Untis GmbH
Belvederegasse 11
A-2000 Stockerau

+43 2266 62241
office@untis.at
www.untis.at

Vertrag

über die

Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO (AVV)

Der Verantwortliche:

(nachstehend **Auftraggeber** genannt)

Der Auftragsverarbeiter:

Untis GmbH
Belvederegasse 11
AT-2000 Stockerau

(nachstehend **Auftragnehmer** genannt)

gemeinsam auch **die Parteien** genannt

§ 1 Vertragsgegenstand

(1) Der Auftragnehmer erbringt für den Auftraggeber Leistungen auf Grundlage des zwischen den Parteien geschlossenen Nutzungsvertrages oder, sofern es sich um eine unentgeltliche Test- oder Demoversion für einen beschränkten Zeitraum handelt, auf Grundlage einer konkreten Vereinbarung. Dabei verarbeitet der Auftragnehmer personenbezogene Daten i.S.d. Art. 4 Nr. 4 DSGVO für den Auftraggeber (nachfolgend „Auftraggeber-Daten" genannt) ausschließlich im Auftrag und nach Weisung des Auftraggebers. Rahmen und Umfang der Datenverarbeitung ergeben sich aus dem Nutzungsvertrag.

(2) Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung. Den Auftragnehmer trifft keinerlei Verpflichtung, Weisungen des Auftraggebers (datenschutz-)rechtlich zu prüfen. Ist der Auftragnehmer jedoch der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, wird er den Auftraggeber darauf hinweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis die Weisung bestätigt oder geändert wird. Räumt der Auftraggeber auf die Information über eine nach Ansicht des Auftragnehmers rechtswidrige Weisung die Bedenken des Auftragnehmers nicht aus, kann dieser die Durchführung der betreffenden Weisung ablehnen, soweit sie seine Verantwortungssphäre betrifft.

(3) Dieser Vertrag nimmt Bezug auf die folgenden durch den Auftragnehmer durchgeführten Tätigkeiten, deren konkrete Art und Umfang sich aus den jeweils geschlossenen Hauptverträgen ergibt:

- Betrieb der Web-Leistungen der Untis Plattform entsprechend des durch den Auftraggeber gebuchten Leistungsumfangs, um diese den Kunden über das Internet zur Verfügung zu stellen, einschließlich der Bereitstellung der Mobile App, eine für mobile Endgeräte bereitgestellte Anwendung zum Zugriff auf und zur Nutzung der Web-Leistungen, sofern diese durch die nutzende Person aktiviert wird,

- Durchführen von Unterstützungsleistungen für die Applikationen der der Untis Plattform entsprechend des durch den Auftraggeber gebuchten Leistungsumfangs und der Mobile App,

- Durchführen von Wartungstätigkeiten für die Applikationen der Untis Plattform entsprechend des durch den Auftraggeber gebuchten Leistungsumfangs,

- Bereitstellung von individuellen Integrationslösungen von Drittanbietern auf der WebUntis-Plattform.

(4) Dieser Vertrag konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit den Auftraggeber-Daten in Erfüllung des Nutzungsvertrags.

§ 2 Dauer der Verarbeitung

(1) Laufzeit und Kündigung dieses Vertrags richten sich nach den Bestimmungen zu Laufzeit und Kündigung des Nutzungsvertrags. Eine Kündigung des Nutzungsvertrags bewirkt automatisch auch eine Kündigung dieses Vertrages.

(2) Eine isolierte Kündigung dieses Vertrages ist ausgeschlossen.

§ 3 Umfang, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, Kategorien betroffener Personen

(1) Der Auftragnehmer verarbeitet die Auftraggeber-Daten ausschließlich im Auftrag und nach dokumentierter Weisung des Auftraggebers. Der Auftraggeber bleibt Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO.

(2) Die Verarbeitung der Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erfolgt entsprechend der in **Anlage 1** zu diesem Vertrag enthaltenen Festlegungen zu Art und Zweck der Datenverarbeitung. Sie bezieht sich auf die in **Anlage 1** festgelegte Art der Auftraggeber-Daten und die dort aufgeführten Kategorien betroffener Personen.

(3) Die Verarbeitung der Auftraggeber-Daten findet im Gebiet der Republik Österreich, Bundesrepublik Deutschland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Dies gilt auch für Auftraggeber mit Sitz außerhalb der EU bzw. des EWR.

§ 4 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung sowie für die Wahrung der Rechte der betroffenen Personen aus den Art. 12 bis 22 DSGVO ist der Auftraggeber allein verantwortlich.

