihrer Möglichkeiten durch geeignete technische und organisatorische Maßnahmen, um die Verpflichtungen des Verantwortlichen, wie insbesondere, Anfragen zur Wahrnehmung der Rechte von Datensubjekten betroffenen Personen im Rahmen des Datenschutzrechts , zu erfüllen.

10.2 Der Auftragsverarbeiter unterstützt den Verantwortlichen dabei, die Einhaltung der Verpflichtungen gemäß Abschnitt 4 (Sicherheit) zu gewährleisten, sowie bei vorhergehenden Gesprächen mit Aufsichtsbehörden, die aufgrund von Artikel 36 der Datenschutz-Grundverordnung notwendig sind, unter Berücksichtigung der Art der Verarbeitung und der Informationen, die der Auftragsverarbeiter zur Verfügung stehen.

10.3 Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Verpflichtungen des Verantwortlichen nachzuweisen Hierzu zählt auch die Verpflichtung Audits, einschließlich Kontrollen, die vom Verantwortlichen oder einem anderen, vom Verantwortlichen eingesetzten Auditor, durchgeführt werden, zu ermöglichen und dazu beizutragen.

11. Haftung

11.1 Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung.

12. Abweichung und Änderung der Datenschutzvereinbarung

12.1 Im Fall der Abweichung der Bestimmungen dieser Datenverarbeitungsvereinbarung von den Bestimmungen des Hauptvertrages haben die Bestimmungen dieser Datenverarbeitungsvereinbarung Vorrang.

12.2 Sofern die Parteien von den Klauseln dieses Datenverarbeitungsvertrags abweichen oder diese ergänzen möchten, werden diese Abweichungen und / oder Ergänzungen von den Parteien in einer Übersicht beschrieben und begründet. Eine in diesem Fall auszufüllende Übersicht ist diesem

Datenverarbeitungsvertrag als Anhang 4 beigefügt. Die Bestimmungen dieses Absatzes gelten nicht für Ergänzungen und / oder Änderungen der Anlagen 1, 2 und 3.

12.3 Bei wichtigen Änderungen des Hauptvertrages, die Einfluss auf die Verarbeitung personenbezogener Daten haben, ist der Datenschutzbeauftragte in klarer Sprache über die Folgen dieser Änderungen zu informieren. Außerdem hat der Datenschutzbeauftragte diese Vorhaben zu bestätigen. Wichtige Änderungen sind insbesondere: das Hinzufügen oder Ändern einer Funktion, die zu einer Erhöhung der zu verarbeitenden personenbezogenen Daten und der Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, führt. Mögliche Änderungen sind in Anhang 2 dieser Datenverarbeitungsvereinbarung aufgeführt.

12.4 Die Klauseln dieses Datenverarbeitungsvertrags können von den Parteien nur durch gemeinsame schriftliche Vereinbarungen geändert werden.

13. Laufzeit und Beendigung

13.1 Dieser Datenverarbeitungsvertrag tritt am Datum seiner Unterzeichnung in Kraft und wird für denselben Zeitraum wie der Dienstleistungsvertrag geschlossen.

13.2 Wenn der Dienstleistungsvertrag aus welchem Grund auch immer beendet wird, behält dieser Datenverarbeitungsvertrag seine volle Gültigkeit, solange der Auftragsverarbeiter personenbezogene Daten verarbeitet, z.B. im Rahmen eines reibungslosen Übergangs; in diesem Fall endet dieser Datenverarbeitungsvertrag automatisch zu dem Zeitpunkt, sobald der reibungslose Übergang vollzogen ist.

13.3 Die Beendigung oder der Ablauf dieses Datenverarbeitungsvertrags entlässt diese Auftragsverarbeiterin nicht aus seinen ihren Verpflichtungen zur Geheimhaltung im Sinne von Artikel 3.2.

14. Teilunwirksamkeit

14.1 Sollte eine Bestimmung dieser Datenverarbeitungsvereinbarung ungültig, nichtig oder auf andere Weise nicht durchsetzbar sein oder werden, bleiben die übrigen Bestimmungen dieser Vereinbarung in vollem Umfang in Kraft. Die Parteien haben sich in diesem Fall zu beraten, durch welche wirksame und durchsetzbare Alternativbestimmung die unwirksame und nicht durchsetzbare Bestimmung ersetzt werden kann, wobei der Zweck der ungültigen, aufgehobenen oder anderweitig nicht durchsetzbaren Bestimmung so weit wie möglich mitzuberücksichtigen ist.

