Universität Regensburg

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO

Auftraggeber (Verantwortlicher):
Leonhart-Fuchs-Grundschule Wemding, Oettinger Str. 16, 86650 Wemding

Auftragnehmer (Auftragsverarbeiter):
Universität Regensburg, Universitätsstraße 31, 93053 Regensburg

1. Gegenstand und Dauer der Verarbeitung

Der Auftrag umfasst die Verarbeitung von personenbezogenen Daten zur evidenzbasierten Diagnose der Lesefähigkeit von Schülerinnen und Schülern durch verschiedene standardisierte Lesetests über die digitale *eddipuls*-Plattform und der Bereitstellung der individuellen Ergebnisse an die jeweilige Lehrkraft.

Der Auftragnehmer verarbeitet dabei personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DSGVO auf Grundlage dieses Vertrages. Die Datenschutzvereinbarungen dieses Vertrages gelten auch für Auftragsverhältnisse zwischen den Parteien, bei denen die Verarbeitung personenbezogener Daten zwar nicht intendiert ist, aber auch nicht ausgeschlossen werden kann.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in der Bundesrepublik Deutschland erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Dauer des Auftrags
Der Vertrag beginnt am 07.10.2024 und wird auf unbestimmte Zeit geschlossen. Kündigungsfrist sind 30 Tage ab Vertragsbeginn.

Der Auftraggeber kann den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragnehmers gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, der Auftragnehmer eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer Kontrollrechte des Auftraggebers vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):
Durch Weiterleitung auf die Diagnose-Plattform werden für die Zuordnung der Lehrkraft zu Schule, Klasse und den unterrichteten Schülerinnen und Schülern Daten übermittelt. Diese Daten dienen einerseits der Persistenz von Personen und Kontexten auf der Plattform, andererseits auch zur Plausibilisierung der Lehrkraft sowie der Schülerinnen und Schüler. So muss nicht nur die Lehrkraft eine Übersicht haben, welche

Schülerinnen und Schüler gerade den Test bearbeiten, sondern auch die einzelnen Schülerinnen und Schüler, ob sie sich beim richtigen Test angemeldet haben. Für die Einsicht der Ergebnisse der Lehrkraft ist es wichtig zu wissen, welche Schülerinnen und Schüler welche Ergebnisse haben.

Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14 und 15 DSGVO):

Um die oben genannten Ziele zu erreichen, sind zum einen folgende Daten nötig, die automatisch von ByCS an die Diagnose-Plattform übermittelt werden:

- Pseudonymisierte ID und Name der Lehrkraft.
- Pseudonymisierte ID und Bezeichnung der Klassen, in denen die Lehrkraft unterrichtet.
- Pseudonymisierte ID und Name der einzelnen Schülerinnen und Schüler, die den obigen Klassen zugeordnet sind.
- Schulnummer der Schule, an der die Lehrkraft unterrichtet.

Dabei werden die pseudonymisierten IDs permanent im System der Diagnose-Plattform gespeichert. Sämtliche Klarnamen werden aber nur flüchtig gespeichert und angezeigt, solange die Lehrkraft in der Diagnose-Plattform zum Zweck der Testung oder zum Zweck der Analyse der Ergebnisse eingeloggt ist.

Zum anderen umfassen die Daten der Tests durch die Schülerinnen und Schüler Folgendes:

- 2. Jahrgangsstufe: Testdaten (geschlossene Aufgaben, single choice) zur Leseflüssigkeit.
- 3. Jahrgangsstufe: Testdaten (geschlossene Aufgaben, single & multiple choice) zur Leseflüssigkeit und zum Leseverstehen.
- 4. Jahrgangsstufe: Testdaten (geschlossene Aufgaben, single & multiple choice) zur Leseflüssigkeit, zum Leseverstehen und zum Leseverstehen im digitalen Kontext

Unter Voraussetzung einer Einwilligungserklärung durch die Erziehungsberechtigten werden außerdem Daten zu Alter, Geschlecht, Selbstkonzept Lesen, Lesemotivation Sprache im Haushalt, Zahl der digitalen Medien, Häufigkeit des Vorlesens, Zugang zur Bibliothek, Anzahl der eigenen Bücher, Häufigkeit des Lesens) erfasst und zu Forschungszwecken sowie einem Bildungsmonitoring verwendet.

