Nach den Artikeln 13 und 14 der europäischen Datenschutz-Grundverordnung (DSGVO) hat der Verantwortliche bei der Datenerhebung die folgenden Informationen bereit zu stellen. Dieser Informationspflicht kommt dieses Merkblatt nach.

1) Datenerfassung und Datenschutz in der Schule

- **Wer ist verantwortlich für die Verarbeitung der personenbezogenen Daten?**

Verantwortlich ist die Schule:

Henry-Harnischfeger-Schule
Frankfurter Str. 67
63628 Bad Soden – Salmünster

- **An wen kann ich mich wenden, wenn ich Fragen zum Datenschutz habe?**

Fragen zum Datenschutz können Sie an den behördlich bestellten schulischen Datenschutzbeauftragten stellen:

Frau F. Deist: datenschutz@hhs-live.de

- **Auf welcher Grundlage erheben Schule Personenbezogene Daten?**

- Das Recht zur Verarbeitung und Speicherung von personenbezogenen Daten an der HHS ergibt sich aus dem Hessischen Schulgesetz (HSchG), dem Hessischen Datenschutz- und Informationsfreiheitsgesetz (HDSIG), der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen und dem Artikel 6 Abs. 1 lit. e) der Datenschutzgrundverordnung (DSGVO).
- Werden personenbezogene Daten erhoben, ohne dass die Verarbeitung zur Erfüllung des Bildungs- und Erziehungsauftrages erforderlich ist, erfolgt die Verarbeitung aufgrund einer Einwilligung nach Artikel 6 Abs. 1 lit. a) i.V.m. Artikel 7 DSGVO.
- Die Veröffentlichung personenbezogener Daten im Internet oder in lokalen oder regionalen Printmedien erfolgt nur aufgrund einer Einwilligung nach Artikel 6 Abs. 1 lit. a) i.V.m. Artikel 7 DSGVO.

- **Welche Daten werden erhoben?**

Wenn Sie Ihr Kind an einer hessischen Schule anmelden, wird dort eine **Schülerakte** angelegt. Darin werden folgende Daten erfasst und gesammelt (Art. 30 Abs. 1 S. 2 lit. c DS-GVO):

- **Persönliche Daten, die bei der Schulanmeldung von Ihnen abgefragt wurden: a) Daten der SuS:** Name, Anschrift, Telefonnummer, Geschlecht, Geburtsort, Geburtsdatum, Zugehörigkeit zu einer Religionsgemeinschaft, Staatsangehörigkeit. **b) Daten der Eltern:** Name und Vorname, Stellung zum Kind (z.B. Mutter oder Vater), ggf. alleinige Sorgeberechtigung, Anschrift, Telefonnummer.
- **Schullaufbahndaten:** Beginn der Schulpflicht, Jahr der Einschulung, Zeiten und Bezeichnung aller bisher besuchten Schulen, Versetzungsentscheidungen, Wiederholung von Klassen, bereits erworbene Abschlüsse, ggf. Unterlagen zu sonderpädagogischem Förderbedarf, (Fördergutachten, Beschlüsse der Förderkommission und (Förderbescheide), aufnehmende Schule, Rückmeldungen zur Kontrolle der Schulpflichterfüllung, Datum und Grund des Austritts aus der Schule.

- **Verwaltungsdaten:** Bildungsgang, Klasse, Kurs, Jahrgang, Stufe, Klassenlehrer, Tutor, Fehlzeiten und Entschuldigungen, ggf. ärztliche Atteste, ggf. Teilnahme an der Schülerbeförderung, ggf. Aufzählung der ausgeliehenen Lernmittel, ggf. verhängte Erziehungsmittel oder Ordnungsmaßnahmen, ggf. Unfallberichte und Unfallmeldungen an den GUV.

- **Leistungsdaten:** Entscheidungen über die Zulassung zu Prüfungen und Bildungsgängen, Benachrichtigungen über gefährdete Versetzungen und Abschlüsse, Zeugnisse, Dokumentation der individuellen Lernentwicklung.