15. Anwendbares Recht und zuständiges Gericht

15.1 Für diesen Datenverarbeitungsvertrag gilt deutsches Recht mit Ausnahme der Bestimmungen des internationalen Privatrechts. Alle Streitigkeiten, die sich aus oder im Zusammenhang mit diesem Datenverarbeitungsvertrag ergeben, sind ausschließlich dem zuständigen Gericht in Deutschland vorzulegen.

Die an diesem Vertrag beteiligten Parteien haben diesen Datenverarbeitungsvertrag zur Unterzeichnung durch ihre befugten Vertreter ausgefertigt.

Verantwortlicher	Auftragsverarbeiter
_____	_____
Name:	Name:
Titel:	Titel:
Datum:	Datum:

Version 1.0

7. Juni 2019

Anlage 1: Kontaktdaten

Kontaktdaten des Datenschutzbeauftragten des Verantwortlichen:

_____
_____
_____
_____
_____
_____

Kontaktdaten des Datenschutzbeauftragten/Compliance-Beauftragten des Auftragsverarbeiters:

Prowise GmbH
Herr L. Loeff (Datenschutzbeauftragter)
(+31) (0) 495 497110
privacy@prowise.com

Anlage 2: Kategorien und Zwecke der personenbezogenen Daten sowie Unterauftragsverarbeiter bzw. Unterauftragsverarbeiter eines Unterauftragsverarbeiters

Kategorien von betroffenen Personen, personenbezogenen Daten und Verarbeitungstätigkeiten
Im Zusammenhang mit der Entwicklung, dem Betrieb und dem Hosting der webbasierten Dienste unter dem Namen Prowise Learn (nachstehend die „Dienstleistungen") im Auftrag des Verantwortlichen erteilt der Verantwortliche die Anweisung (oder die Zustimmung), die nachstehenden Daten zu den nachstehend beschriebenen Zwecken zu verarbeiten:

1. Datenverarbeitungszwecke

Verarbeitung, die wesentlicher Bestandteil der Dienstleistung ist
Die Verarbeitung erfolgt, um es Bildungseinrichtungen zu ermöglichen, Bildungsangebote bereitzustellen, deren Fortschritt zu verfolgen, den Fortschritt der Schüler zu verfolgen und sie anzuleiten.

Im Zuge der Nutzung der Dienstleistungen finden folgende Verarbeitungstätigkeiten statt:

- Speicherung von Lern- und Testergebnissen
- Empfang von Lern- und Testergebnissen
- Bewertung von Lern- und Testergebnissen, um Lern- und Testmaterialien zu entwickeln, die speziell an die Lernbedürfnisse von Schülern angepasst sind
- Bewertung von Lern- und Testergebnissen eines Schülers im Verhältnis zu den Ergebnissen einer Gruppe von Schülern, um Erkenntnisse über die Leistung eines Schülers im Verhältnis zur Gruppe zu gewinnen(zum Beispiel: prozentuale Ergebnisse)
- Analyse und Interpretation von Lernergebnissen
- Bereitstellung/Ingebrauchnahme der Dienstleistungen
- Zugang zu den Dienstleistungen und externen Datensystemen, einschließlich Identifizierung, Authentifizierung und Autorisierung
- Sicherheit, Kontrolle und Verhinderung von Missbrauch und unangemessener Nutzung sowie Verhinderung der Unregelmäßigkeit und Unzuverlässigkeit der verarbeiteten personenbezogenen Daten
- Kontinuität und angemessene Funktion der Dienstleistungen, einschließlich Wartungsarbeiten, Erstellen von Back-ups, Korrekturen nach Fehlern oder Ungenauigkeiten und Supportdienste
- Forschung und Analyse auf der Grundlage strenger Bedingungen, vergleichbar mit bestehenden Verhaltensregeln in Forschung und Statistik, zugunsten (der Verbesserung) des Lernprozesses, der Dienstleistungen oder der Richtlinien ders DatenverantwortlichenVerantwortlichen

- Bereitstellung von komplett anonymisierten Daten zu Forschungs- und Analysezwecken durch die Bildungseinrichtung, um die Qualität der Bildung zu verbessern
- Bereitstellung von personenbezogenen Daten, sofern dies notwendig ist, um die rechtlichen Anforderungen zu erfüllen, die für digitale Bildungsinhalte gelten
- Umsetzung oder Anwendung sonstiger Gesetze.

