

Vereinbarung zur Auftragsverarbeitung

Version vom 17. Mai 2018

Gültig mit Durchsetzbarkeit der EU-DSGVO ab 25. Mai 2018

1. Grundlegendes

Die europäische Datenschutzgrundverordnung definiert in Art. 4 (1) EU-DSGVO den Begriff *personenbezogene Daten*. Sobald personenbezogene Daten verarbeitet werden – darunter fällt nach Art. 4 (2) EU-DSGVO auch die Speicherung von Daten – müssen die Rechtsgrundsätze der EU-DSGVO eingehalten werden.

Verschlüsselte Daten fallen nach Art. 4 (5) EU-DSGVO zwar unter den Begriff *pseudonymisierte Daten*, deren Verarbeitung weniger strenge Auflagen hat, dennoch unterliegt auch die Verarbeitung von pseudonymisierten Daten der EU-DSGVO. Im Folgenden wird der Einfachheit halber nur von personenbezogenen Daten gesprochen, auch dann, wenn pseudonymisierte Daten gemeint sind.

Sobald personenbezogene Daten von dem Verantwortlichen zu einem Auftragsverarbeiter übermittelt werden, liegt eine Auftragsverarbeitung vor, welche nach Art. 28 (3) EU-DSGVO nur auf Grundlage einer Vereinbarung erfolgen kann. Die Begriffe *Verantwortlicher* und *Auftragsverarbeiter* werden in Art. 4 (7) und (8) EU-DSGVO definiert. Der Verantwortliche ist in diesem Fall die Schule, welche die Lizenz für die Software erworben hat. Diese wird vertreten durch einen Angestellten, den Anwender der Software. Auftragsverarbeiter ist die Firma *Software für die Schule*.

Ein betrieblicher Datenschutzbeauftragter ist beim Auftragsverarbeiter nicht bestellt, da die gesetzliche Notwendigkeit für eine Bestellung nicht vorliegt.

2. Gegenstand und Dauer der Verarbeitung

Durch *Teamwork* erhält der Anwender die Möglichkeit, Ende-zu-Ende verschlüsselte Daten an einen oder mehrere Empfänger zu senden. Diese Daten können vor dem Versand vom Anwender frei zusammengestellt werden. Die Daten werden temporär auf einem Server zwischengespeichert, bis sie von allen Empfängern abgerufen wurden.

Über die Software *TeamViewer* kann bei Bedarf durch Fernwartung Hilfestellung bei Problemen gegeben werden. Die Verbindung muss grundsätzlich vom Anwender initiiert werden, indem die Software gestartet und uns per Telefon das temporäre Passwort mitgeteilt wird.

Die Dauer der Verarbeitung von *Teamwork* sowie *TeamViewer* erfolgt auf unbestimmte Zeit und endet mit Einstellung der Zahlung des jährlichen Beitrags.

3. Unterauftragsverhältnisse

Teamwork speichert die verschlüsselten Daten temporär auf einem Server der Firma *1&1 Internet SE*. Ein entsprechender Auftragsverarbeitungsvertrag wurde von uns abgeschlossen.

Sollten sich die Unterauftragsverhältnisse ändern, erfolgt das nur mit vorheriger Information und erneuter Zustimmung der geänderten Vereinbarung.

4. Art und Zweck der Verarbeitung

Der Datenaustausch über *Teamwork* soll die Zusammenarbeit zwischen mehreren Anwendern erleichtern. Um die Sicherheit zu gewährleisten, werden alle Daten über eine sichere Verbindung übertragen. Außerdem sind sämtliche mit *Teamwork* versendeten Daten, ob personenbezogen oder nicht, Ende-zu-Ende verschlüsselt.

Um bei Problemen schnelle und präzise Hilfestellung zu ermöglichen, wird auf Wunsch *TeamViewer* eingesetzt. Mit Hilfe von Fernwartung kann einer unserer Supportmitarbeiter den Bildschirminhalt des Anwenders sehen und optional auch dessen Maus sowie Tastatur übernehmen. Dadurch können Missverständnisse umgangen und Probleme schneller gelöst werden.

5. Technische Umsetzung und Datenschutz

Für die Nutzung von *Teamwork* bekommt jeder Anwender durch die Erstellung eines Benutzerkontos ein auf *RSA* basiertes Schlüsselpaar zugewiesen, bestehend aus einem öffentlichen sowie einem privaten Schlüssel. Der öffentliche Schlüssel liegt auf unserem Server, der private Schlüssel beim Anwender. Beim Versand werden die ausgewählten Daten mit einem zufällig generierten Schlüssel unter Verwendung von *AES* verschlüsselt. Für jeden Empfänger wird dieser zufällige Schlüssel mit dessen öffentlichem Schlüssel verschlüsselt. Die verschlüsselten Daten werden zusammen mit den verschlüsselten Schlüsseln an unseren Server übermittelt und können anschließend von den jeweiligen Empfängern abgerufen werden. Zum Entschlüsseln der Daten wird der private Schlüssel des Empfängers genutzt, der niemandem sonst bekannt ist. Ohne diesen privaten Schlüssel können die Daten nicht entschlüsselt werden. Da die Daten nur temporär auf dem Server liegen und jederzeit erneut versendet werden können, wird zu keinem Zeitpunkt ein serverseitiges Backup angelegt.