• Darf eine Schule Daten weitergeben und an wem?

Nur die Schule, die Ihr Kind gerade besucht, kann und darf auf diese Daten und die Akte zugreifen. Ggf. dürfen aber bestimmte personenbezogene Daten gegenüber folgenden Kategorien von Empfänger offengelegt werden (Art. 30 Abs. 1 S. 2 lit. d): Schulen bei Schulwechsel, betr. Eltern, betr. Schülerinnen und Schüler, Staatliches Schulamt (SSA), Hessisches Kultusministerium, ggf. Drittland oder internationale Organisation (als Kategorie), Archiv (siehe Aufbewahrungsfristen).

• Was ist mein Auskunftsrecht?

Der betroffenen Person stehen unter den in den Artikeln jeweils genannten Voraussetzungen die nachfolgenden Rechte zu:

- das Recht auf Auskunft nach Artikel 15 DSGVO,
- das Recht auf Berichtigung nach Artikel 16 DSGVO,
- das Recht auf Löschung nach Artikel 17 DSGVO,
- das Recht auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO,
- das Recht auf Datenübertragbarkeit nach Artikel 20 DSGVO,
- das Widerspruchsrecht nach Artikel 21 DSGVO,
- das Recht auf Beschwerde bei einer Aufsichtsbehörde nach Artikel 77 DSGVO
- das Recht, eine erteilte Einwilligung jederzeit widerrufen zu können, ohne dass die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung hierdurch berührt wird.

Bei den hier genannten Informationsrechten gelten allerdings ggf. besondere Einschränkungen.

• Wie und wo werden diese Daten gespeichert, verarbeitet, geschützt und wann werden sie gelöscht?

Personenbezogene Daten werden folgendermaßen erfasst und verarbeitet:

- in elektronischer Form in der Lehrer- und Schülerdatenbank (LUSD) und im Schulportal Hessen (SPH). (Bei Office 365 und Microsoft Teams werden nur wenige Grund- und Log-Daten verarbeitet. Siehe dazu Punk 3 „Microsoft Teams“)
- in Papierform (Schülerakte):

Der Zugriff in elektronischer Form ist nur im Rahmen eines pädagogischen Auftrags erlaubt. Die Datenbanken sind nur von AdministratorInnen über ein abgesichertes Schulverwaltungsnetz erreichbar. Die Einsicht in die Papier-Akten ist nicht unbeschränkt. Sie sind nur berechtigten Personen zugänglich, sind per Dienstanweisung vertraulich zu behandeln, verlassen nie die Schule und sind außerhalb der Dienstzeiten versperrt.

Ausführliche Informationen über die gespeicherten Daten von Schülerinnen und Schülern, Eltern, Lehrkräften und Ausbildern sowie deren Speicherdauer liefert die Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen:

- Informationen zu den verarbeiteten und gespeicherten Daten (lt. Verordnung): Anlage I (30.01.22)
- Informationen zur Speicherdauer (lt. Verordnung): Anlage III (30.01.22)
- Link zur Verordnung: https://www.rv.hessenrecht.hessen.de/bshe/document/hevr-SchulStatErhVHEV1IVZ (Zum 30.01.22 aktuelle verfügbare Fassung der Gesamtausgabe. Stand: letzte berücksichtigte Änderung: § 17 geändert durch Artikel 3 der Verordnung vom 1. April 2015 (ABl. S. 113)
- Weitere Informationen HIER. (30.01.22)

2) Lehrer- und Schülerdatenbank (LUSD)

Im Jahre 2007 wurde die Lehrer- und Schülerdatenbank (LUSD) als ein zentrales, vom Hessischen Kultusministerium initiiertes und technisch mitbetreutes Instrumentarium für die Schulverwaltung geschaffen.

