Ausfüllhilfe für die Vereinbarungen zur DSGVO

Vereinbarung

über eine

Auftragsverarbeitung nach Art 28 EU Datenschutz-Grundverordnung

Der Verantwortliche:

Tragen Sie hier den Schulnamen & die Adresse der Schule ein

(im Folgenden Auftraggeber)

Der Auftragsverarbeiter:

Untis Baden-Württemberg GmbH
Benzstr. 8
70839 Gerlingen

(im Folgenden Auftragnehmer)

1. GEGENSTAND DER VEREINBARUNG

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:

- Support-Leistungen für die Applikationen Untis und WebUntis auf Basis vom § 3 des Service- und Updatevertrages.

(2) Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten (Art. 4 Nr. 1, 13, 14, 15 DSGVO)	**Kreis der Betroffenen** (Art. 4 Nr. 1 DSGVO)	**Art der Verarbeitung** (Art. 4 Nr. 2 DSGVO)
• Foto • Familienname • Vorname • Kurzname • Externe Id • Geburtsdatum • Geschlecht • Eintrittsdatum • Austrittsdatum • Klasse • Text • Attestpflicht • Schulpflicht • Volljährig • Katalognummer • Vordergrundfarbe • Hintergrundfarbe • E-Mail Adresse	Schüler	Im Rahmen des Supports ist ein Zugriff auf diese Daten nicht ausgeschlossen. Möglicherweise erfolgt dabei bedarfsorientiert eine Speicherung, Anpassung oder Veränderung, ein Auslesen, Abfragen, eine Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung oder der Abgleich dieser Daten.

• Mobiltelefon • Telefonnummer • Faxnummer • Straße • Aktiv • Postleitzahl • Stadt • technische Protokolldaten • Stundenplan		
Bei Verwendung des Klassenbuchs zusätzlich: • Abwesenheiten • Klassenbucheinträge • Noten • Befreiungen • Klassendienste	Schüler	w.o.
• Aktiv • Kurzname • Familienname • Vorname • Titel • Personalnummer • Externe Id • Text • Geburtsdatum • Geschlecht • Eintrittsdatum • Austrittsdatum • Lehrerstatus • Soll/Woche • Lehrperson ist abrechnungsrelevant • Andere Tätigkeiten [%] • Raum • Zugewiesene Abteilungen • Foto • Zugewiesene Lehrbefähigungen • Klassenvorstand der Klassen • Vordergrundfarbe • Hintergrundfarbe • E-Mail Adresse • Mobiltelefon • Telefonnummer • Faxnummer • Straße • Postleitzahl • Stadt • technische Protokolldaten • Stundenplan • Abwesenheiten • Anrechnungen	Lehrer	Im Rahmen des Supports ist ein Zugriff auf diese Daten nicht ausgeschlossen. Möglicherweise erfolgt dabei bedarfsorientiert eine Speicherung, Anpassung oder Veränderung, ein Auslesen, Abfragen, eine Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung oder der Abgleich dieser Daten.

• Benutzername • Fremdbenutzername • Personenrolle • Person • Benutzergruppe • Benutzerzugang aktiv • Benutzerzugang gesperrt • Sprache • E-Mail Adresse • Letzte Anmeldung • Passwort • Google Authenticator Schlüssel • Office 365 Identität	Benutzer (Eltern, Lehrer, Schüler)	Im Rahmen des Supports ist ein Zugriff auf diese Daten nicht ausgeschlossen. Möglicherweise erfolgt dabei bedarfsorientiert eine Speicherung, Anpassung oder Veränderung, ein Auslesen, Abfragen, eine Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung oder der Abgleich dieser Daten.

2. DAUER DER VEREINBARUNG

Die Vereinbarung gilt, solange der Auftragnehmer in einem gültigen Vertragsverhältnis mit der Untis GmbH betreffend Support der Produkte der Untis GmbH steht.

3. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat, oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat und ermöglicht diesbezüglich auch Prüfungen durch den Auftraggeber (weitere Informationen sind der Anlage 1 zu entnehmen).
Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(4) Der Auftragnehmer ergreift technische und organisatorische Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn

irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) 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.

