

Fürst-Johann-Ludwig-Schule Hadamar

Digitale Dienste für Schülerinnen und Schüler sowie Lehrkräfte
Nutzungsbedingungen
Hinweise zum Datenschutz und Datenschutzerklärung

Stand: V4.2 08/2022

Inhaltsverzeichnis

1	Einleitung und Zweck der Datenverarbeitung	2
2	Nutzungsvereinbarung	2
2.1	Geltungsbereich	2
2.2	Laufzeit	2
2.3	Umfang	3
2.4	Datenschutz und Datensicherheit	3
2.5	Verantwortungsvolles und sicheres Handeln	4
2.5.1	Passwörter	4
2.5.2	Zugangsdaten	4
2.5.3	Personenbezogene Daten	4
2.6	Urheberrecht	5
2.7	Unzulässige Inhalte und Handlungen	6
2.8	Zu widerhandlungen	6
2.9	Zusätzliche Nutzungsbedingungen von Microsoft für MS365	6
3	Datenschutzrechtliche Informationen nach Art. 13 DS-GVO	8
3.1	Datenverarbeitende Stelle	8
3.2	Zwecke der Verarbeitung personenbezogener Daten	8
3.3	Rechtsgrundlage der Verarbeitung personenbezogener Daten	8
3.4	Kategorien betroffener Personen	8
3.5	Kategorien von personenbezogenen Daten	8
3.5.1	Pädagogisches Netz	8
3.5.2	MS365 und Moodle	9
3.6	Kategorien von Empfängern	9
3.6.1	Pädagogisches Netz	9
3.6.2	MS365 und Moodle	9
3.6.3	Löschfristen	9
3.7	Recht auf Widerruf	10
3.8	Weitere Betroffenenrechte	10
3.9	Wichtiger Hinweis - Freiwilligkeit	10
4	Zusätzliche Informationen	11
4.1	Datenschutz bei Verarbeitung von personenbezogenen Daten in den USA	11
4.2	Thema CLOUD-Act	11
4.3	Wo werden meine personenbezogenen Daten verarbeitet?	11
4.4	Wie sicher ist MS365?	11
4.5	Wo kann ich mehr zum Datenschutz von MS365 erfahren?	12
4.6	Was tut die Schule zum Schutz meiner personenbezogenen Daten in @fjls.Cloud-Diensten?	12
4.7	Kann eine Einwilligung nach dem Urteil des EUGH zum EU-US Privacy Shield noch genutzt werden?	12
4.8	Was kann ich als Nutzer zusätzlich tun, um den Schutz meiner personenbezogenen Daten zu erhöhen?	13

1 Einleitung und Zweck der Datenverarbeitung

Für alle Arbeiten im Unterricht und in Phasen des eigenverantwortlichen Lernens erhältst Du / erhalten Sie Zugang zum pädagogischen Netz unserer Schule, bestehend aus

- drei PC-Räumen mit Internetzugang
- mehreren Arbeitsplätzen in der Bibliothek
- W-LAN Zugang, ggf. mit zeitlicher Nutzungsbeschränkung (Detaillierte Bedingungen gehen durch den Schulträger gesondert zu.)
- Leihgeräten zur individuellen Nutzung (Nach Verfügbarkeit; detaillierte Bedingungen werden bei Ausleihe ausgehändigt.)

und zu unserer Arbeitsplattform „@fjls.Cloud“, im weiteren Verlauf „Dienste“ genannt, bestehend aus

- dem Schulportal des Landes Hessen (SPH)
- Moodle als Lernplattform
- Microsoft 365 Education als Kommunikationsplattform, darüber
 - die gängigen Office-Programme, auch für die Arbeit zu Hause (Vollversionen, 5 Lizenzen)
 - ein E-Mail-Postfach
 - Teams für Besprechungen, Nachrichten und Kurzmitteilungen
 - OneDrive/SharePoint (1024 GB pro Person) als Datenspeicher
- Untis/WebUntis als Verwaltungsprogramm für Stunden- und Vertretungspläne
- iServ als Zugangspunkt für Geräte in der Schule und W-LAN

Den Zugang zu den o. g. Werkzeugen stellen wir Dir/Ihnen, soweit zugänglich, auch außerhalb des Unterrichts **zur schulischen Nutzung** Verfügung. Die Nutzung setzt einen verantwortungsvollen Umgang mit den Netzwerkressourcen, den Arbeitsplattformen sowie den eigenen personenbezogenen Daten und denen von anderen in der Schule lernenden und arbeitenden Personen voraus. Die folgende Nutzungsvereinbarung informiert und steckt den Rahmen ab für eine verantwortungsvolle Nutzung und ihre Annahme bzw. die Einwilligung sind Voraussetzung für die Erteilung bzw. Beibehaltung eines Nutzerzugangs.

2 Nutzungsvereinbarung

2.1 Geltungsbereich

Die Nutzungsvereinbarung gilt für Schülerinnen und Schüler sowie für Lehrkräfte, nachfolgend „Benutzer“ genannt, welche das von der Schule bereitgestellte pädagogische Netzwerk und Dienste zur elektronischen Datenverarbeitung nutzen.

