

Informationen gemäß Artikel 12 ff. EU-Datenschutz-Grundverordnung (DSGVO) aufgrund der Erhebung von personenbezogenen Daten

Im Zusammenhang mit der Einführung eines Lernmanagementsystems an unserer Schule werden Ihre personenbezogenen Daten als **Schülerin, Schülern oder Elternteil** erhoben. Bitte beachten Sie hierzu nachstehende Datenschutzhinweise:

1. Angaben zum Verantwortlichen und dessen Vertreter

Verantwortlich für die Datenerhebung ist:
Bezeichnung: Gemeinschaftsschule Wartbergschule Niederndodeleben
Schulleitung: Herr Rüdiger Schöndube
Straße: Goethestr. 15
Postleitzahl: 39167
Ort: Niederndodeleben
Telefon: 039204 7690
E-Mail-Adresse: kontakt@sk-niederndodeleben.bildung-lsa.de

2. Angaben zum Datenschutzbeauftragten der Schule/ des LSA

Die Kontaktdaten des Datenschutzbeauftragten der Schule lauten:
Rüdiger Schulze / stellv. Direktor
Straße: Goethestr. 15
Postleitzahl: 39167
Ort: Niederndodeleben
Telefon: 039204 7690
E-Mail-Adresse: planer@sk-niederndodeleben.bildung-lsa.de

3. Zweck/e der Verarbeitung, Kategorien der Daten und Rechtsgrundlage/n der Verarbeitung

Wir beabsichtigen die unten angegebenen Datenarten zum Zweck der Bereitstellung eines pädagogischen Schulnetzwerks auf Basis der AIX-Concept-Software-Lösung von MSNpro Cloud¹ zu verarbeiten. Damit werden u.a. folgende Funktionalitäten angeboten:

- Interaktives Arbeiten
- Zugriff von Smartphone und Tablet mit Apps
- Effektives Nutzen von Anwendungen im Unterricht
- Material mit Schülern, Klassen und dem Kollegium teilen
- Zugriff vom eigenen Smartphone oder Tablet
- Teilen von Tafelbildern und multimedialen Inhalten
- Verschlüsselung und Speicherung personenbezogener Daten
- Gemeinsame Datennutzung
- Einholung einer Einwilligung zur Datenverarbeitung

Folgende Datenarten sind regelmäßig Gegenstand der Verarbeitung:

- Stammdaten wie Benutzername, Passwort (verschlüsselt), Anzeigename, Familienname, Vorname, Klasse, Kurse, Kursjahr bzw. Schuljahr, E-Mailadresse

¹ Siehe: <https://aixconcept.de/>, AixConcept GmbH, Wallonischer Ring 37, 52222 Stolberg

- Technische Daten wie Benutzergruppe, Personenrolle, Benutzerzugang (aktiv, gesperrt), Spracheinstellung, Letzte Anmeldung, Protokolldaten, persönliche Programmeinstellungen

Bei Verwendung der Unterrichtszentrale: Rechnername, IP-Adresse.

Bei Verwendung des Einwilligungsportals: IP-Adresse zum Zeitpunkt der Einwilligung / des Widerrufs der Einwilligung, Name des Schülers und/oder dessen Vertreter, E-Mailadresse des Schülers oder dessen Vertreter, Mobilfunknummer des Schülers oder dessen Vertreter sowie Datum der Einwilligung / des Widerrufs der Einwilligung.

Bei der Nutzung von Online-Meetings hängt der Umfang der Daten davon ab, welche Angaben zu Daten Sie vor bzw. bei der Teilnahme an einem „Online-Meeting“ machen. Regelmäßig werden folgende personenbezogene Daten verarbeitet: Meeting-Metadaten, z. B. Datum, Uhrzeit, Meeting-ID, Telefonnummern, Ort sowie Text-, Audio- und Videodaten. Sie können die Kamera oder das Mikrofon im Vorfeld oder nachträglich jederzeit selbst abschalten bzw. stummstellen.

Rechtsgrundlage für die Verarbeitung Ihrer personenbezogenen Daten innerhalb des pädagogischen Netzwerks ist Ihre Einwilligung nach Art. 6 Abs. 1 S. 1 Buchstabe a DSGVO.