Die digitale Speicherung der Gesamtdaten erfolgt auf Dienstrechnern der Universität Regensburg. Diese Rechner können nur mit Passwort benutzt werden. Eine Bildschirmsperre bei Abwesenheit ist eingerichtet.

Der Zugang zu den Daten erfolgt für die Forschenden über die Plattform mit einem Passwort. Dort können die Daten in pseudonymisierter Form (ohne Klarnamen und mit gehashten IDs) via csv-Datei heruntergeladen werden.

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
Schülerinnen und Schüler, Lehrkräfte.

3. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist der Auftragnehmer verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Nr. 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

Weisungsberechtigte Personen des Auftraggebers sind:
Prof. Dr. Sven Hilbert, Lehrstuhl Educational Data Science, 0941 943 7444

Weisungsempfänger beim Auftragnehmer sind:
Dr. Mario Frei, Lehrstuhl Educational Data Science, 0941 943 7627, mario.frei@ur.de
Stefan Böhringer, Lehrstuhl Educational Data Science, 0941 943 7635, stefan.boehringer@ur.de

Für Weisung zu nutzende Kommunikationskanäle:
E-Mail und Telefonnummer

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach dokumentierten Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

Der Auftragnehmer verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden. Der Auftragnehmer hat seine technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e) und f) DSGVO). Er hat die dazu erforderlichen Angaben jeweils unverzüglich an die zuständige Stelle des Auftraggebers weiterzuleiten.

Der Auftragnehmer wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die

Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). Der Auftragnehmer sichert zu, dass er, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

Die Verarbeitung von Daten in Privatwohnungen (Tele- bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist nur mit Zustimmung des Auftraggebers gestattet. Soweit die Daten in einer Privatwohnung verarbeitet werden, ist vorher der Zugang zur Wohnung des Beschäftigten für Kontrollzwecke des Arbeitgebers vertraglich sicherzustellen. Die Maßnahmen nach Art. 32 DSGVO sind auch in diesem Fall sicherzustellen.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO bekannt sind. Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb**.**

Behördliche Datenschutzbeauftragte:
Die Datenschutzbeauftragte
0941 – 943 5376
dsb@ur.de

Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich mitzuteilen.

6. Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DSGVO. Der Auftragnehmer sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DSGVO, welche auf einem der o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig und angemessen zu überprüfen. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

Zurzeit sind für den Auftragnehmer die in Anlage 1 bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

8. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Für die auftragsgemäße Verarbeitung personenbezogener Daten wird folgende Methodik zur Risikobewertung verwendet, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt:
Der Auftraggeber prüft – jeweils unter Anwendung pflichtgemäßen Ermessens –, ob eine Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO erforderlich ist und führt diese ggf. durch. Dabei findet insbesondere ein Abgleich mit der Bayerischen Blacklist (https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf) und den Leitlinien des Europäischen Datenschutzausschusses statt. Sobald der Bayerische Landesbeauftragte für den Datenschutz eine eigene „Muss-Liste“ veröffentlicht, findet diese ebenfalls Beachtung. Die Gesamtschau der Datenkategorien, der Verarbeitungstechnik, der Umstände und Zwecke der Verarbeitung, des Umfangs an Daten, des Gefährdungspotentials für die Betroffenen und weiterer relevanter Merkmale wird mit den technischen und organisatorischen Maßnahmen des Auftragnehmers verglichen, um zu eruieren, ob ein ausreichender Datenschutz vorliegt und wie dieser ggf. noch zu verbessern ist.

Der Auftragnehmer hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DSGVO). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber mitzuteilen.

Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen. Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich.

Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten. Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

Zudem finden Sie eine ausführliche Darstellung der technischen und organisatorischen Maßnahmen der

eddipuls-Plattform der Universität Regensburg in Anlage 2.