Um die Fernwartung in Anspruch zu nehmen startet der Anwender *TeamViewer* und teilt dem Supportmitarbeiter per Telefon das temporäre Passwort mit. Anschließend stellt der Supportmitarbeiter eine Verbindung zum Anwender her. Der Anwender hat die Möglichkeit, die Übernahme seiner Maus und Tastatur zu deaktivieren. Nach Abschluss der Arbeit wird die Verbindung getrennt und *TeamViewer* kann vom Anwender geschlossen werden. Abgesehen von den für der Fernwartung benötigten Informationen werden keine zusätzlichen Daten übertragen und es werden zu keinem Zeitpunkt Daten gespeichert.

6. Art der personenbezogenen Daten

Mit *Teamwork* können folgende personenbezogene Daten versendet werden: Kontaktdaten der Schüler, Identifikationsmerkmale der Schüler, Religionszugehörigkeiten, Schülerbilder, Noten, Beurteilungen, Ankreuzzeugnisse, Dokumentationen, Beratungsprotokolle, Kontaktdaten der Erziehungsberechtigten, Kontaktdaten der Notfallkontakte sowie Namen und Kürzel der Klassenlehrer.

Es ist nicht möglich genau anzugeben, welche personenbezogenen Daten mit *TeamViewer* übertragen werden könnten. Unter anderem könnten sich darunter aber die bereits im vorigen Absatz genannten personenbezogenen Daten befinden.

7. Kategorien betroffener Personen

Die mit *Teamwork* versendeten personenbezogenen Daten beziehen sich auf die Schüler, Klassenlehrer, Erziehungsberechtigten und Notfallkontakte der vom Anwender ausgewählten Klassen

bzw. Schüler. Sollten keine Klassen bzw. Schüler ausgewählt worden sein, werden auch keine personenbezogenen Daten übermittelt.

Es ist nicht möglich genau anzugeben, welche Kategorien von Personen durch die Übertragung per *TeamViewer* betroffen sind. Unter anderem könnten sich darunter aber die bereits im vorigen Absatz genannten Kategorien befinden.

8. Recht auf Vergessenwerden

Durch *Teamwork* versendete Daten werden nur solange auf dem Server gespeichert, bis sie von allen Empfängern abgerufen wurden oder die Benutzerkonten besagter Empfänger gelöscht wurden. Benutzerkonten können jederzeit durch den Administrator der Schule gelöscht werden. Durch das Löschen eines Benutzerkontos werden automatisch dessen noch nicht abgerufenen Daten vom Server gelöscht. Sollte Ihre Schule die Zahlung des jährlichen Beitrags einstellen, werden automatisch alle Benutzerkonten der Schule unwiderruflich gelöscht.

Durch die Nutzung von *TeamViewer* werden keinerlei Daten gespeichert.

9. Pflichten des Auftragsverarbeiters

9.1 Der Auftragsverarbeiter verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen dieser Vereinbarung zu verarbeiten. Erhält der Auftragsverarbeiter einen behördlichen Auftrag, Daten des Verantwortlichen herauszugeben, so hat er - sofern gesetzlich zulässig - den Verantwortlichen unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragsverarbeiters eines schriftlichen Auftrages.

9.2 Der Auftragsverarbeiter 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 Auftragsverarbeiter aufrecht.

9.3 Der Auftragsverarbeiter erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art. 32 EU-DSGVO ergriffen hat.

9.4 Der Auftragsverarbeiter ergreift die technischen und organisatorischen Maßnahmen, damit der Verantwortliche die Rechte der betroffenen Person innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Verantwortlichen alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragsverarbeiter gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Verantwortlichen der von ihm betriebenen Datenanwendung hält, hat der Auftragsverarbeiter den Antrag unverzüglich an den Verantwortlichen weiterzuleiten und dies dem Antragsteller mitzuteilen.

9.5 Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Einhaltung der in den Art. 32 bis 36 EU-DSGVO genannten Pflichten.

9.6 Der Auftragsverarbeiter wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art. 30 EU-DSGVO zu errichten hat.

- 9.7 Der Auftragsverarbeiter ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Verantwortlichen zu übergeben oder in dessen Auftrag zu vernichten. Wenn der Auftragsverarbeiter die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Verantwortlichen in dem Format, in dem er die Daten vom Verantwortlichen erhalten hat oder in einem anderen, gängigen Format herauszugeben.
- 9.8 Der Auftragsverarbeiter hat den Verantwortlichen unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Verantwortlichen verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.
- 9.9 Im Falle einer Inanspruchnahme des Verantwortlichen durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 EU-DSGVO, verpflichtet sich der Auftragsverarbeiter den Verantwortlichen bei der Abwehr des Anspruchs im Rahmen seiner Möglichkeiten zu unterstützen.

10. Pflichten des Verantwortlichen

- 10.1 Der Verantwortliche wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art. 30 EU-DSGVO zu errichten hat.
- 10.2 Der Verantwortliche hat den Auftragsverarbeiter unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.
- 10.3 Im Falle einer Inanspruchnahme des Verantwortlichen durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 EU-DSGVO, gilt Abs. 9.9 dieser Vereinbarung entsprechend.

11. Anfragen betroffener Personen

Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragsverarbeiter, wird der Auftragsverarbeiter die betroffene Person an den Verantwortlichen verweisen, sofern eine Zuordnung an den Verantwortlichen nach Angaben der betroffenen Person möglich ist. Der Auftragsverarbeiter leitet den Antrag der betroffenen Person unverzüglich an den Verantwortlichen weiter. Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragsverarbeiter haftet nicht, wenn das Ersuchen der betroffenen Person vom Verantwortlichen nicht, nicht richtig oder nicht fristgerecht beantwortet wird.