Die LUSD entlastet die Schulen des Landes im täglichen **Verwaltungsbetrieb**. Die bundesweit einzigartige IT-Lösung verbessert zusätzlich den Informationsfluss zwischen Schulen, Schulämtern, Lehrkräfteakademie und Ministerium. Bis zur Einführung dieser web-basierten, zentralen Datenbank nutzten die 2000 hessischen Schulen dezentrale IT-Anwendungen, was nicht zuletzt im Sinne des Datenschutzes hinsichtlich der Integrität der Daten und des Zugriffsschutzes problembehaftet war. Der zentrale Lösungsansatz stellt einerseits **einen datenschutzrechtlichen Mehrwert** dar, weil die zentrale Architektur der Datenbank einheitliche Standards im Rahmen der Datenverarbeitung sicherstellt. Zum anderen ist die Qualität und Aktualität der Daten durch die zentralen Eingabe- und Meldestrukturen auf eine bessere Grundlage gestellt. **Schüler-, Unterrichts- und Leistungsdaten werden in Hessen mit der LUSD erfasst und bearbeitet**. Die Verwaltung des **Unterrichtseinsatzes der Lehrkräfte** zählt dabei ebenso zum Aufgabenbereich wie die **Prüfung von Kursbelegungen** bis hin zur **Zulassung für Abitur, Haupt- und Realschulabschlüsse**. Der **Zeugnisausdruck** erfolgt ebenfalls über die LUSD. Die Bildungsverwaltung hat so jederzeit online Zugriff auf aktuelle Informationen – und das gesichert dank des geschützten **Schulverwaltungsnetzes**.

Zusätzliche Anwendungserweiterungen bieten ergänzende Funktionen, wie z.B. die Informations- und Kommunikationsplattform (LUSDIK), die unterschiedliche Auswertungen auf Basis aggregierter Daten durch die Schulämter ermöglicht.

Die **Datenhaltung** erfolgt beim zentralen **IT-Dienstleister des Landes Hessen**, der Hessischen Zentrale für Datenverarbeitung (HZD). Die datenschutzrechtlichen Anforderungen an die Anwendung wurden zur damaligen Zeit in direktem Kontakt zwischen dem Hessischen Datenschutzbeauftragten und dem HKM geklärt. Die spezifische Anwendung für die hessische Schul- und Schulverwaltungslandschaft, verbunden mit einer sicheren Cloudlösung, dem kontinuierlichen Support sowie einer nutzerbezogenen Weiterentwicklung sind ein erstes Beispiel für digitale Souveränität. Dabei basiert die Anwendung selbst wie auch die Verarbeitung der personenbezogenen Daten zehntausender Lehrkräfte und hunderttausender Schülerinnen und Schüler auf der Grundlage von Parametern, die durch **datenschutzrechtlicher Vorgaben den erforderlichen Grundrechtsschutz für die Betroffenen sicherstellt**.

3) Schulportal Hessen (SPH)

Es existiert seit mehr als zehn Jahren und hat sich über die Jahre zu einem umfangreichen Set an Anwendungen und Services angereichert. Bei den Anwendungen kommt grundsätzlich nur Open-Source zum Einsatz. Ein Teil der Anwendungen wurde ausgebaut und auf eine skalierbare Cloudumgebung migriert, um ab dem Schuljahr 2020/2021 als nutzerfreundliche Plattform allen hessischen Schulen zur Verfügung zu stehen. Das HKM als oberste Schulaufsichtsbehörde sowie die HZD als zentraler IT-Dienstleister für die Hessische Landesverwaltung beauftragten hierfür den deutschen Dienstleister German Edge Cloud mit Sitz in Eschborn bei Frankfurt am Main. Auch wenn derzeit eine umfangreiche, datenschutzrechtliche Bewertung des SPH durch den HBDI erst beginnt, erscheinen wesentliche Strukturen des Portals im Hinblick auf die Datensouveränität und damit Wahrung der Rechte der von der Datenverarbeitung Betroffenen zielgerichtet gewährleistet.
90 Prozent der weiterführenden öffentlichen Schulen nutzen jetzt die Plattform. [1]

4) Corona-Maßnahmen

Antigen Tests und Dokumentation des Corona-Impfschutzes:

Mit dem **Wegfall der Testpflicht am 02.05.2022** entfallen auch die Rechtsgrundlagen für die Datenverarbeitung, die daran bisher anknüpften. Die bisher gespeicherten Daten werden unverzüglich nach Ablauf des 30. April 2022, spätestens aber bis zum 15. Mai 2022, gelöscht.