2.2 Laufzeit

Dem Benutzer werden innerhalb seiner Dienstzeit/Schulzeit folgende Benutzerkonten zur Verfügung gestellt:

Konto	Auftragsdatenverarbeitung bei
Nutzerkonto beim SPH Hessen	Rechenzentrum des Landes Hessen (im Moment nur für Lehrkräfte)
Nutzerkonto bei Moodle (Open Source)	Rechenzentrum Mittwald Medien
Nutzerkonto bei Microsoft 365 Education	Microsoft Deutschland GmbH

+Nutzungslizenzen für Schülerinnen und Schüler bzw. Lehrkräfte über den Digitalpakt 4.0 des Landes Hessen	Deutsches Rechenzentrum Europäisches Rechenzentrum
Nutzerkonto Untis WebUntis	Server bei der Strato AG in Deutschland Support durch Untis GmbH, Stockerau, Österreich Untis GmbH, Stockerau, Österreich
Nutzerkonto iServ	Server in der Schule Support und Bereitstellung Landkreis Limburg-Weilburg

Beim Verlassen der Schule werden sämtliche Benutzerkonten deaktiviert und alle Inhalte gelöscht sowie die Zuweisung der MS365 Education-Lizenz aufgehoben.

2.3 Umfang

Zum Umfang des von der Schule für die Benutzer kostenlos bereitgestellten Paketes gehören:

- Zugang zum pädagogischen Netzwerk mit „iServ“ mit einem persönlichen Nutzerkonto und Speicherplatz
- Zugang zu MS365 mit
 - einer schulischen E-Mail-Adresse
 - **1024 GB** Online-Speicherplatz auf Microsoft OneDrive
 - Microsoft Office Online (Word, Excel, PowerPoint, Outlook, OneNote, [...])
- Die Möglichkeit, die Vollversionen des Microsoft Office Paketes auf bis zu 5 Privatgeräten für schulische Zwecke zu verwenden
- Der Zugang zu personen- und kursbezogenen Inhalten auf der Lernplattform Moodle
- Der Zugang zu Stunden- und Vertretungsplänen mit Untis

2.4 Datenschutz und Datensicherheit

Der Schulträger und Schule sorgen durch technische und organisatorische Maßnahmen für den Schutz und die Sicherheit der im pädagogischen Netz verarbeiteten personenbezogenen Daten.

Mit den auftragsverarbeitenden Unternehmen Untis, Strato, Mittwald und Microsoft wurden zur Nutzung der entsprechenden Dienste Verträge abgeschlossen, welche gewährleisten, dass personenbezogene Daten von Benutzern nur entsprechend den Vertragsbestimmungen verarbeitet werden. So verpflichtet sich Microsoft, die personenbezogenen Daten von Benutzern in MS365 nicht zur Erstellung von Profilen zur Anzeige von Werbung oder Direkt-Marketing zu nutzen.

Ziel unserer Schule ist es, durch Minimierung personenbezogener Daten bei der Nutzung der o.g. Dienste auf das maximal erforderliche Maß, die Anwendung empfohlener technisch-organisatorischer Schutzmaßnahmen, und die Separation von Daten das Recht auf informationelle Selbstbestimmung unserer Schüler und Lehrkräfte bestmöglich zu schützen.

Dieses ist nur möglich, wenn die Benutzer selbst durch verantwortungsvolles Handeln zum Schutz und zur Sicherheit ihrer personenbezogenen Daten beitragen und auch das Recht anderer Personen an der Schule auf informationelle Selbstbestimmung respektieren.

An erster Stelle gilt dieses für die Nutzung von personenbezogenen Daten im Rahmen der Internet-Dienste des SPH, WebUntis, Moodle und insbesondere MS365. Es gilt jedoch auch für das pädagogische Netzwerk der Schule.

Personenbezogene Daten gehören grundsätzlich **nicht** in die Cloud, weder die eigenen noch die von anderen! Jeder Benutzer hat dafür zu sorgen, dass Sicherheit und Schutz von personenbezogenen Daten nicht durch leichtsinniges, fahrlässiges oder vorsätzliches Handeln gefährdet werden.

2.5 Verantwortungsvolles und sicheres Handeln

bedeutet:

2.5.1 Passwörter

- müssen sicher sein und dürfen nicht erratbar sein. Sie müssen aus **mindestens 6 Zeichen** bestehen und mindestens drei verschiedene Zeichentypen enthalten.
- sollen nicht für Anmeldungen bei anderen Diensten verwendet werden.

2.5.2 Zugangsdaten

- Der Benutzer ist verpflichtet, die eigenen Zugangsdaten zum pädagogischen Netz und zu den @FJLS.cloud Konten geheim zu halten. **Sie dürfen nicht an andere Personen weitergegeben werden.**
- Sollten die eigenen Zugangsdaten durch ein Versehen anderen Personen bekannt geworden sein, ist der Benutzer verpflichtet, sofort Maßnahmen zum Schutz der eigenen Zugänge zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist unverzüglich ein schulischer Administrator zu informieren.
- Sollte der Benutzer in Kenntnis fremder Zugangsdaten gelangen, so ist es untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Der Benutzer ist jedoch verpflichtet, den Eigentümer der Zugangsdaten oder einen schulischen Administrator zu informieren.
- Nach Ende der Unterrichtsstunde oder der Arbeitssitzung an einem schulischen Rechner bzw. Mobilgerät meldet sich der Benutzer von allen Diensten und vom pädagogischen Netz ab (ausloggen).

2.5.3 Personenbezogene Daten

Für die Nutzung von personenbezogenen Daten wie dem eigenen Namen, biografischen Daten, der eigenen Anschrift, Fotos, Video und Audio, auf welchen der Benutzer selbst abgebildet ist und ähnlich gelten die Prinzipien der Datenminimierung und Datensparsamkeit.

2.5.3.1 Pädagogisches Netz

- Innerhalb des pädagogischen Netzes sollen keine personenbezogenen Daten gespeichert werden.