Rechtsgrundlage für die Verwendung des Einwilligungsportals, also die Verarbeitung Ihrer eMail-Adresse bzw. dem Namen des Schülers/der Schülerin zur elektronischen Einholung dieser Einwilligung ist unser berechtigtes Interesse nach Art. 6 Abs. 1 S. 1 Buchstabe f DSGVO. Falls Sie uns Ihre eMail-Adresse nur zu diesem Zweck direkt übermitteln, ist die Rechtsgrundlage Ihre Einwilligung nach Art. 6 Abs. 1 S. 1 Buchstabe a DSGVO.

Die Erteilung der Einwilligung ist freiwillig. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile. Sie können Ihre Einwilligung jederzeit widerrufen. Wenden Sie sich dazu bitte an den Vertreter des Verantwortlichen gemäß Punkt 1. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Datenverarbeitung wird dadurch nicht berührt.

Wenn wir Daten auf Basis eines berechtigten Interesses/ einer Interessenabwägung verarbeiten, haben Sie als Betroffene/r das Recht, unter Berücksichtigung der Vorgaben von Art. 21 DSGVO der Verarbeitung der personenbezogenen Daten zu widersprechen.

4. Evtl. Empfänger der personenbezogenen Daten (einschließlich des Zwecks der „Übermittlung“, der unter 3. bereits dargestellt ist)

Der technische Betrieb unserer Datenverarbeitungssysteme erfolgt in unserem Auftrag durch

- Microsoft Ireland Operations Ltd., Dublin, Irland, zur Bereitstellung von Onlinediensten, welche für den Betrieb des pädagogischen Netzwerks bzw. des Verwaltungsnetzwerks notwendig sind sowie
- AixConcept GmbH, Stolberg Rhld., zur Bereitstellung, zum Betrieb, zur Wartung und zur Weiterentwicklung des pädagogischen Netzwerks bzw. des Verwaltungsnetzwerks.

Für einzelne Verfahren setzen wir weitere (Unter-) Auftragsverarbeiter ein.

Schulinterne Empfänger (Schulleitung und von der Schulleitung beauftragte Schul-Admins mit Benutzerverwaltungsrechten, Lehrkräfte sowie Schülerinnen und Schüler der eigenen Lerngruppe(n) oder Klasse(n)) nach den konkret zugewiesenen Berechtigungen innerhalb der Schule.

5. Absicht Übermittlung an Drittland oder eine internationale Organisation

Personenbezogene Daten werden in unserem Auftrag verarbeitet von Auftragsverarbeitern, welche die Daten in den Ländern verarbeiten, in denen sie oder ihre Unterauftragsverarbeiter tätig sind. Hauptverarbeitungsstandort ist die Europäische Union. Darüber hinaus übermitteln unser Auftragsverarbeiter Daten auch an Drittländer.

Für Übermittlungen von personenbezogenen Daten an ein Drittland gelten die EU-Standardvertragsklauseln in Verbindung mit zusätzlichen Garantien. Somit unterliegen sie angemessenen Absicherungen, wie sie in Art. 46 DSGVO beschrieben sind. Bitte treten Sie mit uns in Kontakt, falls Sie eine Kopie der abgeschlossenen EU-Standardvertragsklauseln und den zusätzlichen Garantien erhalten möchten.

6. Dauer der Speicherung

Tritt eine Person aus der Schule aus (beispielsweise durch Wegzug oder Ende der Schulzugehörigkeit), wird das zugeordnete Nutzerkonto entfernt und nach einer Karenzzeit von 30 Tagen unwiderruflich gelöscht. Daneben gibt es die Möglichkeit, personenbezogene Daten des Betroffenen auf Anforderung direkt zu löschen, beispielsweise nach Widerruf Ihrer Einwilligung.