Das betrifft im Einzelnen

- die **Einwilligungserklärungen zur Durchführung regelmäßiger AntigenSelbsttests**, soweit sie nicht die freiwillig fortgesetzte Testung von Schülerinnen und Schülern mit Anspruch auf sonderpädagogische Förderung in den Förderschwerpunkten „geistige Entwicklung“ oder „körperlichmotorische Entwicklung“ betreffen,

- Daten, die im Fall eines **Positivtests** aufgenommen worden waren, um sie dem Gesundheitsamt zu übermitteln,

- Angaben über die Vorlage von **Test-, Impf- oder Genesenennachweisen,**

- **dienstliche Erklärungen der Lehrkräfte und des sonstigen Personals** an Schulen über die Durchführung häuslicher Testungen,

- die **Dokumentation der Befreiung** einer Schülerin oder eines Schülers mit sonderpädagogischem Förderbedarf von der Nachweispflicht und Testteilnahme sowie

- die **elterliche Erklärung** über häusliche Testungen dieser Schülerinnen und Schüler.

Zu löschen sind darüber hinaus, sofern sie noch in den Schulen vorhanden sind, auch **Angaben über die Vorlage von ärztlichen Attesten**, die bestätigen, dass eine Person aufgrund einer Behinderung oder einer gesundheitlichen Beeinträchtigung keine medizinische Maske tragen kann. Sofern für die Befreiung von der Teilnahme am Präsenzbetrieb im Einzelfall weiterhin ärztliche Atteste zur Begründung des Umstands vorgelegt werden, dass die befreite Person oder eine im häuslichen Umfeld lebende Person im Fall der Ansteckung mit dem SARS-CoV2-Virus einem erhöhten Risiko eines schweren Krankheitsverlaufs ausgesetzt wäre, können die Angaben über die Vorlage dieser ärztlichen Atteste selbstverständlich weiterhin gespeichert werden. Dasselbe gilt für die Speicherung der Angabe von

[1] Quelle: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Digitale%20Souveraenitaet%2005_04_2022_0.pdf (Stand: 05. April 2022)

Schulversäumnissen als solchen, soweit sie in der Schülerakte oder im Klassenbuch dokumentiert sind; nicht gespeichert werden darf der Grund des Versäumnisses.

Die mit Schreiben vom 23. August 2021 übersandten „Hinweise zur Datenverarbeitung im Zusammenhang mit Maßnahmen zur Bewältigung der COVID-19-Pandemie“ finden daher bis auf Weiteres keine Anwendung mehr. [2]

5) Microsoft – Teams

Auf dieser Seite informieren wir dich/ Sie über die zur Nutzung von **Microsoft Teams** erforderliche Verarbeitung von personenbezogenen Daten.

- **Zu welchem Zweck sollen meine Daten verarbeitet werden?**

Die Verarbeitung ist erforderlich zur Nutzung von **Microsoft Teams,** einer Kommunikations- und Lernplattform mit der Möglichkeit zu Audio- und Videokonferenzen und zur Durchführung von Online-Unterrichtseinheiten in der Lerngruppe und zur individuellen Betreuung und Beratung in Kleingruppen oder Einzeltreffen zwischen SchülerInnen und Lehrkraft.

- **Auf welcher Rechtsgrundlage erfolgt die Verarbeitung?**

Die Verarbeitung erfolgt auf der Grundlage deiner/ Ihrer Einwilligung.