(2) Die Verarbeitung der Auftraggeber-Daten durch den Auftragnehmer im Rahmen dieser Vereinbarung erfolgt ausschließlich nach Weisung des Auftraggebers gemäß Art. 28 Abs. 3 S. 2 lit. a DSGVO, es sei denn, der Auftragnehmer ist nach dem Recht der Europäischen Union oder dem Recht des Mitgliedstaates, dem er unterliegt, zur weiteren Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(3) Der Auftraggeber behält sich im Rahmen der in dieser Vereinbarung getroffenen Auftragsbeschreibung ein umfassendes Weisungsrecht über Art und Zwecke der Datenverarbeitung vor, dass er durch Einzelweisungen konkretisieren kann.

(4) Einzelweisungen nach Abschluss des Vertrages bedürfen der Textform und sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren.

(5) Erteilt der Auftraggeber Einzelweisungen hinsichtlich des Umgangs mit Auftraggeber-Daten, die über den im Nutzungsvertrag vereinbarten Leistungsumfang hinausgehen sind die dadurch begründeten Kosten vom Auftraggeber zu tragen.

(6) Der Auftraggeber informiert den Auftragnehmer unverzüglich und vollständig, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung von Auftraggeber-Daten durch den Auftragnehmer oder seiner Weisungen feststellt.

(7) Weisungsberechtigte Personen des Auftraggebers sind:

_____

(Vorname, Name, E-Mail-Adresse, Telefon)

Weisungsempfänger beim Auftragsverarbeiter ist:

Der / die Datenschutzbeauftragte der Untis GmbH, Belvederegasse 11, A-2000 Stockerau; datenschutz@untis.at

(8) Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

§ 5 Pflichten des Auftragnehmers

(1) Der Auftragnehmer stellt sicher, dass die Verarbeitung der Auftraggeber-Daten im Rahmen der Leistungserbringung nach dem Nutzungsvertrag in seinem Verantwortungsbereich, der die Unterauftragnehmer nach § 9 dieses Vertrags einschließt, in Übereinstimmung mit den Bestimmungen dieses Vertrages erfolgt.

(2) Der Auftragnehmer ist verpflichtet, dem Auftraggeber auf Antrag die erforderlichen Informationen, einschließlich Zertifizierungen sowie Überprüfungs- und Inspektionsergebnisse, die dem Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten dienen, zur Verfügung zu stellen.

(3) Der Auftragnehmer hat die zur Verarbeitung von Auftraggeber-Daten befugten Personen gemäß Art. 28 Abs. 3 lit. b DSGVO schriftlich zur Vertraulichkeit zu verpflichten, sofern diese nicht bereits einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(4) Der Auftragnehmer ist verpflichtet, einen fachkundigen und zuverlässigen Datenschutzbeauftragten schriftlich zu bestellen, der seine Tätigkeit gemäß der Art. 37, 38 und 39 DSGVO ausüben kann, sofern und solange die gesetzlichen Voraussetzungen für eine Bestellpflicht gegeben sind. Der Auftragnehmer wird die aktuellen Kontaktdaten des Datenschutzbeauftragten auf seiner Webseite leicht zugänglich hinterlegen (Art. 37 Abs. 7 DSGVO).

(5) Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, das alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält. Diese Pflicht besteht nicht, wenn die Voraussetzungen von Art. 30 Abs. 5 DSGVO erfüllt sind.

(6) Der Auftragnehmer darf ohne vorherige Zustimmung durch den Auftraggeber im Rahmen der Auftragsverarbeitung keine Kopien oder Duplikate der Auftraggeber-Daten anfertigen. Hiervon ausgenommen sind jedoch Kopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung und zur ordnungsgemäßen Erbringung der Leistungen gemäß dem Nutzungsvertrages (einschließlich der Datensicherung) erforderlich sind, sowie Kopien, die zur Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(7) Der Auftragnehmer ist verpflichtet den Auftraggeber, im Rahmen des Zumutbaren und Erforderlichen sowie gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten, bei der Erfüllung von dessen Pflichten aus Art. 12 bis 22 sowie Art. 32 bis 36 DSGVO zu unterstützen. Die Unterstützung erfolgt unter Berücksichtigung der Art der Verarbeitung und der dem Auftragnehmer zur Verfügung stehenden Informationen sowie nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen, insbesondere bei der Beantwortung von Anträgen auf Wahrnehmung der entsprechend in Art. 12 bis 22 DSGVO genannten Rechte der betroffenen Personen (§ 10).

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft die erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere die in

Anlage 2 aufgeführten Maßnahmen der Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungskontrolle.