Optionale Verarbeitung:

Im Zuge der Nutzung der Dienstleistungen können abhängig von den Entscheidungen, Präferenzen oder Einstellungen des Verantwortlichen auch andere Formen der Verarbeitung stattfinden:

- Möglichkeit, Lern- und Testergebnisse mit Schülerverwaltungssystemen des Verantwortlichen auszutauschen
- Möglichkeit, Lern- und Testergebnisse mit von dem Verantwortlichen genutzten Instrumenten auszutauschen
- manche Kontaktdaten sind optional, zum Beispiel die Telefonnummern von Lehrkräften/Administratoren und Schüleradressen
- manche Kontaktdaten sind optional, zum Beispiel die Telefonnummern von Lehrkräften/Administratoren und Email-Adressen der Schüler.
- Die Verarbeitung der E-Mail-Adresse für Newsletter ist optional und erfolgt über Opt-In.
- Die Aufbewahrung personenbezogener Daten für Forschungs- und Produktoptimierungsprojekte. Zur näheren Erläuterung siehe Artikel 2.

2. Aufbewahrungsfristen und wissenschaftliche Forschung

Personenbezogene Daten von Schülern und Lehrkräften unserer Bildungseinrichtungen werden bis zu 12 Monate nach Ende des Abonnements für die Dienstleistungen gespeichert, es sei denn, der Verantwortliche beantragt ausdrücklich eine kürzere Aufbewahrungsfrist. So erhalten Bildungseinrichtungen die Gelegenheit, die Aufzeichnungen eines weiteren Jahres aufzurufen, wenn sie erfahren möchten, mit welchen Ergebnissen ihre Schüler die Dienstleistungen genutzt haben. Wenn eine Bildungseinrichtung zum Beispiel ein anderes Lerninstrument einsetzt, hat die Bildungseinrichtung außerdem die Gelegenheit, die Lernergebnisse des neuen Produkts mit denen unserer Dienstleistungen zu vergleichen. Außerdem können Bildungseinrichtungen ihre Entscheidung, die Nutzung unserer Dienstleistungen zu beenden, innerhalb von 12 Monaten revidieren, und die Schüler können dort weitermachen, wo sie aufgehört haben.

Daten werden in komplett anonymisierter Form zu wissenschaftlichen Forschungszwecken gespeichert. Außerdem können die anonymisierten Daten zu wissenschaftlichen Forschungszwecken auch Dritten zur Verfügung gestellt werden.

3. Beschreibung der Kategorien personenbezogener Daten

Betroffene Personen: Benutzer - Administratoren/Lehrkräfte

Kategorie	**Erläuterung**
Kontaktdaten	Name, Vornamen, E-Mail-Adresse, Telefonnummer (optional)
Bildungsteilnehmernummer	Eine Verwaltungsnummer, anhand derer der Teilnehmer identifiziert werden kann
Daten der Schule/Bildungseinrichtung	Name der Schule/Klasse
Benutzereinstellungen und -handlungen	Anzahl der Anmeldungen, Handlungen, die eine Lehrkraft auf Klassenebene ausführt, z.B. Spieleinstellungen
Technische Daten	- Browserkennung (User Agent), um festzustellen, welche Software der Kunde nutzt, und um Probleme zu lösen - IP-Adresse zu internen Zwecken (Einblick in Benutzerstatistiken) und zur Vermeidung von Missbrauch (Netzüberlastung)

Betroffene Personen: Benutzer - Spieler (Kinder, Schüler, Erwachsene)