- **Darf die Schule Office 365 einsetzen?**

Grundsätzlich dürfen Bildungseinrichtungen die Unternehmens-Plattform **Microsoft Office 365** einsetzen, wenn sie dabei die Datenschutzgrundverordnung einhalten. Es ist wichtig zu verstehen, dass die Datenschutzverantwortung bei jedem IT-Dienst, den die Bildungseinrichtung einsetzt, zur Gänze bei der Bildungseinrichtung liegt, nicht bei **Microsoft**. Bildlich gesprochen bietet Microsoft ein Fahrzeug an, das nach StVO alle Vorschriften erfüllt und zugelassen ist, aber der Fahrer ist die Bildungseinrichtung. Sie muss festlegen, warum und welche personenbezogene Daten verarbeitet und gespeichert werden, wie lange sie gespeichert bleiben und wer Zugriff auf die Daten hat.

- **Welche personenbezogenen Daten werden bei der Nutzung von Microsoft Teams verarbeitet?**

Verarbeitet werden Daten zur Erstellung eines **Nutzerkontos** (E-Mail Adresse, Passwort, Schulzugehörigkeit, Zugehörigkeit zu Teams, Rollen und Rechte), zur Anzeige eines **Nutzerstatus** und von **Lesebestätigungen** (Chat), erstellte **Chat-Nachrichten**, **Sprachnotizen**, **Bild- und Tondaten** in Video- und Audiokonferenzen, Inhalte von **Bildschirmfreigaben**, durch Hochladen **geteilte Dateien**, erstellte **Kalendereinträge**, **Status von Aufgaben** (zugewiesen, abgegeben, Fälligkeit, Rückmeldung), in Word, Excel, PowerPoint und OneNote **erstellte und bearbeitete Inhalte**, Eingaben bei **Umfragen**, **technische Nutzungsdaten** zur Bereitstellung der Funktionalitäten und Sicherheit von Microsoft Teams und in Teams integrierte Funktionen. **Eine Speicherung der Bild- und Tondaten von Videokonferenzen durch die Schule erfolgt nicht.**

[2] *Ministerschreiben an Schulleitungen und Lehrkräfte* und Anlage *Informationen über das freiwillige Testangebot zum Nachweis des Coronavirus SARS-CoV-2 ab Montag, den 2. Mai 2022* vom 28.04.22

- **Wer hat Zugriff auf meine personenbezogenen Daten?**

Auf alle in **Teams** durch NutzerInnen eingestellten Dateien, Inhalte und Kommentare haben jeweils die Personen Zugriff, mit denen sie geteilt werden. Das können Einzelpersonen sein oder MitgliederInnen eines Teams oder Channels in einem Team. Lehrkräfte haben Zugriff auf innerhalb von gestellten Aufgaben vorgenommene Bearbeitungen und erstellte Inhalte. Alle TeilnehmerInnen einer Videokonferenz haben Zugriff im Sinne von Sehen, Hören und Lesen auf Inhalte der Videokonferenz, Chats, geteilte Dateien und Bildschirmfreigaben. In einem Chat haben alle TeilnehmerInnen Zugriff auf eingegebene Inhalte und geteilte Dateien. **Der Anbieter** hat Zugriff auf die bei der Nutzung von **Microsoft Teams** anfallenden Daten, soweit dieses zur Erfüllung seiner Verpflichtung im Rahmen des mit der Schule abgeschlossenen Vertrags zur Auftragsverarbeitung erforderlich ist. **US-Ermittlungsbehörden** haben Zugriff nach US amerikanischem Recht (siehe unten).

- **An wen werden die Daten übermittelt?**

Microsoft verarbeitet deine/Ihre personenbezogenen Daten ausschließlich in unserem Auftrag. Demnach darf **Microsoft** sie nur entsprechend unserer Weisungen und für unsere Zwecke und nicht für eigene Zwecke nutzen, also weder für Werbung und auch nicht, um sie an Dritte weitergeben.