(2) Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, ist es dem Auftragnehmer gestattet, alternative und adäquate Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in **Anlage 2** festgelegten Maßnahmen nicht unterschritten wird. Der Auftragnehmer wird solche Änderungen dokumentieren. Wesentliche Änderungen der Maßnahmen bedürfen der vorherigen Zustimmung des Auftraggebers.

§ 7 Mitzuteilende Verstöße des Auftragnehmers

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er feststellt, dass er oder ein Mitarbeiter bei der Verarbeitung von Auftraggeber-Daten gegen datenschutzrechtliche Vorschriften oder gegen Festlegungen aus diesem Vertrag verstoßen haben, sofern die Gefahr einer Verletzung des Schutzes personenbezogener Daten des Auftraggebers im Sinne des Art. 4 Nr. 12 DSGVO besteht.

(2) Soweit den Auftraggeber aufgrund eines Vorkommnisses nach Absatz (1) gesetzliche Informationspflichten wegen einer unrechtmäßigen Kenntniserlangung von Auftraggeber-Daten (insbesondere nach Art. 33 und 34 DSGVO) treffen, hat der Auftragnehmer den Auftraggeber bei der Erfüllung der Informationspflichten auf dessen Ersuchen im Rahmen des Zumutbaren und Erforderlichen gegen Erstattung der dem Auftragnehmer hierdurch entstehenden Aufwände und Kosten zu unterstützen.

(3) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen, informiert hierüber den Auftraggeber und ersucht um weitere Weisungen.

(4) Meldungen nach Art. 33 oder 34 DSGVO für den Auftraggeber darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers durchführen.

§ 8 Kontrollrechte des Auftragsgebers

(1) Der Auftraggeber überzeugt sich auf eigene Kosten vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß **Anlage 2** und dokumentiert das Ergebnis. Dies geschieht durch Einholung einer Selbstauskunft des Auftragnehmers, die dieser auch durch Vorlage eines geeigneten Zertifikats eines Sachverständigen erfüllen kann.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf schriftliche Anforderung alle erforderlichen Auskünfte und Informationen bezüglich seiner Pflichten aus dieser Vereinbarung zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen der **Anlage 2** nachzuweisen. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann durch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 oder Zertifizierungen nach gemäß Art. 42 DSGVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz), erfolgen.

(3) Der Auftraggeber oder ein entsprechend Beauftragter haben das Recht vorgenannte Kontrollen zu den üblichen Geschäftszeiten vorzunehmen. Diese Kontrollen sind rechtzeitig (in der Regel

mindestens zwei Wochen vorher) anzukündigen und haben den Betriebsablauf beim Auftragnehmer so wenig wie möglich zu beeinträchtigen.

(4) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich ebenso zu verpflichten, wie auch der Auftraggeber aus diesem Vertrag verpflichtet ist. Zudem hat er den Dritten auf Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitsverpflichtung unterliegt. Auf Verlangen des Auftragnehmers hat der Auftraggeber diesem die Verpflichtungsvereinbarungen mit dem Dritten vorzulegen. Der Auftraggeber darf keinen Wettbewerber des Auftragnehmers mit der Kontrolle beauftragen.

§ 9 Unterauftragsverhältnisse

(1) Der Auftraggeber stimmt der Beauftragung der in **Anlage 3** aufgeführten Unterauftragnehmer unter der Bedingung einer vertraglichen Vereinbarung nach Maßgabe des Art. 28 Abs. 1 bis 4 DSGVO ausdrücklich zu. Dem Auftragnehmer ist die Beauftragung weiterer Unterauftragnehmer (weitere Auftragsverarbeiter) gestattet.

(2) Der Auftragnehmer wird den Auftraggeber unverzüglich über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Unterauftragnehmer informieren. Gegen derartige Änderungen darf der Auftraggeber aus wichtigem, dem Auftragnehmer nachzuweisenden Grund, Einspruch erheben. Der Einspruch ist binnen einer Frist von einer Woche ab Zugang einer entsprechenden Mitteilung des Auftragnehmers schriftlich auszusprechen.

(3) Keiner Mitteilung bedarf die Einschaltung von Unterauftragnehmern, bei denen der Unterauftragnehmer lediglich eine Nebenleistung zur Unterstützung bei der Leistungserbringung nach dem Nutzungsvertrag in Anspruch nimmt, z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder zur Entsorgung von Datenträgern sowie für sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen, auch wenn dabei ein Zugriff auf Auftraggeber-Daten nicht ausgeschlossen werden kann. Der Auftragnehmer wird auch diese mit der gebotenen Sorgfalt auswählen und im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Schutz der Auftraggeber Daten zu gewährleisten.