2.5.3.2 MS365, Moodle, SPH, WebUntis

- Personenbezogene Daten des Benutzers haben in Online-Diensten nichts verloren. Soll mit personenbezogenen Daten gearbeitet werden (z. B. Lebenslauf), sollten diese anonymisiert und/oder zusätzlich verschlüsselt werden.
- Eine unverschlüsselte Speicherung von personenbezogenen Daten in Microsoft OneDrive ist nicht zulässig.
- Die Nutzung aller Dienste für private Zwecke nicht zulässig.
- Bei der Nutzung von MS365 auf privaten Geräten ist darauf zu achten, dass keine Synchronisation privater Daten mit dem o. g. Dienst OneDrive erfolgt.

2.5.3.3 E-Mail

Bestandteil des MS365 Paketes ist auch eine schulische E-Mail-Adresse, die gleichzeitig Teil der Zugangsdaten ist.

- Die Nutzung des schulischen E-Mail-Kontos ist **nur für schulische Zwecke** zulässig. Eine Nutzung für private Zwecke ist nicht erlaubt.
- Wie bei den anderen Komponenten von MS365, ist auch beim Versand von E-Mails die Nutzung von personenbezogenen Daten zu minimieren.
- Eine automatische Weiterleitung schulischer E-Mails auf eine private E-Mail-Adresse ist nicht gestattet.

2.5.3.4 Audio-/Videokonferenzen, digital-gestützter Distanzunterricht nach § 127c Hessisches Schulgesetz

- Konferenzplattformen und -software dürfen ausschließlich zu schulischen Zwecken genutzt werden.
- Die Zugangsdaten oder Links dürfen nicht an Dritte weitergegeben werden. Sollten Dritte Kenntnis von den Daten erhalten haben, ist die Schule umgehend hierüber zu informieren.
- Das Aufzeichnen von Audio- und Videokonferenzen sowie von Zuschaltungen von zu Hause in den Unterricht sind nicht erlaubt. Sofern ein Chat vorhanden ist, darf auch dieser nicht extern gespeichert werden. Ebenso sind das Anfertigen und Speichern von Screenshots, Fotos oder Videos oder die Übertragung an Dritte untersagt.
- Die Teilnahme an Audio- und Videokonferenzen sowie digital-gestütztem Distanzunterricht ist ausschließlich Schülerinnen und Schülern sowie Lehrkräften gestattet.
- Der Austausch von Materialien wie Texte, Bilder, Musik, Töne oder Videos zwischen den Nutzern ist ausschließlich für schulische Zwecke erlaubt.
- Die Zuschaltung zu und Übertragung von digital-gestütztem Distanzunterricht bedarf einer besonderen Einwilligung, die von der Schule abgefragt wird und jederzeit gesondert widerrufen werden kann. **Nutzern, die die Einwilligung nicht erteilen, dürfen keine Nachteile entstehen.**
- Foto-, Bild- und Tonaufnahmen stellen personenbezogene Daten im Sinne von Art. 4 Nr. 1 DS-GVO dar. Die Aufnahmen dürfen nur mit freiwilliger und informierter Einwilligung der Betroffenen im Sinne des Art. 6 Abs. 1 Buchst. a DS-GVO gemacht und veröffentlicht werden. **Das heißt: Die Nutzung der Kamerafunktion ist stets freiwillig und bleibt den einzelnen Beteiligten überlassen.**

2.5.3.5 Kalender

Die Aufnahme von privaten, nicht schulischen Terminen in den Kalender von MS365 ist nicht zulässig. Dazu gehören auch die Geburtstage von anderen Benutzern aus der Schule.

2.5.3.6 Kopplung mit privaten Konten oder anderen Diensten

- Zur Wahrung des Schutzes und der Sicherheit der eigenen personenbezogenen Daten ist es nicht zulässig, das schulische MS365 Konto mit anderen privaten Konten von Microsoft oder anderen Anbietern zu verbinden.
- Eine Nutzung des schulischen MS365 Kontos zur Authentifizierung an anderen Online-Diensten ist nicht zulässig, außer es handelt sich um von der Schule zugelassene Dienste. Diese Zulassung wird durch die IT-Administration der Schule zentral erteilt und besteht aktuell für folgende Dienste:
 - **statista.de** – Statistikportal, Zugang kostenlos zur für Schulen des Landkreises durch den Landkreis Limburg-Weilburg. Neben der Möglichkeit personalisierte Zugänge zu verwenden, kann das Angebot auch durch einen anonymen Link wahrgenommen werden.
 - **GeoGebra** – Mathematiksoftware - Neben der Möglichkeit personalisierte Zugänge zu verwenden, kann das Angebot auch durch einen anonymen Link wahrgenommen werden.
 - **Goodnotes** – Notizprogramm für Apple iPads (als Alternative zu Microsoft OneNote). Hier ist lediglich eine Verbindung zu OneDrive als Cloudspeicher erlaubt. Daten oder Benutzerkonten können im Augenblick nicht übertragen werden. Die Vollversion muss privat erworben werden.
 - **WebUntis** – Abruf der persönlichen Stunden- und Vertretungspläne. Hier wird nur Kontozuordnung abgefragt und keine Daten an die Authentifizierungsstelle übertragen.

2.6 Urheberrecht

- Bei der Nutzung des pädagogischen Netzes der Schule und der @fjls.Cloud-Dienste sind die geltenden Bestimmungen des Urheberrechtes zu beachten. Fremde Inhalte, deren Nutzung nicht durch freie Lizenzen wie Creative Commons, GNU oder Public Domain zulässig ist, haben ohne schriftliche Genehmigung der Urheber nichts im pädagogischen Netz oder in MS365 zu suchen, außer ihre Nutzung erfolgt im Rahmen des Zitatrechts.
- Fremde Inhalte (Texte, Fotos, Videos, Audio und andere Materialien) dürfen nur mit der schriftlichen Genehmigung des Urhebers veröffentlicht werden. Dieses gilt auch für digitalisierte Inhalte. Dazu gehören eingescannte oder abfotografierte Texte und Bilder. Bei vorliegender Genehmigung ist bei Veröffentlichungen auf einer eigenen Website ist, der Urheber zu nennen, wenn dieser es wünscht.