- **Wo werden meine personenbezogenen Daten verarbeitet?**

Die Verarbeitung von personenbezogenen Daten in **Microsoft Teams** und angebundenen Produkten erfolgt auf Servern mit Standort Europa. Die Speicherung der Nutzdaten erfolgt nur innerhalb der EU und die Daten verlassen die EU nicht. **Microsoft** Rechenzentren werden laufend nach strengsten internationalen Standards zertifiziert, sowohl nach ISO 27001, 27002, als auch nach dem Datenschutzstandard ISO 27018. Alle Nutzdaten sind server- und verbindungsseitig verschlüsselt. Es ist möglich, dass sogenannte Telemetriedaten, eine Art Diagnosedaten, in den USA verarbeitet werden (siehe unten).

- **Was macht Microsoft mit den Daten?**

✓ **Microsoft** gibt für die Unternehmenscloud **Office 365** weder Daten weiter noch werden sie inhaltlich in irgendeiner Art und Weise ausgewertet.
✓ Das Angebot ist strikt werbefrei.
✓ Die **Microsoft** Rechenzentren für deutsche Kunden liegen in Deutschland (Frankfurt und Berlin). Die Daten in den Rechenzentren sind in mehreren Ebenen verschlüsselt.
✓ **Microsoft** ermöglicht dem Nutzer von **Office 365** eine Ende-zu-Ende Verschlüsselung, Mehrfaktor-Anmeldung, besonderen Schutz gegen gefährliche Anhänge in E-Mails und gegen gefälschten Links in Daten.
✓ Die Nutzdaten bleiben immer in Deutschland gespeichert und verlassen somit die EU nicht.
✓ Der Datentransfer zu **Office 365** ist verbindungstechnisch verschlüsselt und zusätzlich innerhalb und zwischen den Rechenzentren verschlüsselt.

- **Wer sieht die Anmeldedaten?**

Der Anmeldename in **Office 365** wird auf allen Anmeldeservern von **Microsoft** weltweit gespeichert, damit Sie auch im Nicht-EU Ausland auf Ihre Daten zugreifen können. Alle weiteren Daten verlassen jedoch die EU nicht. **Microsoft** Supportingenieure aus der EU erhalten nur nach expliziter Anforderung durch unseren Systembetreuer Zugriff auf Daten, um ein technisches

Problem zu lösen. Supportingenieure außerhalb der EU können technisch durch die sog. Lock-Box-Technologie keinen Zugriff auf **Office 365** Instanzen der EU erhalten.

- **Wie lange werden meine Daten gespeichert?**

Die Speicherung von Daten, welche zur Bereitstellung des Nutzerkontos verarbeitet werden, sowie erstellte und geteilte Inhalte, Kommentare, Chat-Nachrichten, Sprachnachrichten, zugewiesene, bearbeitete und abgegebene Inhalte und Kalendereinträge, endet, sobald der Nutzer/die Nutzerin die Schule verlassen hat, seine Einwilligung ganz oder in Teilen widerruft oder einer Verarbeitung widerspricht. Die Löschung erfolgt innerhalb von 2 Monaten nach Verlassen der Schule. Die Löschung aus den Systemen von **Microsoft** ist vom Zeitpunkt der Löschung eines Kontos oder von Inhalten durch die Schule nach 90 Tagen abgeschlossen. Derselbe Zeitraum gilt auch für die Löschung von Dateien durch den Nutzer selbst. Ton- und Bilddaten von Video- und Audiokonferenzen werden von der Schule nicht aufgezeichnet und gespeichert. Inhalte in von anderen geteilten Dateien, bearbeitete und abgegebene Aufgaben und Nachrichten in Gruppenchats werden gespeichert, solange ein Team besteht. Teams für Klassen- und Lerngruppen werden spätestens 5 Jahre nach Ende der Schulzeit der betroffenen SchülerIn samt ihren von SchülerInnen erstellten, geteilten und bearbeiteten Inhalten und Chats gelöscht. Inhalte von Chats bestehen, solange das Konto des anderen Nutzers besteht.

- **Datenschutz bei Verarbeitung von Daten in den USA**

Bei der Nutzung von **Microsoft Teams** 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.