(4) Im Fall der Hinzuziehung eines Unterauftragnehmers erlegt der Auftragnehmer diesem, im Wege eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats, dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind. Der Vertrag ist so auszugestalten, dass es dem Auftraggeber möglich ist, im Bedarfsfall angemessene Überprüfungen und Inspektionen beim Unterauftragnehmer, auch vor Ort durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

(5) Sofern eine Einbeziehung von Unterauftragnehmern in einem Drittstaat erfolgen soll, stellt der Auftragnehmer sicher, dass beim Unterauftragnehmer ein entsprechendes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis von EU-Standarddatenschutzklauseln).

(6) Auf Verlangen wird der Auftragnehmer dem Auftraggeber den Abschluss der vorgenannten Vereinbarungen mit seinen Unterauftragnehmern nachweisen.

§ 10 Rechte der betroffenen Personen

(1) Die Rechte der durch die Datenverarbeitung betroffenen Personen sind gegenüber dem Auftraggeber geltend zu machen.

(2) Soweit eine betroffene Person sich unmittelbar an den Auftragnehmer zur Wahrnehmung ihrer Rechte gemäß der Art. 12 bis 22 DSGVO der sie betreffenden Daten wenden sollte, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen.

(3) Im Übrigen gilt § 5 Abs. (7)(6) dieser Vereinbarung.

§ 11 Haftung

(1) Für den Ersatz von Schäden, die eine Person wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverhältnisses erleidet, haften Auftraggeber und Auftragnehmer als Gesamtschuldner.

(2) Für den Ersatz von Schäden, die eine betroffene Person wegen einer nach dem geltenden Datenschutzrecht unzulässigen oder unrichtigen Verarbeitung von Auftraggeber-Daten im Rahmen der Auftragsverarbeitung erleidet, ist im Innenverhältnis zum Auftragnehmer alleine der Auftraggeber verantwortlich.

(3) Der Auftraggeber verpflichtet sich, den Auftragnehmer im Innenverhältnis von allen Ansprüchen Dritter frei zu stellen, solange und soweit er nicht nachweist, dass der Auftragnehmer seinen speziell den Auftragnehmer treffenden Pflichten aus der DSGVO nicht nachgekommen ist oder unter Nichtbeachtung einer rechtmäßig erteilten Weisung des Auftraggebers oder gegen eine rechtmäßig erteilte Weisung gehandelt hat.

(4) Sollte eine Datenschutzbehörde oder ein Gericht gegen den Auftragnehmer eine Geldbuße auf Grund einer Datenverarbeitung des Auftragnehmers verhängen, die auf einer Weisung des Auftraggebers beruht, hat der Auftraggeber dem Auftragnehmer den entsprechenden Betrag auf schriftliche Mitteilung hin in voller Höhe innerhalb von 30 Tagen ab der schriftlichen Mitteilung zu erstatten.

(5) Der Auftraggeber hat dem Auftragnehmer sämtliche sich aus der von ihm zu vertretenden Rechtsverletzung gemäß Absatz 3 und 4 ergebenden Kosten zu erstatten, einschließlich der Kosten der Rechtsverfolgung.

(6) Unbeschränkte Haftung: Der Auftragnehmer haftet unbeschränkt für Vorsatz und grobe Fahrlässigkeit, bei Verletzung einer vertraglich gewährten Garantie sowie nach Maßgabe des Produkthaftungsgesetzes. Für leichte Fahrlässigkeit haftet der Auftragnehmer bei Schäden aus der Verletzung des Lebens, des Körpers und der Gesundheit von Personen. Im Übrigen gilt folgende beschränkte Haftung: Bei leichter Fahrlässigkeit haftet der Auftragnehmer nur im Falle der Verletzung einer wesentlichen Vertragspflicht des Nutzungsvertrages, deren Erfüllung die ordnungsgemäße Durchführung des Nutzungsvertrages überhaupt erst ermöglicht und auf deren Einhaltung der Auftraggeber regelmäßig vertrauen darf (Kardinalpflicht). Die Haftung für leichte Fahrlässigkeit ist der Höhe nach beschränkt auf die bei Vertragsschluss vorhersehbaren Schäden, mit deren Entstehung typischerweise gerechnet werden muss.