9. Support

Um die reibungslose Nutzung der Plattform zu gewährleisten, wird ein Support-Angebot vom Auftragnehmer zur Verfügung gestellt. Dieses ist auf zwei Wegen zu erreichen:

1) Im Rahmen der Teilintegration in die *BayernCloud Schule* (ByCS) werden Support-Anfragen, die an die ByCS-Support via E-Mail oder Telefon gerichtet sind, vollständig in Form von durchnummerierten Tickets und via E-Mail an den Support von *Eddipuls* (support@eddipuls.de) weitergeleitet. Die entsprechende Ticket-Bearbeitung wird zurück an den ByCS-Support geschickt, der mit der Support-anfragenden Person in Kommunikation tritt. Beim Auftragnehmer werden diese Tickets ausschließlich zu Nachweis- sowie Optimierungszwecken gespeichert.
2) Auf der Anwendungsseite eddipuls.de wird zudem ein Support-Button angezeigt, der ebenfalls ein durchnummeriertes Ticket erstellt und die Informationen über ein direktes Kontaktformular einholt.

Der Support steht nur für Lehrkräfte zur Verfügung. In der Testumgebung der Schülerinnen und Schüler, die ohne eine Lehrkraft keine Zugangsmöglichkeit zur Plattform haben, gibt es keinen Button „Support“ und somit keine Möglichkeit, das Support-Angebot zu nutzen. Dies geschieht ausnahmslos über die Lehrkraft. Über ein Kontaktformular können die Nutzerinnen und Nutzer das Anliegen an den Support weitergeben. Die dabei hinterlegten Kontaktmöglichkeiten (Mail, Telefon) werden nur zu Kommunikationszwecken und zur Kontaktaufnahme gespeichert.
Als Anbieter wird das Ticket-System der Zammad GmbH verwendet.

10. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DSGVO

Nach Abschluss der vertraglichen Arbeiten hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen. Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

11. Haftung

Auf Art. 82 DSGVO wird verwiesen.

12. Sonstiges

Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim

Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Unterschriften

Wemding ,den 07.10.2024	Regensburg ,den 07.10.2024
Gez. Margit Stimpfle _____ Auftraggeber	 _____ Auftragnehmer

Universität Regensburg

Anlage 1 – Subunternehmer

XDEV GmbH
Postgasse 1
92637 Weiden i.d.Opf.

Pegasus GmbH
Bayernstr. 10
93128 Regenstauf

Zammad GmbH
Marienstr. 18
10117 Berlin

Universität Regensburg

Anlage 2: Technische und organisatorische Maßnahmen des Auftragnehmers für die *eddipuls* Plattform

I. Übergreifende Maßnahmen

a) Verhinderung eines unautorisierten räumlichen Zutritts, eines unautorisierten Zugangs zu Geräten und Systemen sowie eines unautorisierten Zugriffs auf Anwendungen, Dienste und Daten

(z. B. Maßnahmen zu Verhinderung eines unautorisierten Zutritts bzw. Zugangs zu Gebäuden, Räumen, Hardware, Archiven, transportablen Medien, Ausdrucken usw.; Prozesse zur Zuteilung und zum Entzug von Zutritts-, Zugangs- sowie Zugriffsdaten/-mitteln; Mobile Device Management; Identifikation und Authentifizierung inkl. Passwortschutz; Mandantentrennung; Rollen- und Berechtigungskonzept; Pseudonymisierung; Verschlüsselung; Maßnahmen gegen Schadsoftware)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:

- Maßnahmen gegen den unberechtigten Zugang/Zugriff der eingesetzten Serverinfrastruktur werden vom Dienstleister umgesetzt.
- Restriktive Zugangsberechtigung für Büroräume der Mitarbeiterinnen und Mitarbeiter, die mit Sicherheitsschlössern versehen sind (zusätzlich werden Gebäudetüren zwischen 22 und 5 Uhr durch Wachpersonal verschlossen)
- Geregelter Prozess zur zentralen Verwaltung von Benutzeridentitäten, insbesondere zur Anlage (z. B. neuer Mitarbeiter), Änderung (z. B. Namenswechsel nach Heirat) und Löschung (z. B. Weggang Mitarbeiter); Vergabe von eindeutigen Kennungen für jeden Mitarbeitenden durch Verwaltung der Universität Regensburg
- Eine zentrale Geräteverwaltung ist vorhanden (Virenscanner sowie zusätzliche Firewalls auf Endgeräten: Windows Defender, Mac.OS-Firewall)
- Verhinderung der Ausführung von (aus dem Internet) heruntergeladener Software, deren Quellen als unsicher gekennzeichnet werden
- Verwendung von individuellen Zugangskonten (Benutzername+Passwort) für Endgeräte und interne Services der Universität Regensburg (auf Campus oder außerhalb via VPN-Zugang; Benutzerberechtigungen werden über Workgroupmanager geregelt)
- Passwort-Richtlinie
    - Benutzerkonto pro Nutzer/Nutzerin
    - Verwendung von sicheren Passwörtern (u. a. Passwortlänge, regelmäßiger Wechsel, Passwortwiederholungssperre); Einhaltung der Richtlinie bei Passwort-Eingabe
    - Authentifizierung mit Benutzername und Passwort