- **Thema CLOUD-Act**

Der Cloud-Act regelt das Recht eines normalen Zivilgerichts der USA, Daten im Rahmen eines Strafverfahrens z. B. von **Microsoft** oder einer anderen Firma in der Welt direkt zu erbitten statt über ein Rechtshilfeverfahren, das Jahre dauert und nicht mehr zeitgemäß ist. Im Rahmen des CLOUD-Act haben US-Ermittlungsbehörden auch Möglichkeiten, bei **Microsoft** die Herausgabe von personenbezogenen Daten, die auf Servern in der EU gespeichert sind, zu verlagern. Dort werden die meisten Daten gespeichert, die bei einer Nutzung von **Microsoft/ Office 365 und Teams** anfallen. EU Bürger sind davon nicht betroffen (solange Sie nicht in USA strafbar werden).
Am 20.11.2020 kündigte Microsoft an, diese Klauseln DSGVO-Konform zu ändern. Mehr dazu **HIER**.(30.01.22)

- **Wie sicher ist Microsoft Teams?**

Die Plattform genügt allen gängigen Sicherheitsstandards für Cloud Plattformen. Jeder Hersteller von Software, die über das Internet bezogen oder genutzt wird, benötigt zur Vertragserfüllung Daten, mit der die korrekte und sichere Funktion der Software sichergestellt werden kann. Das gilt für jedes Betriebssystem, für jeden Browser, egal ob OpenSource oder kommerziell. Microsoft speziell überträgt

niemals Nutzerdaten ohne Kenntnis und Zustimmung des Betroffenen und dokumentiert sehr sorgfältig, welche Telemetriedaten für welchen Zweck übertragen werden.
Als Reaktion auf geäußerte Bedenken des EUGH zu den EU Standardvertragsklauseln hat **Microsoft** seine Vertragsklauseln kürzlich noch einmal erweitert, sodass sie über die neuen Vorgaben hinausgehen. Dies wurde auch von den Landesdatenschutzbehörden in Baden-Württemberg und Bayern sehr positiv bewertet. Die Speicherung der Nutzdaten erfolgt nur innerhalb der EU und die Daten verlassen die EU nicht. **Microsoft** Rechenzentren werden laufend nach strengsten internationalen Standards zertifiziert, sowohl nach ISO 27001, 27002, als auch nach dem Datenschutzstandard ISO 27018. Alle Nutzdaten sind server- und verbindungsseitig verschlüsselt.

- **Hat der Hessische Datenschutzbeauftrage (HDBI) über die Nutzung von Microsoft Position bezogen?**

Ja, im Interesse einer flexiblen Bekämpfung der Corona-Pandemie hat der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) übergangsweise den Einsatz von Videokonferenzsystemen in Schulen weitgehend **für alle zur Verfügung stehenden Anwendungen** auf der Grundlage von Art. 6 Abs. 1 Buchst. d) und e) der Datenschutz-Grundverordnung (DS-GVO) **geduldet**, auch wenn deren Datenschutzkonformität noch nicht abschließend geklärt war. Mehr dazu **HIER** (Artikel vom 31.01.22, abgerufen am 28.04.22.)
Am 20.11.2020 kündigte **Microsoft** an, seine Standardvertragsklauseln ergänzen zu wollen. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit begrüßt die Initiative zur Absicherung internationaler Datentransfers. Mehr dazu **HIER**. (30.01.22)

- **Wo kann ich mehr zum Datenschutz von Microsoft Teams erfahren?**

Die aktuelle Datenschutzerklärung von Microsoft kann hier in deutscher Sprache eingesehen werden:

Privacy.microsoft (Aktualisierung vom 12.2021 - abgerufen am 30.01.22)

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."*

Weitere FAQ und Informationen HIER (30.01.22)

6) Dokumentation des Masern-Impfschutzes[3]