§ 12 Rückgabe und Löschung überlassener Auftraggeber-Daten

(1) Der Auftragnehmer hat sämtliche Auftraggeber-Daten nach Beendigung der vertragsgegenständlichen Leistungserbringung (insbesondere bei Ablauf der vereinbarten unentgeltlichen Test- oder Demoversion, Kündigung oder sonstiger Beendigung des Nutzungsvertrages), nach Wahl des Auftraggebers, zurückzugeben oder zu löschen und bestehende Kopien zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der Daten besteht.

(2) Der Auftragsnehmer hat die Löschung bzw. Vernichtung von Auftraggeber-Daten zu dokumentieren und den Nachweis dem Auftraggeber auf Anforderung nachzuweisen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung oder gesetzlichen Aufbewahrungsfristen dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 13 Sonstiges

(1) Soweit in diesem Vertrag keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Nutzungsvertrages. Im Fall von Widersprüchen zwischen diesem Vertrag und Regelungen aus sonstigen Vereinbarungen, insbesondere aus dem Nutzungsvertrag, gehen die Regelungen aus diesem Vertrag vor.

(2) Der Auftraggeber und der Auftragnehmer und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Anlagen:

Anlage 1 Zwecke und Art der Datenverarbeitung, Art der Daten und Kategorien betroffener Personen
Anlage 2 Technische und organisatorische Maßnahmen
Anlage 3 Zulässige Unterauftragnehmer

Anlage 1 – Zweck und Art der Datenverarbeitung, Art der Daten und Kategorien der betroffenen Personen

Der Auftragnehmer erbringt die nach dieser Anlage vereinbarten Leistungen gegenüber dem Auftraggeber ausschließlich nach Weisung des Auftraggebers und auf Grundlage der zwischen den Parteien geschlossenen Vereinbarung über die Verarbeitung personenbezogener Daten im Auftrag.

Der Auftragnehmer verarbeitet im Auftrag des Auftraggebers nachfolgende personenbezogene Daten zu den genannten Zwecken:

Art der Daten	**Art und Zweck der Datenverarbeitung**	**Kategorien der betroffenen Personen**
Grundlegend erfolgen folgende Verarbeitungen: • Kurzname • Nachname • Text • Titel • Vorname • Personalnummer • E-Mail Adresse • Telefonnummer • Geburtsdatum • Eintrittsdatum • Austrittsdatum • Mobiltelefon • Geschlecht • Stundenplan/Veranstaltungsplan	Es erfolgt eine Speicherung dieser Daten. Im Rahmen des Hostings und Betriebs ist ein Zugriff auf diese Daten nicht ausgeschlossen. Möglicherweise erfolgt dabei weisungsgebundene Anpassung, Veränderung, ein Auslesen, Abfragen, eine Verwendung, oder die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung oder der Abgleich dieser Daten.	Lehrer*innen/Dozent*innen
Bei Web App (SaaS) gilt zusätzlich: • Aktiv • ID • Externe Id • Lehrerstatus/Dozentenstatus • Soll/Woche • Lehrperson/Dozent (Abrechnungsrelevanz) • Andere Tätigkeiten [%] • Raum • Zugewiesene Abteilungen • Foto • Zugewiesene Lehrbefähigungen • Klassenvorstand der Klassen /Vorstand der Semester • Vordergrundfarbe • Hintergrundfarbe • Faxnummer • Straße • Postleitzahl	wie zuvor	Lehrer*innen/Dozent*innen

• Stadt • technische Protokolldaten • Abwesenheiten (auch mit Begründung) • Anrechnungen • Lehrstoff • Hausaufgaben • Prüfungen		
Bei Web App (SaaS) gilt zusätzlich: • Foto • Nachname • Vorname • Kurzname • ID • Externe ID • Nationale ID • Geburtsdatum • Geschlecht • Eintrittsdatum • Austrittsdatum • Klasse/Semester • Text • Attestpflicht • Schulpflicht • Volljährig • Katalognummer • Vordergrundfarbe • Hintergrundfarbe • E-Mail Adresse • Mobiltelefon • Telefonnummer • Faxnummer • Straße • Aktiv • Postleitzahl • Stadt • technische Protokolldaten • Stundenplan	wie zuvor	Schüler*innen/Student*innen
Bei Verwendung von Klassenbuch zusätzlich: • Abwesenheiten • Klassenbucheinträge • Noten • Befreiungen • Klassendienste • Lehrstoff • Hausaufgaben • Prüfungen	wie zuvor	Schüler*innen/Student*innen
Bei Web App (SaaS) gilt zusätzlich: • Benutzername • ID • Fremdbenutzername	wie zuvor	Benutzer (Eltern/Erziehungsberechtigte, Lehrer*innen/Dozent*innen, Schüler*innen/Student*innen)