Kategorie	**Erläuterung**
Kontaktdaten	Name, Vornamen, Geschlecht, Geburtsmonat, Schuljahr, E-Mail-Adresse (optional)
Bildungsteilnehmernummer	Eine Verwaltungsnummer, anhand derer der Teilnehmer identifiziert werden kann
Daten der Schule/Bildungseinrichtung	Name der Schule/Klasse, Lehrkraft
Lernergebnisse	Abgeschlossene Übungen einschließlich Antworten und Reaktionszeit Daraus abgeleitete Daten, z.B. Bewertungen von Fähigkeiten, Bewertungen von Lernzielen und prozentuale Bewertungen
Benutzereinstellungen und -handlungen	Das beinhaltet unter anderem Belohnungen, verfügbare Spiele, gewählte Schwierigkeitsgrade, Anzahl der Anmeldungen und angesehene Anleitungsvideos
Technische Daten	- Browserkennung (User Agent), um festzustellen, welche Software der Kunde nutzt, und um Probleme zu lösen - IP-Adresse zu internen Zwecken (Einblick in Benutzerstatistiken) und zur Vermeidung von Missbrauch (Netzüberlastung)

4. Unterauftragsverarbeiter und Länderstandort

- Oefenweb.nl B.V., Niederlande (Erbringung der Dienstleistungen)
- Prowise B.V., Niederlande (Support/Helpdesk/Development)

5. Unterunterauftragsverarbeiter und Länderstandort

- Leaseweb, Niederlande (Hosting-Provider)
- Hetzner, Deutschland (Hosting-Provider)

6. Version und Änderungen

Der Auftragsverarbeiter kann den Inhalt der Anlage 2 regelmäßig aktualisieren. Die aktuellste Version ist durch sie fortlaufend unter https://www.prowise.com/de/world-of-education/ verfügbar zu halten. Bei wichtigen Änderungen, wie dem Hinzufügen neuer Datenverarbeitungsmaßnahmen, hat der Auftragsverarbeiter den Verantwortliche aktiv zu informieren (zum Beispiel per E-Mail). Nach Bekanntgabe einer (vorgeschlagenen) Änderung hat der Verantwortliche 30 Tage Zeit, um der Änderung zu widersprechen, wobei die Gründe für den Widerspruch anzugeben sind. Sofern keine entsprechende Benachrichtigung erfolgt, gilt die Änderung als von dem Verantwortlichen genehmigt.

Anlage 3: Sicherheitsmaßnahmen

1. Zugang zu personenbezogenen Daten

Der Auftragsverarbeiter gewährleistet, dass Autorisierungsrichtlinien gelten, die dafür sorgen, dass Mitarbeiter nur dann auf personenbezogene Daten zugreifen können, wenn dies im Rahmen ihrer Tätigkeit notwendig ist.

Mitarbeiter und Daten	**Maßnahmen**
Kundenservicemitarbeiter haben Zugang zu Daten, die sich auf das Abonnement und die Nutzung beziehen.	Verwaltungsmaßnahmen und Endkundensupport.
Fachkräfte aus den Bereichen Entwicklung und Analyse von Lernmaterialien haben Zugang zu Ergebnissätzen, die sich auf die Nutzung dieser Lernmaterialien beziehen.	Analyse der Lernmaterialien zur Verbesserung der Materialien, Entwicklung und Optimierung adaptiver Lernmaterialien, Erkennung und Beseitigung von Fehlern bei der Verwendung der digitalen Lerninhalte. In manchen Fällen auch Beantwortung spezifischer Fragen im Zusammenhang mit Lernergebnissen.
IT- und Datenbankadministratoren sowie Entwickler haben Zugang zu den Dienstleistungen und verwandten (Live-)Datenbänken.	Die Tätigkeiten der IT- Datenbankadministratoren sind so gestaltet, dass sie die Verfügbarkeit, Kontinuität und Optimierung von ICT-Systemen und Software gewährleisten.

2. Maßnahmen zum Schutz personenbezogener Daten vor Missbrauch

Organisation der Datensicherheit und Kommunikationsprozesse

- Es gibt einen Ausschuss für Datenschutz & Sicherheit, der Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten identifiziert, das Bewusstsein für Sicherheitsprobleme erhöht, Einrichtungen überprüft und Maßnahmen ergreift, die die Einhaltung von Informationssicherheitsrichtlinien gewährleisten sollen.
- Zwischenfälle im Zusammenhang mit der Informationssicherheit werden erfasst und genutzt, um die Informationssicherheitsrichtlinien zu verbessern.
- Ein Prozess zur Kommunikation von Zwischenfällen im Zusammenhang mit der Informationssicherheit wird eingerichtet und dokumentiert.