- Bei der unterrichtlichen Nutzung von freien Bildungsmaterialien (Open Educational Resources - **OER**) sind die jeweiligen Lizenzen zu beachten und entstehende neue Materialien, Lernprodukte bei einer Veröffentlichung entsprechend der ursprünglichen Creative Commons Lizenzen zu lizenzieren.
- Digitalisierte Kopiervorlagen oder Inhalte aus Schulbüchern und Arbeitsheften, die von Lehrkräften im Rahmen des "Gesamtvertrag „Vervielfältigungen an Schulen“"¹ im pädagogischen Netz oder in @fjls.Cloud-Diensten in digitalem Format eingestellt wurden, dürfen vom Benutzer nicht an andere Personen außerhalb der Klassen- oder Kursgruppe weitergegeben werden.
- Bei von der Schule über das pädagogische Netz oder @fjls.Cloud-Dienste zur Verfügung gestellten digitalen Inhalten von Lehrmittelverlagen ist das Urheberrecht zu beachten. Eine Nutzung ist nur innerhalb der schulischen Plattformen zulässig. Nur wenn die Nutzungsbedingungen der Lehrmittelverlage es gestatten, ist eine Veröffentlichung oder Weitergabe digitaler Inhalte von Lehrmittelverlagen zulässig.
- Stoßen Benutzer im pädagogischen Netz oder in MS365 auf urheberrechtlich geschützte Materialien, sind sie verpflichtet, dieses bei einer verantwortlichen Person anzuzeigen.
- Die Urheberrechte an Inhalten, welche Benutzer eigenständig erstellt haben, bleiben durch eine Ablage oder Bereitstellung im pädagogischen Netz oder anderen Diensten unberührt.

2.7 Unzulässige Inhalte und Handlungen

Benutzer sind verpflichtet, bei der Nutzung des pädagogischen Netzes und aller Dienste geltendes Recht einzuhalten.

- Es ist verboten, pornografische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über das pädagogische Netz und MS365 abzurufen, zu speichern oder zu verbreiten.
- Die geltenden Jugendschutzvorschriften sind zu beachten.
- Die Verbreitung und das Versenden von belästigenden, verleumderischen oder bedrohenden Inhalten sind unzulässig.
- Die E-Mail-Funktion von MS365 darf nicht für die Versendung von Massen-Nachrichten (Spam) und/oder anderen Formen unzulässiger Werbung genutzt werden.
- Die Kommunikationsfunktionen des Systems darf nur zu unterrichtlichen Zwecken genutzt werden.

2.8 Zuwiderhandlungen

Im Falle von Verstößen gegen diese Nutzungsordnung behält sich die Schulleitung der Fürst-Johann-Ludwig-Schule das Recht vor, den Zugang zu einzelnen oder allen Diensten zu sperren. Davon unberührt behält sich die Schulleitung weitere dienstrechtliche Maßnahmen (Lehrkräfte) oder Ordnungsmaßnahmen (Schüler) vor.

2.9 Zusätzliche Nutzungsbedingungen von Microsoft für MS365

Es gelten außerdem die Nutzungsbedingungen des Microsoft-Servicevertrags: <https://www.microsoft.com/de-de/servicesagreement/>. Dabei soll primär hingewiesen werden auf den

Verhaltenskodex

Inhalte, Materialien oder Handlungen, die diese Bestimmungen verletzen, sind unzulässig. Mit Ihrer Zustimmung zu diesen Bestimmungen gehen Sie die Verpflichtung ein, sich an diese Regeln zu halten:

1. Nehmen Sie keine unrechtmäßigen Handlungen vor.
2. Unterlassen Sie Handlungen, durch die Kinder ausgenutzt werden, ihnen Schaden zugefügt oder angedroht wird.
3. Versenden Sie kein Spam. Bei Spam handelt es sich um unerwünschte oder unverlangte Massen-E-Mails, Beiträge, Kontaktanfragen, SMS (Textnachrichten) oder Sofortnachrichten.
4. Unterlassen Sie es, unangemessene Inhalte oder anderes Material (das z. B. Nacktdarstellungen, Brutalität, Pornografie, anstößige Sprache, Gewaltdarstellungen oder kriminelle Handlungen zum Inhalt hat) zu veröffentlichen oder über die Dienste zu teilen.

¹ "Schulbuchkopie." <http://www.schulbuchkopie.de/>. Abgerufen 11 Nov. 2020.

5. Unterlassen Sie Handlungen, die betrügerisch, falsch oder irreführend sind (z. B. unter Vorspiegelung falscher Tatsachen Geld fordern, sich als jemand anderes ausgeben, die Dienste manipulieren, um den Spielstand zu erhöhen oder Rankings, Bewertungen oder Kommentare zu beeinflussen).
6. Unterlassen Sie es, wissentlich Beschränkungen des Zugriffs auf bzw. der Verfügbarkeit der Dienste zu umgehen.
7. Unterlassen Sie Handlungen, die Ihnen, dem Dienst oder anderen Schaden zufügen (z. B. das Übertragen von Viren, das Belästigen anderer, das Posten terroristischer Inhalte, Hassreden oder Aufrufe zur Gewalt gegen andere).
8. Verletzen Sie keine Rechte anderer (z. B. durch die nicht autorisierte Freigabe von urheberrechtlich geschützter Musik oder von anderem urheberrechtlich geschütztem Material, den Weiterverkauf oder sonstigen Vertrieb von Bing-Karten oder Fotos).
9. Unterlassen Sie Handlungen, die die Privatsphäre von anderen verletzen.
10. Helfen Sie niemandem bei einem Verstoß gegen diese Regeln

3 Datenschutzrechtliche Informationen nach Art. 13 DS-GVO

Zur Nutzung unseres pädagogischen Netzes und von der @fjls.Cloud-Dienste an der Fürst-Johann-Ludwig-Schule ist die Verarbeitung von personenbezogenen Daten erforderlich. Darüber möchten wir Sie/Euch im Folgenden informieren.