(6) 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.

(7) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(8) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(9) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die personenbezogene Daten enthalten, im Auftrag des Auftraggebers zu vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. 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.

5. PFLICHTEN 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.

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 vor Beginn der Verarbeitung und so- dann regelmäßig in angemessener Weise wie unter Punk 3 Abs. 3 festgelegt 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.

6. WEISUNGSBERECHTIGTE DES AUFTRAGGEBERS, WEISUNGSEMPFÄNGER DES AUFTRAGNEHMERS

Weisungsberechtigte Personen des Auftraggebers sind:
Tragen Sie hier die weisungsberechtigten Personen ein (z.B. Schulleitungsmitglieder)

_____
(Vorname, Name, Organisationseinheit, Telefon)

Weisungsempfänger beim Auftragnehmer sind:

Steffen Eichfuss, Untis Baden-Württemberg GmbH, 07156/178200

_____
(Vorname, Name, Organisationseinheit, Telefon)

Für Weisung zu nutzende Kommunikationskanäle:

bw@untis.at, Tel: 07156/178200, Fax: 07156/17820-22

_____
(genaue postalische Adresse/ E-Mail/ 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

7. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

8. SUB-AUFTRAGSVERARBEITER

Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter hinzuziehen:

Untis GmbH
Belvederegasse 11
AT-2000 Stockerau

Der Auftragnehmer ist befugt, folgende Personen als Sub-Auftragsverarbeiter hinzuziehen:

Herrn Stefan Bader Gluckstr.3 89518 Heidenheim	Herrn Horst Grüning Leinbergstr. 8 36391 Sinntal	Herrn Udo Kohler Sulzer Str. 72 72175 Dornhan	Frau Karen Weinand Karl-Ladenburg-Str.10 68163 Mannheim

Beabsichtigte Änderungen der bzw. des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies gegebenenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen.

Ort , am **Datum**

Für den Auftraggeber:

Unterschrift einer unterschriftsberechtigten Person der Schule

.....

Gerlingen, am 07.01.2019

Für den Auftragnehmer:

.....

Steffen Eichfuss,
Geschäftsführer Untis Baden-Württemberg GmbH

Anlage 1 – Technisch-organisatorische Maßnahmen

1. PSEUDONYMISIERUNG

- Eine Veränderung der Support-Daten ist nicht möglich, da im Rahmen des Supports mit Produktiv-Daten gearbeitet werden muss. Die in den Tickets zur Verfügung gestellten Support-Daten werden systemseitig nach 12 Monaten gelöscht.
- Die kundenbezogenen Personenstammdaten der Ansprechpartner können im Kundenmanagement-System nicht pseudonymisiert werden.

2. VERSCHLÜSSELUNG

- Die Supportdaten aus Untis werden ab Version 2019 nur noch verschlüsselt erzeugt. Ein Entschlüsseln der Daten ist nur mit entsprechendem Schlüssel möglich. Dieser Schlüssel liegt nur den Supportmitarbeiter der Untis Baden-Württemberg GmbH und deren Sub-Auftragsverarbeiter vor.