7. Rechte der Betroffenen

Sie haben gegenüber uns folgende Rechte hinsichtlich der Sie betreffenden personenbezogenen Daten:

- Recht auf Auskunft (Art. 15 DSGVO),
- Recht auf Berichtigung (Art. 16 DSGVO) bzw. Löschung (Art. 17 DSGVO),
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO) sowie
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO),

Zur Ausübung Ihrer Rechte wenden Sie sich bitte an den Verantwortlichen für die Datenverarbeitung oder seinen Datenschutzbeauftragten. Kontaktdaten finden Sie dazu unter Punkt 1 und 2.

8. Beschwerderecht bei einer Aufsichtsbehörde

Sie haben das Recht, bei einer Datenschutz-Aufsichtsbehörde Beschwerde einzulegen, falls Sie der Auffassung sind, dass eine Verarbeitung Ihrer personenbezogenen Daten gegen Datenschutzrecht verstößt.

9. Pflicht zur Bereitstellung der personenbezogenen Daten

Sie sind nicht verpflichtet, Ihre personenbezogenen Daten für diese Verarbeitung bereitzustellen.

10. Quelle der Daten

Die durch die Verarbeitung verarbeiteten Daten stammen von Ihnen / ihrem Vertreter.

Einwilligung zur Verarbeitung personenbezogener Daten

Ich willige (als Vertreter) der Verarbeitung der personenbezogenen Daten der Schülerin / des Schülers

Vorname / Nachname _____

Klassenbezeichnung _____

zur Einrichtung und Bereitstellung eines pädagogischen Netzwerks auf Basis von MNSpro Cloud (Office365) ein.

Mein Vor- und Nachname sowie meine schulspezifische E-Mail-Adresse (z. B. vorname.nachname@schulname.de) wird dazu schul- und gruppenintern in einem Verzeichnis bereitgestellt, um die Kontaktaufnahme und Kommunikation untereinander zu ermöglichen.

Das pädagogische Netzwerk übermittelt Anzeigenname, Benutzername und (falls Bestandteil dieser genannten Namen) gegebenenfalls auch Vor- und Nachname sowie E-Mail-Adresse an andere Nutzer des pädagogischen Netzwerks. Des Weiteren wird der Online-Status und das Profilbild übermittelt – falls der Betroffene diese Angaben freischaltet. Die Gruppenzugehörigkeit eines Betroffenen übermitteln wir an andere Mitglieder dieser Gruppe.

Die Erteilung der Einwilligung ist freiwillig. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile.

Sie können Ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen.

**Wenden Sie sich dazu bitte an Gemeinschaftsschule Wartbergschule
Niederndodeleben postalisch unter Goethestr. 15, 39167, Niederndodeleben,
telefonisch unter 039204 7690 oder per eMail an**

kontakt@sks-niederndodeleben.bildung-lsa.de

Die oben genannten Informationen gemäß Artikel 12 ff. DSGVO aufgrund der Erhebung von personenbezogenen Daten habe ich zur Kenntnis genommen.

Ort, Datum: _____

Unterschrift der Schülerin/des Schülers

und der Erziehungsberechtigten

Schwellenwertanalyse

zur Bestimmung
der Notwendigkeit einer
Datenschutz-Folgenabschätzung



Rüdiger Schöndube / Rüdiger Schulze
Gemeinschaftsschule
Wartbergsschule, Goethestr. 15,
39167 Niederndodeleben

Inhaltsverzeichnis

1 Grundlegendes zur DSFA

2 Erfordernis der Schwellenwertanalyse

3 Diskurs der Hauptbedrohungen

4 Maßnahmen der Schule

5 weitere Abschätzungsgegenstände

6 Einschätzung des Risikoschweregrades

Grundlegendes zur DSFA

Gemäß dem "Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO", welche von der Datenschutzkonferenz (stand: 17.12.2018) herausgegeben wurde, ist eine DSFA nur dann durchzuführen, wenn aus der Abschätzung (Schwellenwertanalyse) der Risiken von Verarbeitungsvorgängen ein hohes Risiko besteht. Im Fall der Entscheidung gegen eine Durchführung der DSFA ist dies schriftlich zu dokumentieren.

Wann muss eine DSFA durchgeführt werden?