3.1 Datenverarbeitende Stelle

Kontakt Daten Schule Fürst-Johann-Ludwig-Schule Freiherr-vom-Stein-Straße, 65589 Hadamar Telefon-Nr. 06433 2076 Vertretungsberechtigter: Direktor Peter Laux schulleitung@fjls.de	Schulischer Datenschutzbeauftragter Alexander Groh Freiherr-vom-Stein-Straße 65589 Hadamar Groh@fjls.cloud
---	---

3.2 Zwecke der Verarbeitung personenbezogener Daten

Personenbezogene Daten der Benutzer des pädagogischen Netzes und der @fjls.Cloud-Dienste werden erhoben, um dem Benutzer die genannten Dienste zur Nutzung im Unterricht und zur Vor- und Nachbereitung von Unterricht zur Verfügung zu stellen, die Sicherheit dieser Dienste und der verarbeiteten Daten aller Benutzer zu gewährleisten und im Falle von missbräuchlicher Nutzung oder der Begehung von Straftaten die Verursacher zu ermitteln und entsprechende rechtliche Schritte einzuleiten.

3.3 Rechtsgrundlage der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten bei Nutzung des pädagogischen Netzes, des Schulportals Hessen (SPH), von Moodle und MS365 erfolgt auf der Grundlage von DS-GVO Art. 6 lit. a (Einwilligung). Die Nutzung des pädagogischen Netzwerks erfolgt im Rahmen des Pflichtunterrichts auf der Grundlage von DS-GVO Art. 6 lit. c (rechtliche Verpflichtung).

3.4 Kategorien betroffener Personen

Schülerinnen und Schüler, Lehrkräfte

3.5 Kategorien von personenbezogenen Daten

3.5.1 Pädagogisches Netz

- **Anmeldeinformationen** (Nutzerkennung, Passwort, Passworthinweis)
- **Nutzerinhalte** (erzeugte Dateien und Inhalte, Versionen von Dateien)
- **technische Daten** (Datum, Zeit, Gerät, Traffic, IP-Nummern aufgesuchter Internetseiten und genutzter Dienste)
- **Geräte-Identifikationsdaten privater Geräte** (Gerätename, MAC-Adresse)

3.5.2 MS365 und Moodle

- **Anmeldeinformationen**, Rechte und Rollen, Zuteilung zu Gruppen, **Geräte- und Nutzungsdaten, Nutzungsdaten von Inhalten, Interaktionen, Suchvorgänge und Befehle, Text-, Positionsdaten, Inhalte², Lizenzinformationen** (Anzahl Installationen, bei Nutzung von MS365 Pro Plus)

3.6 Kategorien von Empfängern

3.6.1 Pädagogisches Netz / iServ

Intern:

- **Lehrkräfte, Mitarbeiter/-innen, Schüler/-innen** (nur gemeinsame Daten oder von Nutzern in ein gemeinsames Verzeichnis übermittelte Daten oder Freigaben),
- **Schulträger** (alle technischen und öffentlichen Daten, soweit für administrative Zwecke erforderlich)
- **Administratoren** (alle technischen und öffentlichen Daten, soweit für administrative Zwecke erforderlich),
- **Schulleitung** (alle technischen und öffentlichen Daten; Daten im persönlichen Nutzerverzeichnis **nur** im begründeten Verdachtsfall einer Straftat oder bei offensichtlichem Verstoß gegen die Nutzungsvereinbarung **und** nach vorheriger Information der Benutzer **und** im Beisein von Zeugen – *Vier-Augen-Prinzip*)

Extern:

- **iServ GmbH, Administratoren** (alle Daten, soweit für administrative Zwecke erforderlich, auf Weisung des Schulträgers)
- **Ermittlungsbehörden** (alle Daten betroffener Nutzer, Daten im persönlichen Nutzerverzeichnis nur im Verdachtsfall einer Straftat)
- **Betroffene** (Auskunftsrecht nach Art. 15 DS-GVO)

3.6.2 MS365 und Moodle (Online-Dienste)

Intern:

- **Schulische Administratoren** (alle technischen Daten, soweit für administrative Zwecke erforderlich)
- **Schulleitung** (Zugangsdaten, alle technischen und öffentlichen Daten und Kommunikationsdaten **nur** im begründeten Verdachtsfall einer Straftat oder bei offensichtlichem Verstoß gegen die Nutzungsvereinbarung **und** nach vorheriger Information der Benutzer **und** im Beisein von Zeugen – *Vier-Augen-Prinzip*)

Extern:

- **Microsoft** (zur Bereitstellung der Dienste von MS365, auf Weisung der Schulleitung, gemäß der gültigen Onlinedienstvereinbarungen³ frühestens vom 13.08.2019)
- **Ermittlungsbehörden** (alle Daten betroffener Benutzer, Daten im persönlichen Nutzerverzeichnis nur im Verdachtsfall einer Straftat)
- **US-Ermittlungsbehörden** haben Zugriff nach US-amerikanischem Recht (weitere Informationen, siehe unten).
- **Betroffene** (Auskunftsrecht nach Art. 15 DS-GVO)