3. VERTRAULICHKEIT

- **Zutrittskontrolle:**
  Der Support wird in durch Sicherheitsschlösser gesicherten Räumen durchgeführt, zu denen nur beschränkter Zutritt möglich ist. Die dafür ausgegebenen Schlüssel sind nachvollziehbar. Das Reinigungspersonal wurde sorgfältig ausgewählt und vertraglich zur Vertraulichkeit und auf die Einhaltung des Datengeheimnisses verpflichtet.
- **Zugangskontrolle**:
- Der Zugang zu den entsprechenden Systemen unterliegt Sicherheitsrichtlinien und ist ausschließlich durch sichere Kennwörter, etc. möglich. Die Übermittlung der Zugangsdaten zu externen Systemen erfolgt getrennt. Dabei handelt es sich lediglich um das Ticket-System (OTRS) sowie das Kundenmanagement-System der Untis GmbH, auf welche die Untis Baden-Württemberg GmbH Zugriff hat.
- Die Übermittlung der Zugangsdaten zu den Produktivsystemen der Kunden erfolgt ausschließlich auf dem Postweg. Die dort vergebenen Standard-Passwörter müssen nach der Erst-Anmeldung durch den Kunden geändert werden. Alle weiteren Benutzer werden durch die Kunden selbst angelegt. Hierbei können Passwortrichtlinien durch den Kunden hinterlegt werden.
- Zur Sicherung des internen Netzwerkes und den darin genutzten Daten, wird eine stets aktuelle Anti-Viren-Software auf den Client-PCs und dem Server eingesetzt. Ferner wird das Netzwerk durch eine im Router integrierte Firewall-Lösung geschützt. Die Client-PCs nutzen zusätzlich die Firewall des Betriebssystems.
- **Zugriffskontrolle**:
- Jeder Zugriff auf relevante Systeme wird protokolliert und ist somit nachvollziehbar.
- Ein Zugriff auf vom Kunden geführte Systeme (WebUntis) ist nur nach Freigabe durch den Kunden möglich. Werden Support-Daten (Untis) benötigt, so müssen diese von Kunden erzeugt werden und an das Ticketsystem übermittelt werden. Ein direkter Zugriff auf Untis-Kundendaten ist nicht möglich.
- Sollte zu Supportzwecken eine Fernwartungssoftware (wie z.B. Teamviewer) eingesetzt werden, so ist dies nur mit Einverständnis des Kunden möglich. Die für einen Fernwartungszugriff notwendigen Passwörter werden für jede Sitzung systemseitig beim Kunden neu generiert und müssen mitgeteilt werden.
- Der Zugriff auf Kundenstammdaten im Kundenmanagementsystem erfolgt über personalisierte Zugänge im Rahmen eines Berechtigungskonzepts, unter Berücksichtigung

des Grundsatzes „need-to-know“. Es gibt etablierte Prozesse für die Vergabe und den Entzug von Zugriffsberechtigungen, weiters werden diese periodisch überprüft und ggf. angepasst.

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

4. INTEGRITÄT

- **Weitergabekontrolle**:
  Durch den Einsatz entsprechender Verschlüsselungskontrolle bzw. entsprechender Übertragungsprotokolle ist die Veränderung von Daten während des Transports, der Übermittlung bzw. bei der Speicherung und Verarbeitung ausgeschlossen.
- **Eingabekontrolle**:
  Die Veränderung personenbezogener Daten wird durch entsprechende Zugriffsbeschränkungen eingeschränkt, bzw. ist durch systemseitige Protokollierungsmaßnahmen nachvollziehbar.

5. VERFÜGBARKEIT UND BELASTBARKEIT

- **Verfügbarkeitskontrolle**:
  Die Verfügbarkeit und Stabilität der Systeme ist durch technische und organisatorische Maßnahmen sichergestellt:
  - Backup-Strategie (mindestens 4 Komplettsicherungen pro Tag - an allen Wochentagen – der Daten des Kundenmanagement-Systems und wichtiger Daten / Dateien im Netzwerk)
  - Notfallplanung
  - Firewall-Systeme (im Router sowie im Betriebssystem)
  - Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
- **Löschungsfristen**:
  Bei Beendigung der Zusammenarbeit können personenbezogene Kundenstammdaten (fachliche Ansprechpartner) durch einen simplen Befehl sofort gezielt gelöscht werden. Die Kundendaten (Institution / Schulen) bleiben im Rahmen handelsrechtlicher Fristen gespeichert.

6. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

- Ein entsprechendes Datenschutz-Management einschließlich regelmäßiger Mitarbeiter-Schulungen ist etabliert.
- Es werden regelmäßige Audits zur Feststellung des adäquaten Schutzniveaus durchgeführt.
- Sämtliche Voreinstellungen sind datenschutzfreundlich umgesetzt.
- **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, Vorabüberzeugungspflicht, Nachkontrollen eingesetzt.