Eine DSFA **muss** immer dann durchgeführt werden, wenn Folgendes erfolgt:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung (auch Profiling) gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten (Systeme zu Leistungsbeurteilung von Schülern, Zeugniserstellung usw.) oder diese in ähnlich erheblicher Weise beeinträchtigen
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (also z.B. Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen oder Gesundheitsdaten)
- systematische Überwachung öffentlich zugänglicher Bereiche, darunter fällt auch der Einsatz von Videobeobachtung oder Videoaufzeichnung

Erfordernis der Schwellenwertanalyse

Im Zuge der Digitalisierung des Bildungssystem hat sich auch die Gemeinschaftsschule Barleben dazu entschieden mithilfe von AIXConcept ihren Schülern und Lehrern ein digitales Lernen zu ermöglichen.

AIXConcept (Office 365) basiert auf Microsoft (Microsoft Corp. USA) dies **ermöglicht die**

Nutzung folgender Tools:

- Microsoft Office 365 (E-Mail: Vor- und Nachname inkl. Domain der Schule)
- Microsoft Teams (E-Mail: Vor- und Nachname inkl. Domain der Schule)
- OneDrive (Online Speicherplatz)
- Online-Nutzung (Word, Excel, PowerPoint etc.) --> Lizenzabhängig
- Installierung von Microsoft Office 365 auf bis zu 5 Privatgeräten

Folgende Funktionalitäten bildet die cloudbasierte IT-Lösung von AIXConcept ab:

- Interaktives Arbeiten und Videokonferenzen (lehrerzentriert)
- Zugriff von Smartphone und Tablet mit Apps
- Effektives Nutzen von Anwendungen im Unterricht
- Material mit Schülern, Klassen und dem Kollegium teilen
- Zugriff vom eigenen Smartphone oder Tablet (nicht gestattet)
- Teilen von Tafelbildern und multimedialen Inhalten
- Verschlüsselung und Speicherung personenbezogener Daten
- Gemeinsame Datennutzung

Diskurs der Hauptbedrohungen

Bedrohungen:

- Interner Abzug von personenbezogenen Daten
- Externer Abzug von personenbezogenen Daten

FISA 702 (EU – US – Datenübertragungen)

Unter FISA 702 ist es US-Sicherheitsbehörden gestattet, auf durch US-Unternehmen verarbeitete Daten, die in den USA gespeichert sind, Zugriff zu nehmen.

Der CLOUD Act stellt fest, dass die Zugangsrechte der US-Sicherheitsbehörden auch dann bestehen, wenn US-Unternehmen Daten außerhalb der USA – zum Beispiel im EWR (Europäischen Wirtschaftsraum) – verarbeiten. Hiermit kann eine US-Sicherheitsbehörde **theoretisch** an jedes US-Unternehmen herantreten und verlangen, die in Europa gespeicherten Daten herauszugeben, also auch ohne, dass diese zuvor in die USA übermittelt wurden.

Schutzmaßnahmen von Microsoft Ltd.

- Verschlüsselung, Papierdokumentensicherheit
- Überwachung der Datenschutzmaßnahmen, Datenminimierung
- Zugangskontrollen, Betriebssicherheit
- Logische Zugriffskontrollen

Diskurs der Hauptbedrohungen

Die gegebenen Schutzmaßnahmen von Microsoft Ltd. wurden extern und intern geprüft und kamen zu folgenden Ergebnissen:

a. Speicherung der ruhenden Daten auf EU-Servern

Die Speicherung der personenbezogenen Daten findet in Rechenzentren statt, die der Europäischen Union betrieben werden. Der Zugriff auf personenbezogene Daten von Drittstaaten aus kann jedoch nicht ausgeschlossen werden.

b. Verschlüsselung

Microsoft nutzt ausreichende Transportverschlüsselung und Verschlüsselung gespeicherter Daten nach dem Stand der Technik.

“Microsoft uses strong encryption protocols to provide barriers against unauthorized access to commercial and public sector Customer Data. Microsoft’s uses of encryption in connection with Online Services include:

Encrypting by default Customer Data (including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers:

Encrypting Customer Data stored at rest in Online Services;

In the case of Online Services on which Customer or a third-party acting on Customer’s behalf may build applications (e.g., certain Azure services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties.