3.6.3 Untis/WebUntis

Intern:

- **Schulische Administratoren** (alle technischen Daten, soweit für administrative Zwecke erforderlich)
- **Schulleitung** (Zugangsdaten, alle technischen und öffentlichen Daten und Kommunikationsdaten **nur** im begründeten Verdachtsfall einer Straftat oder bei offensichtlichem Verstoß gegen die Nutzungsvereinbarung **und** nach vorheriger Information der Benutzer **und** im Beisein von Zeugen – *Vier-Augen-Prinzip*)

Extern:

- **Untis GmbH** (zur Bereitstellung der Dienste von Untis/WebUntis, auf Weisung der Schulleitung, gemäß des Verarbeitungsvertrages)

² Details siehe <https://privacy.microsoft.com/de-de/privacystatement#mainenterprise-developer-products-module> (soweit auf Office 365 Education zutreffend)

³ OST in der gültigen Fassung unter [Licensing Documents \(microsoft.com\)](https://www.microsoft.com/licensing/documents)

- **Strato AG** (zur Bereitstellung der Server-Dienste von Untis/WebUntis, auf Weisung der Schulleitung, gemäß des Verarbeitungsvertrages)
- **Ermittlungsbehörden** (alle Daten betroffener Benutzer, Daten im persönlichen Nutzerverzeichnis nur im Verdachtsfall einer Straftat)
- **Betroffene** (Auskunftsrecht nach Art. 15 DS-GVO)

3.6.4 Löschfristen

Pädagogisches Netz / iServ

Zugangs- und Nutzungsdaten bleiben bestehen, solange der Benutzer Mitglied im pädagogischen Netz ist. Logdaten von Anmeldungen am pädagogischen Netz und Endgeräten sowie von Internetzugriffen aus dem pädagogischen Netz werden automatisch nach 30 Tagen gelöscht. Nach Ende der Schulzugehörigkeit werden sämtliche Zugangsdaten sowie das Nutzerverzeichnis gelöscht. Bis dahin ist es für den Benutzer möglich, sich die Inhalte des persönlichen Verzeichnisses aushändigen zu lassen.

MS365, Moodle und Untis/WebUntis

Mit dem Ende der Schulzugehörigkeit erlischt das Anrecht auf die Nutzung der Dienste. Entsprechend wird die Zuweisung von MS365 Education-Lizenzen zu Benutzern mit Ende der Schulzugehörigkeit, in der Regel zum Schuljahresende, aufgehoben. Damit verliert der Benutzer den Zugriff auf Online-Dienste und -Daten. Das bedeutet Folgendes:

- Alle Daten im Zusammenhang mit dem Konto dieses Benutzers werden von Microsoft 30 Tage aufbewahrt. Eine Ausnahme bilden Daten mit gesetzlicher Aufbewahrungspflicht, die entsprechend dieser Frist aufbewahrt werden.
- Nach Ablauf der 30-tägigen Frist werden die Daten von Microsoft gelöscht und können nicht wiederhergestellt werden. Ausgenommen sind Dokumente, die auf SharePoint Online-Websites gespeichert sind.⁴ Benutzer müssen ihre Daten vorher eigenständig sichern.

3.7 Recht auf Widerruf

Die erteilte Einwilligung kann für die Zukunft jederzeit widerrufen werden. Dabei kann der Widerruf auch nur auf einen Teil der Datenarten bezogen sein. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Im Falle des Widerrufs sämtlicher Verarbeitung personenbezogener Daten im pädagogischen Netz und in @fjls.Cloud-Diensten werden die entsprechenden Zugangsdaten aus dem System gelöscht und der Zugang gesperrt.

3.8 Weitere Betroffenenrechte

Gegenüber der Schule besteht ein Recht auf **Auskunft** über Ihre personenbezogenen Daten, ferner haben Sie ein Recht auf **Berichtigung**, **Löschung** oder **Einschränkung**, ein **Widerspruchsrecht** gegen die Verarbeitung und ein Recht auf **Datenübertragbarkeit**. Diese Rechte basieren auf dem Artikel 15-18 und 20-21 der DS-GVO.

Zudem steht Ihnen ein **Beschwerderecht** bei der Datenschutzaufsichtsbehörde, der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Hessen, Gustav-Stresemann-Ring 1, 65189 Wiesbaden zu.

www.datenschutz.hessen.de/service/beschwerde

3.9 Wichtiger Hinweis – Freiwilligkeit

Wir möchten darauf hinweisen, dass im Gegensatz zu der Nutzung von Untis, sowohl die Nutzung des pädagogischen Netzes als auch von @fjls.Cloud-Diensten inklusive WebUntis auf freiwilliger Basis nach Art. 6, Abs.1, lit. a erfolgen:

⁴ Siehe [Verwalten der Lizenzen und Inhalte von Absolventen in Office 365 Education](#) (11/2018)

Eine Anerkennung der Nutzervereinbarungen und eine Einwilligung in die Verarbeitung der zur Nutzung des pädagogischen Netzes wie auch von allen Diensten erforderlichen personenbezogenen Daten ist freiwillig.