• Personenrolle • Person • Benutzergruppe • Benutzerzugang aktiv • Benutzerzugang gesperrt • Sprache • E-Mail Adresse • Letzte Anmeldung • Passwort • Google Authenticator Schlüssel • Office 365 Identität		
Bei Web App (DaaS) gilt zusätzlich: • Beschreibung • Statistik-Kennzeichen • Status • Abteilungen • Stammschule • Pers.Nr 2 (Ö) • PM-SAP-Nummer (Ö) • Gesicherte Stunden (Ö) • Zeitwünsche • Vordergrundfarbe • Hintergrundfarbe • Klassenlehrer	wie zuvor	Lehrer*innen/Dozent*innen
Bei Verwendung von Unterrichtsplanung und Wertrechnung zusätzlich: • Lehrbefähigungen • Soll/Woche • Ist-Soll Werte • Anrechnungen • Unterrichtswerte • Wertkorrekturen • Stundensatz	wie zuvor	Lehrer*innen/Dozent*innen
Bei Verwendung von Kursplanung und/oder Studentenstundenplan zusätzlich: • Kurzname • Nachname • Text • Beschreibung • Statistik-Kennzeichen • Vorname • Nummer des Studenten • Klasse des Studenten • Geburtsdatum • Optimierungskennzeichen • Geschlecht (männl., weibl., x (inter)) • E-Mail Adresse • Klausuren	wie zuvor	Schüler*innen/Student*innen
Bei Verwendung von Vertretungsplanung zusätzlich: • Abwesenheiten • Abwesenheitsgründe • Bereitschaften	wie zuvor	Lehrer*innen/Dozent*innen

• Vertretungen • Entfälle • Betreuungen • Vertretungszähler • Wertkorrektur • Veranstaltungen • Vormerkungen • Klausuren		
Bei Verwendung von Abteilungsstundenplan zusätzlich: • Abteilung	wie zuvor	Lehrer*innen/Dozent*innen
Bei Verwendung von Untis MultiUser zusätzlich: • Externer Name • Benutzername • Benutzerrechte	wie zuvor	Lehrer*innen/Dozent*innen, Schulleitung, Schulbüro
Bei Verwendung von Pausenaufsichten zusätzlich: • Pausenaufsichten • Max. Minuten • Pausenaufsichtsvertretungen (in • Kombination mit Modul Vertretungsplanung)	wie zuvor	Lehrer*innen/Dozent*innen
WebApp (DaaS) Benutzer: • Benutzername • Vorname • Nachname • E-Mail Adresse	wie zuvor	Lehrer*innen/Dozent*innen, Schulleitung, Schulbüro

Anlage 2 - Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Untis verfügt über eine durchgängig gültige ISO 27001 Zertifizierung.

Nachfolgend findet sich eine auszugsweise Beschreibung der getroffenen technischen und organisatorischen Maßnahmen des Auftragnehmers zur Umsetzung und Einhaltung der Vorgaben nach Art. 32 DSGVO.

Vertraulichkeit

Zutrittskontrolle

Die Server für den Betrieb der Webapplikationen der Untis Plattform sind in Wien bei dem Housingprovider Firma next layer Telekommunikationsdienstleistungs- und Beratungs GmbH untergebracht. Der Housingprovider gewährleistet in ihren Housingzentren die Zutrittskontrolle durch eine Zutrittskontroll- und Überwachungsanlage, eine Videoüberwachungsanlage und Wachpersonal. Es besteht ein mehrstufiges System zur Identifikation von zutrittsberechtigten Personen (ID-Karte, Fingerabdrucksprüfung).

Der physische Zutritt zu den Servern ist durch einen abgesperrten Serverschrank im zugangskontrollierten Gebäude gegeben. Die Schlüsselvergabe ist genau geregelt und auf die notwendigen Personen beschränkt.

Zugangskontrolle

Nur ausgewählte und an das jeweilige Housingzentrum und den jeweiligen Housingprovider namentlich genannte Mitarbeiter haben Zugang zu den Servern, auf welchen die Webapplikationen der Untis Plattform und/oder deren Erweiterungsmodule betrieben werden. Diese Server werden daher auch ausschließlich von Mitarbeitern von UNTIS GMBH oder deren Partnern betreut und gewartet.

Die Serversysteme sind über das Internet ausschließlich über einen VPN-Zugang zu erreichen. Die Zugangspasswörter unterliegen einem Passwortmanagement, das dem derzeitigen Stand der Technik entspricht und laufend dem aktuellen Stand der Technik angepasst wird.