Beschäftigte

- Mitarbeiter unterzeichnen (interne und externe) Vertraulichkeitserklärungen und Vereinbarungen zur Informationssicherheit.
- Bewusstsein, Schulung und Ausbildung in den Bereichen Datenschutz und Informationssicherheit werden gefördert.

- Eine Autorisierungsrichtlinie wurde erstellt, um zu gewährleisten, dass Mitarbeiter nur dann auf personenbezogene Daten zugreifen können, wenn dies im Rahmen ihrer Tätigkeit notwendig ist.

Physische Sicherheit und Kontinuität von Ressourcen

· Personenbezogene Daten werden nur in einer physischen Umgebung verarbeitet, die angemessen gegen externe Bedrohungen geschützt ist. Die Rechenzentren der Hosting-Provider sind nach ISO 27001 zertifiziert.
· Außerdem gewährleisten georedundante Back-ups die Kontinuität der Dienstleistungen und die Verfügbarkeit der personenbezogenen Daten. Mit anderen Worten: Wenn sich am Hauptstandort ein schwer wiegender Zwischenfall ereignet (z.B. Überschwemmung, Angriff oder Brand), sind die Daten weiterhin an einem alternativen, sicheren Standort verfügbar.
· Es werden regelmäßig (verschlüsselte) Back-ups erstellt, um die Kontinuität der Dienstleistungen zu gewährleisten. Diese Back-ups werden vertraulich behandelt und in einer sicheren Umgebung gespeichert.
· Die Standorte, an denen Daten verarbeitet werden, werden regelmäßig kontrolliert, instandgehalten und auf Sicherheitsrisiken überprüft.

Netzwerk, Server-/Anwendungssicherheit und Wartung

· Die Netzwerkumgebung, in der Daten gespeichert werden, ist streng gesichert. Die Datenströme sind voneinander getrennt, und es wurden Maßnahmen ergriffen, um Missbrauch und Angriffe zu verhindern.
· Die Umgebung, in der personenbezogene Daten verarbeitet werden, wird überwacht, um Angriffe, Einbrüche und Einbruchsversuche so schnell wie möglich zu erkennen.
· Die virtuellen Lernumgebungen, in denen personenbezogene Daten verarbeitet werden, werden anhand eines mehrstufigen Softwareentwicklungsprozesses entwickelt. Es werden größtmögliche Anstrengungen unternommen, um zu gewährleisten, dass die letztgenannte Maßnahme grundsätzlich so umgesetzt wird, dass Sicherheitsverstöße verhindert werden.
· Patch-Management sorgt dafür, dass aktuelle (Sicherheits-)Patches regelmäßig auf den Systemen installiert werden.
· Auf lokalen Arbeitsplatzrechnern und Servern werden geeignete Maßnahmen ergriffen, um zu verhindern, dass bösartige Software oder Funktionen installiert werden.
· Kryptografische Maßnahmen (Hashing), die branchenintern allgemein als sicher erachtet werden, werden auf Passwörter angewendet, um zu gewährleisten, dass diese Daten sicher gespeichert sind. Die einzige Ausnahme davon sind Passwörter von Benutzern, die sie nicht selbst eingegeben haben, um die Passwortverwaltung von Lehrkräften und Administratoren zu erleichtern.
· Anmeldeprozesse nutzen verschlüsselte Verbindungen.
· Der Austausch personenbezogener Daten zwischen des Verantwortliche und den Dienstleistungen ist verschlüsselt.

3. Maßnahmen zur Erkennung von Schwachstellen

Die Sicherheit wird regelmäßig überprüft. Das umfasst unter anderem ein internes Audit auf Schwachstellen und die Überprüfung der besten Praktiken (z.B. OWASP) im Bereich Sicherheit.

Anhang 4: Übertragung in Ländern außerhalb des EWR

Übertragungen in Länder außerhalb des Europäischen Wirtschaftsraums ohne ein angemessenes Schutzniveau, für die der Verantwortliche seine Zustimmung gegeben hat:

KEINE