- Die Nutzung des pädagogischen Netzes setzt keine Nutzung von MS365 oder anderen Diensten voraus. Wer die Nutzungsvereinbarung für einen Teil der Dienste nicht anerkennen möchte, erfährt daraus keinen Nachteil und kann in der Schule mit einer Offlineversion von Microsoft Office arbeiten.
- Die Nutzung der Online-Dienste setzt keine Nutzung des pädagogischen Netzes voraus. Alternativ ist es auch möglich, mit Einwilligung der Eltern über einen eigenen mobilen Zugang mit dem eigenen Gerät auf Online-Dienste zuzugreifen. Für eine brauchbare und zuverlässige Leistung einer Mobilfunkverbindung in allen Gebäudeteilen übernimmt die Schule keine Verantwortung.
- Wer die Nutzungsvereinbarung des pädagogischen Netzes nicht anerkennt, kann keine schulischen Computer außerhalb des verpflichtenden Fachunterrichts und keine Mobilgeräte nutzen.
- Die Nutzung des pädagogischen Netzes setzt immer die Anerkennung der Nutzervereinbarung für das pädagogische Netz **und** die Einwilligung in die diesbezügliche Verarbeitung von personenbezogenen Daten des Betroffenen voraus.
- Die Nutzung von der Online-Dienste setzt immer die Anerkennung der Nutzervereinbarung für MS365 **und** die Einwilligung in die diesbezügliche Verarbeitung von personenbezogenen Daten des Betroffenen voraus.

4 Zusätzliche Informationen

4.1 Datenschutz bei Verarbeitung von personenbezogenen Daten in den USA

Bei der Nutzung von MS365 können auch Daten auf Servern in den USA verarbeitet werden. Dabei geht es weniger um Inhalte von Chats, Videokonferenzen, Terminen und gestellten Aufgaben, Nutzerkonten und Teamzugehörigkeiten, sondern um Daten, welche dazu dienen, die Sicherheit und Funktion der Plattform zu gewährleisten und zu verbessern. Nach der aktuellen Rechtslage in den USA haben US-Ermittlungsbehörden nahezu ungehinderten Zugriff auf alle Daten auf Servern in den USA. Nutzer erfahren davon nichts und haben auch keine rechtlichen Möglichkeiten, sich dagegen zu wehren. Die Risiken, welche durch diese Zugriffsmöglichkeiten von US-Ermittlungsbehörden entstehen, dürften eher gering sein.

4.2 Thema CLOUD-Act

Im Rahmen des CLOUD-Acts haben US-Ermittlungsbehörden auch Möglichkeiten, bei Microsoft die Herausgabe von personenbezogenen Daten, die auf Servern in der EU gespeichert sind, zu verlangen. Dort werden die meisten Daten gespeichert, die bei einer Nutzung von Microsoft/MS365 und Teams anfallen. Nach Angaben von Microsoft ist die Anzahl dieser Anfragen extrem gering, zudem wird Microsoft sich nach eigenem Bekunden gerichtlich dagegen wehren und die jeweiligen Nutzer soweit gesetzlich möglich informieren. Die wenigsten Anfragen dürften, falls überhaupt, schulische Konten betreffen. Microsoft gibt für Juli - Dezember 2019 insgesamt 3.310 Anfragen von Ermittlungsbehörden an. Davon kamen die meisten aus Deutschland.

4.3 Wo werden meine personenbezogenen Daten verarbeitet?

Die Verarbeitung von personenbezogenen Daten in MS365 und angebotenen Produkten erfolgt überwiegend auf Servern mit Standort Deutschland. Es ist möglich, dass in bestimmten Fällen sogenannte Telemetriedaten, eine Art Diagnosedaten, in den USA verarbeitet werden. Dienste, die Daten auf nicht europäischen Servern speichern, werden von der Fürst-Johann-Ludwig-Schule deaktiviert, sodass keine Nutzerdaten anfallen.

4.4 Wie sicher ist MS365?

Die Plattform genügt allen gängigen Sicherheitsstandards für Cloud Plattformen, eingeschlossen der Verschlüsselung der Nutzerdaten bei Transport und Lagerung. Dazu gehören unter anderem die Zertifizierung nach ISO 27001 in Bezug auf die generelle IT-Sicherheit und ISO 27018 hinsichtlich des Umgangs mit personenbezogenen Daten in der Cloud. Microsoft Cloud Services werden auch mindestens jährlich anhand der Standards SOC 1 (SSAE18, ISAE 3402),

SOC 2 (AT Section 101) und SOC 3 überprüft. Aber auch branchenspezifische Zertifizierungen wie HIPAA/HITECH liegen vor.

Damit erfüllt Microsoft auch alle Anforderungen für das C5⁵ Testat des Bundesministeriums für Sicherheit in der Informationstechnik (BSI).

4.5 Wo kann ich mehr zum Datenschutz von MS365 erfahren?

Weitere Informationen zum Thema Datenschutz und Sicherheit bei Microsoft:

<https://www.microsoft.com/de-de/trust-center/privacy>

Die aktuelle Datenschutzerklärung von Microsoft:

<https://privacy.microsoft.com/de-de/privacystatement>

Von besonderer Bedeutung ist dabei bezüglich der personenbezogenen Daten von Personen in der Schule der folgende Abschnitt:

“Für Microsoft-Produkte, die von Ihrer K-12-Schule* bereitgestellt werden, einschließlich Microsoft 365 Education, wird Microsoft:

- neben den für autorisierte Bildungs- oder Schulzwecke erforderlichen Daten keine personenbezogenen Daten von Schülern/Studenten erfassen oder verwenden,
- personenbezogene Daten von Schülern/Studenten weder verkaufen noch verleihen,
- personenbezogene Daten von Schülern/Studenten weder zu Werbezwecken noch zu ähnlichen kommerziellen Zwecken wie Behavioral Targeting von Werbung für Schüler/Studenten verwenden oder freigegeben,
- kein persönliches Profil eines Schülers/Studenten erstellen, es sei denn, dies dient der Unterstützung autorisierter Bildungs- oder Schulzwecke oder ist von den Eltern, Erziehungsberechtigten oder Schülern/Studenten im angemessenen Alter genehmigt, und
- seine Anbieter, an die personenbezogene Daten von Schülern/Studenten ggf. zur Erbringung der Bildungsdienstleistung weitergegeben werden, dazu verpflichten, dieselben Verpflichtungen für personenbezogene Daten der Schüler/Studenten zu erfüllen.”