Zugriffskontrolle

Die Applikationen der Untis Plattform und Ihre Erweiterungsmodule verfügen über passwort-geschützte Benutzerzugänge. Das Berechtigungssystem ermöglicht Zugriffs- und Zuständigkeitsbeschränkungen. Eine Firewall schützt die Server vor unbefugtem Zugriff. Die Hostingprovider haben keine Befugnis zum Zugriff auf die Server von UNTIS GMBH und deren Partner. Die Untis Plattform Daten der einzelnen Auftraggeber sind in getrennten Datenbanken gespeichert. Ein Vermischen der Datenbestände und ein gegenseitiger Zugriff verschiedener Auftraggeber sind durch die konkrete Zuordnung von bestimmten Datenbereichen zu bestimmten Auftraggebern nicht möglich.

Verarbeitungskontrolle

Sämtliche relevante Daten werden während der Verarbeitung durch entsprechende Protokolle bzw. Sicherheitsmaßnahme (z.B. Verschlüsselung, etc.) vor unberechtigtem Zugriff geschützt.

Integrität

Weitergabekontrolle

Durch den Einsatz entsprechender Verschlüsselungskontrolle bzw. entsprechender Übertragungsprotokolle ist die Veränderung von Daten während des Transports bzw. bei der Speicherung und Verarbeitung ausgeschlossen. Zur Gewährleistung der Weitergabekontrolle werden sämtliche personenbezogene Daten während der Übermittlung in den genannten Fällen einer https-Verschlüsselung (nach dem Stand der Technik) unterzogen.

Eingabekontrolle

Die Veränderung personenbezogener Daten wird durch entsprechende Zugriffsbeschränkungen eingeschränkt, bzw. ist durch geeignete Maßnahmen nachvollziehbar. Jede Anmeldung am System wird protokolliert und sämtliche zur Rückverfolgung erforderliche Daten werden festgehalten. Erfolglose Anmeldungen werden ebenso erfasst. Sämtliche Änderungen an den Bewegungsdaten werden von der Untis Plattform automatisch protokolliert. Dies beinhaltet sowohl die inhaltliche Änderung als auch von wem die Änderung durchgeführt wurde.

Auftragskontrolle

Es werden keine Auftragsverarbeiter im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung; z.B. ISO27001, etc.), Vorabüberzeugungspflicht, Nachkontrollen eingesetzt.

Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle

Die Verfügbarkeit und Stabilität der Systeme ist durch technische und organisatorische Maßnahmen sichergestellt:

- Backup-Strategie (online/offline; on-site/off-site)
- Notfallplanung
- Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
- Firewall-Systeme nach aktuellem Stand der Technik
- Distributed Denial of Service (DDoS) Schutz (vUntis und WebUntis)
- Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
- Hinterlegung der Zugangsdaten in Banktresor
- Regelmäßige Restore-Tests

Gespiegelte Festplatten im jeweiligen Server, Datenbankreplikation auf einen zweiten Server und tägliches Backup schützen die Daten vor zufälliger Zerstörung oder Verlust. UNTIS GMBH und deren Partner verarbeiten personenbezogene Daten ausschließlich im Rahmen des gegenständlichen Services und entsprechend den Weisungen des Auftraggebers. Sie verwenden die zur Datenverarbeitung überlassenen Daten für keine anderen Zwecke. Um die Daten vor zufälliger Zerstörung oder Verlust zu schützen, werden in regelmäßigen Abständen Replikationen und Backups der Daten hergestellt. Dem Auftraggeber wird in diesem Zusammenhang zugesichert, täglich Backups (Datensicherungen) bis 1 Monat in die Vergangenheit sowie monatlich (jeweils am Ersten eines jeden Monats) entsprechende Datensicherungen bis 6 Monate in die Vergangenheit vorzunehmen. Andere Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Dem Auftraggeber wird darüber hinaus zugesichert, die im Rahmen des Services bekannt gegebenen personenbezogenen Daten des Auftraggebers, bzw. die vom Auftraggeber in WebUntis oder dessen Erweiterungsmodule eingegebenen personenbezogenen Daten von Schülerinnen und Schülern, Studentinnen und Studenten sowie von Lehrpersonal geheim zu halten.
Darüber hinaus besteht für den Auftraggeber selbst jederzeit die Möglichkeit, ein Backup seiner Daten anzulegen.

Wiederherstellbarkeit

Die rasche Widerherstellbarkeit wird durch entsprechende Segmentierung der Daten erreicht, wodurch bspw. im Fehlerfall nur die betroffenen Datenstände wiederhergestellt werden müssen.