Aufgrund des seit dem 1. März 2020 geltenden Masernschutzgesetztes sind Beschäftigte von Gemeinschaftseinrichtungen und medizinischen Einrichtungen (im folgenden zusammen „Einrichtungen") sowie Schülerinnen und Schüler und in Gemeinschaftseinrichtungen betreute Kinder verpflichtet, einen Nachweis über ihren Masernschutz zu erbringen. Die Bundeszentrale für gesundheitliche Aufklärung erklärt in einem Merkblatt, wie die Masern-Impfung durch den Impfausweis konkret nachgewiesen wird[4]. Die Leitung der Einrichtungen müssen den Impfnachweis bzw. eine ausreichende Masern-Immunität (Serostatus) kontrollieren und dokumentieren, bevor die jeweiligen Personen die Beschäftigung aufnehmen bzw. betreut werden dürfen.
Rechtsgrundlage

- **Auf welcher Rechtsgrundlage erfolgt die Verarbeitung?**

Der Nachweis des Impfschutzes kann nach § 20 Abs. 9 Infektionsschutzgesetz („IfSG") durch Vorlage des Impfpasses oder durch ein ärztliches Attest über den Impfschutz bzw. die Masern-Immunität erbracht werden. Bei einer medizinischen Kontraindikation, die gegen eine Impfung spricht, kann stattdessen ein entsprechendes ärztliches Attest vorgelegt werden.
Die Verarbeitung dieser Gesundheitsdaten durch die Einrichtungen ist in der Regel nach Art. 6 Abs. 1 lit. c) i.V.m. Art. 9 Abs. 2 lit. i) DSGVO i.V.m. § 20 Abs. 9 IfSG und § 20 Abs. 1 Nr. 3 HDSIG bzw. § 22 Abs. 1 Nr. 1 lit. c) BDSG legitimiert. Im Beschäftigtenkontext gilt außerdem § 23a IfSG, nach welchem der Arbeitgeber unter bestimmten Voraussetzungen den Impf- und Serostatuts der Beschäftigten verarbeiten darf. Nach der Gesetzesbegründung zum Masernschutzgesetz ist § 23a IfSG auf die Prüfung des Masern Impf- bzw. Serostatus anwendbar.[2]
Der Schutz vor den Gesundheitsgefahren aufgrund der hoch ansteckenden Infektionskrankheit Masern stellt ein legitimes öffentliches Interesse im Sinne dieser Normen dar. Darüber hinaus sind diese Datenverarbeitungen in der Regel auch zur Verhinderung der Ausbreitung von Maserninfektionen erforderlich.

- **Wie, wo und wie lange werden meine Daten gespeichert?**

Die Daten werden als Aktennotiz in die SchülerInnen-Akte bis Ende der Schulzeit in der Einrichtung abgelegt. Im geänderten IfSG wird der Grundsatz der Datensparsamkeit (§ 20 Abs. 9 S. 1 Nr. 3 IfSG) im Rahmen des Wechsels der Einrichtung berücksichtigt. Die Beschäftigten bzw. betreuten Personen müssen in diesem Fall nicht erneut ihren Impfausweis oder eine ärztliche Bescheinigung vorlegen. Haben sie ihren Impfschutz oder ihre Immunität schon einmal gegenüber einer Einrichtung nachgewiesen,

[3] Quelle: https://datenschutz.hessen.de/datenschutz/gesundheits-und-sozialwesen/gesundheitswesen/datenschutzkonforme-kontrolle-und (30.01.22)
[4] https://www.masernschutz.de/fileadmin/Masernschutzgesetz/Downloads/Merkblatt-Masernschutzgesetz-Masernimpfung.pdf (30.01.22)

können sie sich dies von einer staatlichen Stelle oder der Leitung der alten Einrichtung bestätigen lassen. Diese Bestätigung ist als Nachweis gegenüber der neuen Einrichtung ausreichend und muss von dieser akzeptiert werden. Eine erneute Vorlage des Impfausweises ist nicht notwendig und darf nicht verlangt werden.

7) Datenschutz Leicht erklärt:

Die vom Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. ins Leben gerufene Initiative „Datenschutz geht zur Schule“ sensibilisiert Schüler:innen in ganz Deutschland dafür, mit eigenen Daten und den Daten anderer im Internet und in den sozialen Medien sicherer und bewusster umzugehen.

➔ https://www.datenschutz-leicht-erklaert.de/