(*) Amerikanische Bezeichnung einer öffentlich-rechtlichen Einrichtung „von Kindergarten (K) bis zum 12.Schuljahr (12)“

4.6 Was tut die Schule zum Schutz meiner personenbezogenen Daten in @fjls.Cloud-Diensten?

Als Schule hat für uns der Schutz der personenbezogenen Daten unserer Schüler und Lehrkräfte oberste Priorität. Deshalb sorgen wir durch technische und organisatorische Maßnahmen dafür, dass die Nutzung von @fjls.Cloud-Diensten mit der größtmöglichen Sicherheit abläuft. Wir haben speziell MS365 so voreingestellt, dass durch das Handeln und Fehler der Nutzer selbst möglichst wenige Risiken entstehen können. Ganz zentral ist die Schulung der Nutzer für einen sicheren und verantwortungsvollen Umgang mit allen Werkzeugen. Im Rahmen der Erteilung des Zugangs findet eine Grundschulung statt. Diese wird durch eine jährliche Belehrung und die Nutzungsvereinbarung/Dienstanweisung ergänzt.

4.7 Kann eine Einwilligung nach dem Urteil des EUGH zum EU-US Privacy Shield noch genutzt werden?

Das ist möglich, setzt aber voraus, dass die etwaige Übermittlung von personenbezogenen Daten in die USA entsprechend so abgesichert ist, dass sie den Vorgaben der DS-GVO entspricht. Dieses könnte beispielsweise durch zusätzliche technische Maßnahmen und Garantien seitens Microsofts erfolgen (siehe unten). Die Standardvertragsklauseln, auf welche Microsoft seine Datenübermittlungen aktuell stützt, reichen nach Auffassung des EUGH allein dafür nicht aus. Jede Schule, jeder Schulträger, jedes Bundesland hat darüber hinaus die Möglichkeit, mit Microsoft in Form von Nebenabreden in Ergänzung zu den OST und Data Processing Addendum zusätzliche Maßnahmen und Garantien auszuhandeln.

⁵ [BSI - Kriterienkatalog C5 \(bund.de\)](https://www.bsi.bund.de/BSI/Kriterienkatalog/C5)

Garantien durch Microsoft im Rahmen von „Defending your Data“ seit November 2020:

1. **Anspruch auf Schadensersatz für die betroffene Person**, deren Daten unrechtmäßig verarbeitet wurden und die dadurch einen materiellen oder immateriellen Schaden erlitten hat;
2. **Information der betroffenen Person**, wenn Microsoft durch eine staatliche Anordnung rechtlich bindend dazu verpflichtet wurde, Daten an US-Sicherheitsbehörden herauszugeben;
3. **Verpflichtung von Microsoft**, den Rechtsweg zu beschreiten und die US-Gerichte anzurufen, um die behördliche Anordnung zur Herausgabe der Daten anzufechten.

(Zusammenfassung: Datenschutzbeauftragter des Landes Baden-Württemberg)

Weitere von Informationen von Microsoft hier: [Maßnahmen zum Schutz Ihrer Daten | News Center Microsoft](#)

Eine Liste der zusätzlichen datenschutzbezogenen Maßnahmen der Schule finden Sie auf der Homepage der Schule unter „Datenschutz“.

Ist es nicht möglich, die Übermittlung von personenbezogenen Daten durch zusätzliche technische Maßnahmen abzusichern, sehen viele Fachjuristen Zweifel, diese Übermittlung durch eine Einwilligung zu legitimieren, da Art. 49 Abs. 1 lit. a gemäß Art. 49 Abs. 3 ausdrücklich nicht durch öffentliche Stellen in Ausübung hoheitlicher Tätigkeiten genutzt werden kann.

4.8 Was kann ich als Nutzer zusätzlich tun, um den Schutz meiner personenbezogenen Daten zu erhöhen?

Wenn man von einem privaten Endgerät auf MS365 zugreift, könnte man:

- einen sicheren Browser (Brave, Firefox oder DuckDuckGo auf Mobilgeräten) nutzen, der die Erhebung zusätzlicher Daten einschränkt,
- in Browsern keine Cookies speichern bzw. die absolut erforderlichen nach Ende eine Sitzung automatisch löschen,
- den Zugang nicht über die mobilen Apps, sondern einen sicheren Browser vorzunehmen
- den Zugang über ein VPN laufen lassen, um IP und Geolocation zu verschleiern,
- den Zugang auf ein einziges System/Gerät beschränken,
- den Zugang mit einem speziellen Nutzerkonto auf dem Rechner vorzunehmen, in dem es keine Anmeldungen an anderen Konten wie YouTube, WhatsApp, Instagram ... gibt.
- den Zugang über eine virtuelle Maschine oder ein System von einer Live DVD/Live Boot Stick vorzunehmen.
- wenn der Zugang über ein iPad erfolgen soll, sollte dort kein vorheriger oder gleichzeitiger Login an einer anderen nicht schulischen App oder Web-Plattform erfolgen

Ein Teil dieser Maßnahmen führt zu Komfortverlusten bei der Nutzung. Ob man einige oder mehrere dieser Maßnahmen umsetzen möchte, muss jeder Nutzer für sich entscheiden.