Datenlöschung

Bei Beendigung der Zusammenarbeit können Daten durch einen simplen Befehl sofort gezielt gelöscht werden. Die Löschung aus den Backups erfolgt dann ebenfalls fristgerecht durch einen geregelten Prozess. Während der Zusammenarbeit erfolgt die Löschung entsprechend der Vorgaben des Auftraggebers.

Maßnahmen zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Ein entsprechendes Datenschutz-Management einschließlich regelmäßiger Mitarbeiter-Schulungen ist etabliert.

Ein etabliertes Incident-Response-Management ist vorhanden. Es werden regelmäßige Audits zur Feststellung des adäquaten Schutzniveaus durchgeführt. Sämtliche Voreinstellungen sind datenschutzfreundlich umgesetzt.

Anlage 3 - Genehmigte Unterauftragnehmer

Firma Unterauftragnehmer	Anschrift/Land	Leistung
next layer Telekommunikationsdienstleistungs- und Beratungs GmbH	Mariahilfer Gürtel 37/7 1150 Wien Österreich	Betrieb der Server-Infrastruktur der Untis Plattform
Sleekplan GmbH	Georgenstrasse 66 80799 München Deutschland	Versenden von Neuigkeiten und Erhalten von Feedbackbeiträgen Es findet kein Drittstaatentransfer der Daten statt.
SFDC Ireland Limited	Salesforce Tower 60 R801 North Dock Irland	Betrieb des Tools „Salesforce“ Ticketsystem zur Bearbeitung von Kundenanfragen Es findet kein Drittstaatentransfer der Daten statt.
Google Ireland Limited	Gordon House, Barrow Street, Dublin 4, Irland	Die Mobile App nutzt von Firebase (ein Produkt von Google) bereitgestellte Dienste: • Firebase Cloud Messaging, für das Versenden von Push-Nachrichten, • Firebase Crashlytics, für die Auswertung automatisch erstellter Fehlermeldungen (z.B. bei Abstürzen), • Firebase Remote Config, für Konfigurationsanpassungen in der App, ohne eine neue Version im Store veröffentlichen zu müssen.
Prof. Mag. Michael Kurzthaler	Helenen-Weg 8b 9900 Lienz Österreich	Support- und Service-Dienstleistungen für die Untis Plattform im Bundesland Kärnten und Tirol
Franz Stefan Schreiner	Grymgasse 16 3100 St. Pölten Österreich	Support- und Service-Dienstleistungen für die Untis Plattform im Bundesland Niederösterreich und Oberösterreich
Educ Oy Tuomas Heinonen	Mäntytie 7 86300 Oulainen Finnland	Support- und Service-Dienstleistungen für die Untis Plattform für das Land Finnland
Dialog Computer Systeme GmbH	Helmholtzstr. 2-9 10587 Berlin Deutschland	Support- und Service-Dienstleistungen für die Untis Plattform in den Bundesländern Berlin und Sachsen
PEDAV das Softwarehaus für Schulen GmbH & Co. KG	Schönebecker Straße 1 45359 Essen Deutschland	Support- und Service-Dienstleistungen für die Untis Plattform in den Bundesländern Nordrhein-Westfalen und Hessen
TechTalk GmbH	Leonard-Bernstein-Straße 10 1220 Wien Österreich	2nd-Level Support- und Service-Dienstleistungen für Untis Connector für Moodle und Untis Connector für Teams
LUMASERV GmbH	Universitätsstraße 3 56070 Koblenz Deutschland	2nd-Level Support- und Service-Dienstleistungen für Kurswahl und Notfallhilfe

Bei Aktivierung der folgenden optionalen Integrationen von Drittanbietern über die WebUntis (Integrations-)Plattform durch den Auftraggeber wird der Betreiber dieser Integration

("Integrationspartner") zum Zweck des Betriebs dieser Integrationen zusätzlich zu einem Sub-Auftragsverarbeiter der Untis GmbH, dessen Einsatz durch den Auftraggeber von Anfang an genehmigt wird:

Firma Unterauftragnehmer	**Anschrift/Land**	**Leistung**
Untis Development GmbH	Zum Schwimmbad 44 65232 Taunusstein Deutschland	Betrieb, Wartung und Support der Integrationen WebUntis Schuljahreskalender und WebUntis Noten
eAsistent	Cerkvena ulica 11 4290 Tržic Slovenia	Betrieb, Wartung und Support der Integration „eAssistent" Messenger
Sdui GmbH	Universitätsstrasse 3 56070 Koblenz Deutschland	Betrieb, Wartung und Support der Integration „Sdui" Messenger