- Zugang zum Sourcecode durch Zwei-Faktor-Authentifizierung
- Automatische Weiterleitung von E-Mails an private E-Mail-Accounts ist unterbunden
- IDM-System mit Rechtedokumentation (durch Workgroupmanager der Fakultät)
- Anpassung sicherheitsrelevanter Standardeinstellungen von neuen Programmen und IT-Systemen durch Vorkonfiguration der Programme im Softwarekatalog der Universität Regensburg
- Implementierung von Maßnahmen zur Integritätsprüfung auf Anwendungsebene
- Verpflichtung der Mitarbeitenden zur Wahrung der Vertraulichkeit von Daten anhand einer Leitlinie der Universität Regensburg
- Bei Verlassen des Arbeitsplatzes erfolgt automatische Bildschirmsperre nach spätestens 15 Minuten
- Alle Mitarbeitenden sind angehalten, die Türen Ihres Büros bei Nicht-Anwesenheit zu verschließen (die Schlüsselvergabe ist über die Verwaltung klar geregelt)

b) Netzwerk- und Transportsicherheit
(z. B. Maßnahmen für die Sicherheit von Remotezugängen; Maßnahmen für die sichere Übertragung über öffentliche Netzwerke (z. B. Internet); Schnittstellenkonzept; Absicherung interner Netzwerke insbesondere durch Netzwerksegmentierung, Netzwerküberwachung, Schwachstellenscanner, DMZ, Firewall, Verschlüsselung usw.; Maßnahmen gegen Schadsoftware)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:

- Maßnahmen zum Netzmanagement erfolgt durch den Dienstleister
- Schutz bei Übertragung von Daten vor unbefugter Kenntnisnahme durch
    - Maßnahmen zur verschlüsselten Datenübertragung werden durch den Dienstleister umgesetzt.
    - Der Zugang von Clients aus dem öffentlichen Netz erfolgt über VPN.
- Das Netzwerk ist gegen unerlaubten Zugriff durch eine Firewall geschützt.

c) Patchmanagement
(z. B. Update-Plan mit Übersicht der eingesetzten Systeme; regelmäßige Auswertung von Informationen zu Sicherheitslücken der eingesetzten Systeme)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:
- Maßnahmen zum Patchmanagement auf Systemebene erfolgt durch den Dienstleister.
- Ein Prozess zum Schwachstellen- und Patchmanagement auf Anwendungsebene ist etabliert.

d) Protokollierung
(z. B. Maßnahmen für die Nachverfolgung von Lese-, Speicher-, Änderungs-, Lösch- und Übermittlungsvorgängen inkl. Konfiguration der Speicherdauer der Protokolldaten; einfache Auswertung der Protokolldaten im Hinblick auf einschlägige Fragestellungen; Maßnahmen zur Löschung der Protokolldaten nach Ablauf der zweckgebundenen Speicherdauer)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:
- Systemprotokollierung erfolgt durch den Dienstleister gemäß Protokollierungskonzept.
- Anwendungsprotokollierung gemäß Protokollierungskonzept.
- Eine Versionierung der Anwendung wird protokolliert

e) Verhinderung unbeabsichtigter Datenverluste und Störungen
(z. B. Detektionssysteme; Sicherungs- und Wiederherstellungsinstrumente; redundanten

Systeme/Ressourcen; Notfallmanagement inkl. Wiederanlaufkonzept; vereinbarte Reaktions- und Behebungszeiten in einem Störfall sowie Erreichbarkeit außerhalb normaler Geschäftszeiten)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:

- Maßnahmen zur Detektion werden vom Dienstleister umgesetzt.
- Backup- und Wiederherstellungskonzepte sind erstellt und werden vom Dienstleister umgesetzt.
- Sicherungs- und Wiederherstellungsinstrumente durch Dienstleister geregelt (Backup-Verfahren und Recovery-Prozesse)

f) Vorfallmanagement

(z. B. Konzept für den Umgang mit Datenschutzvorfällen/-hinweisen; Datenschutz-Managementsystem)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:

- Konsequente Einbindung des DSB bei Sicherheitsfragen
- Bei Datenschutzvorfällen und -hinweisen erfolgt Meldung an Datenschutzbeauftragte der Universität Regensburg
- Die Rollen der einzelnen Mitarbeiter im Sicherheitsprozess sind festgelegt (Eskalationsprozesse bei Sicherheitsverletzung sind vorhanden)

g) Test, Prüfung und Freigabe
(z. B. Konzept für Komponenten-, Integrations-, System- und Abnahmetest inkl. Umgang mit Testdaten; Trennung Test- und Produktivsystem; Penetrationstest; Audit, Wirksamkeitsprüfung der Schutzmaßnahmen und sonstige Prüfung/Kontrolle; Zertifizierung)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:

- Durchführung von Tests gemäß Testkonzept

h) Löschung und Vernichtung
(z. B. Löschkonzept inkl. Aufbewahrungsfristen; Konzept für die Löschung/Vernichtung von Datenträgern; Konzept für den Ersatz-/Austausch von Komponenten; Anonymisierung)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:

- Es sind Maßnahmen umgesetzt, welche die Daten gemäß den vertraglichen Bestimmungen löschen bzw. vernichten.

i) Unterweisung der Beschäftigten
(z. B. Sensibilisierung der relevanten Beschäftigten hinsichtlich ihrer Aufgaben und Pflichten sowie damit zusammenhängender Datenschutzaspekte; Sensibilisierung hinsichtlich Social-Engineering-Angriffen und weiterer Angriffs-Szenarien; aktuelles Schulungs- und Unterweisungskonzept)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:

- Unterweisung aller Beschäftigten der Universität Regensburg durch Schulung für Informationssicherheit und Datenschutz mit definierten Sicherheitsleitlinien
- Regelmäßige Auffrischungsschulungen zu Informationssicherheit und Datenschutz
- Datenschutzschulungsinhalte sind für alle betroffenen Mitarbeitenden dauerhaft zugänglich

j) Auftragskontrolle
(z. B. Maßnahmen, die gewährleisten, dass die vertraglichen Vereinbarungen regelmäßig auf Rechtmäßigkeit überprüft werden; weisungsbefugte Personen auf Seiten des Auftraggebers sind benannt und beim Auftragnehmer bekannt; Kontrollmaßnahmen des Auftraggebers sind vereinbart)

In diesem Bereich wurden folgende Maßnahmen wirksam umgesetzt:

- Die Dienstleister werden vertraglich verpflichtet, entsprechend dem Schutzniveau technische und organisatorische Maßnahmen umzusetzen.
- Die Wirksamkeit der von den Dienstleistern umgesetzten Maßnahmen wird regelmäßig überprüft.

II. Verarbeitungsspezifische Maßnahmen

(Technische und organisatorische Maßnahmen, die zusätzlich dem Schutz einzelner Verarbeitungstätigkeiten aus der Anlage 2 dienen, sind an dieser Stelle zu nennen und ergänzen die übergreifenden Maßnahmen. z.B. Maßnahmen zur Sicherstellung von

- Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)

Kennzeichnung erfasster Daten

  - Zuordnung einzelner Schulen über die ByCS-Schulnummer
  - Zuordnung einzelner Support-Anfragen über Ticketsystem (Harmonisierung mit ByCS)

- Richtigkeit (Art. 5 Abs. 1 lit. d DS-GVO)
- Rechenschafts- und Nachweisfähigkeit (Art. 5 Abs. 2, Art. 7 Abs. 1, Art. 24 Abs. 1, Art 28 Abs. 3 lit. a, Art. 30, Art. 33 Abs. 5, Art. 35, Art. 58 Abs. 1 lit. a und lit. e DS-GVO)
- Transparenz für Betroffene (Art. 5 Abs. 1 lit a, Art. 12 Abs. 1 und 3 bis Art. 15, Art. 34 DS-GVO)
- Unterstützung bei der Wahrnehmung von Betroffenenrechten (Art. 12 Abs. 2 DS-GVO)