Proper key management is also an essential element of encryption best practices, and Microsoft works to ensure that all Microsoft-managed encryption keys are properly secured. Additionally, Microsoft publishes a variety of information to assist Customers with their own assessments and security practices, available on the Microsoft Trust Center.”

Diskurs der Hauptbedrohungen

c. Kein Vorhandensein von Backdoors

In der Antwort von Microsoft stehen Aussagen zum Nicht-Vorhandensein von Backdoors. Im „Nachtrag zum Datenschutz - Microsoft-Onlinedienste“ Stand 21. Juli 2020 (auf den sich die Antwort von Microsoft bezieht), wird ebenfalls zugesichert, dass Backdoors nicht vorhanden sind:

„Microsoft wird Dritten Folgendes nicht bereitstellen: (a) einen direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf verarbeitete Daten; (b) für die Sicherung der verarbeiteten Daten verwendete Verschlüsselungsschlüssel für die Plattform, oder die Möglichkeit, eine solche Verschlüsselung zu umgehen; oder (c) den Zugang zu verarbeitete Daten, wenn Microsoft bekannt ist, dass diese Daten für andere als die in der betreffenden Anfrage Dritter angegebenen Zwecke verwendet werden sollen.“

d. Zusicherung der Prüfung und Abwehr von Anfragen der US-Behörden

Ebenfalls werden alle Anfragen von US-Behörden geprüft und soweit möglich abgewehrt.

“We would like to emphasize that for many years Microsoft has had in place legal, technical and organizational measures to support its commitments to Customers, including in the SCCs, and to protect Customer Data, Professional Services Data and Personal Data. These measures include:

- Not giving any government direct access to Customer Data, Professional Services Data or Personal Data
- Scrutiny of all government demands for legal validity and appropriateness, with a proven track record of using the courts to challenge government demands that Microsoft believes are inappropriate and do not adhere to our commitments.”

“Microsoft has gone to court five times to challenge the U.S. government over orders it issued seeking access to people’s data or to protect our ability to tell Customers about them, taking one case to the U.S. Supreme Court. Our challenges have led to greater protections and transparency for our Customers, including through a settlement that enabled us to begin disclosing transparency reports about the number of U.S. national security orders we receive and established new policies within the U.S. government limiting the use of secrecy orders.“

Diskurs der Hauptbedrohungen

e. Zusicherung der Information über Behördenanfragen

Microsoft verpflichtet sich, bei Anordnungen zur Herausgabe von Daten durch Behörden den Kunden (d.h. den Verantwortlichen der Datenverarbeitung) unverzüglich zu benachrichtigen bzw. wenn eine solche Benachrichtigung untersagt sein sollte, alle rechtlichen Mittel einzusetzen, um das Verbot anzugreifen und den Kunden sobald als möglich zu informieren.

Darüber hinaus werden nicht personalisiert berichtet, wie viele Anfragen Demnach wurden im zweiten Halbjahr des Jahres 2019 bei einer (!) Anfrage in diesem Zusammenhang sogenannte „content data“ offenbart.

“Supporting its commitments, Microsoft releases a biannual transparency report to the public, including both a law enforcement requests report and a specific report regarding requests from U.S. national security authorities.
U.S. law limits the information Microsoft can relay on this topic, but Microsoft strictly adheres to its commitments for all government demands for Customer Data”.

f. Nachweis durch Audits und Zertifikate

Die Einhaltung datenschutz- und datensicherheitsbezogener Anforderungen wird regelmäßig durch Microsoft und im Auftrag von Microsoft durch Dritte bewertet und dokumentiert:

„Microsoft wird Prüfungen der Sicherheit der Computer, der Computerumgebung und der physischen Rechenzentren, die Microsoft zur Verarbeitung von Kundendaten und personenbezogenen Daten nutzt, wie folgt durchführen:

Sieht eine Norm oder ein Rahmenkonzept Prüfungen vor, so wird mindestens einmal jährlich eine Prüfung dieser Kontrollnorm oder dieses Rahmenkonzepts veranlasst. Jede Prüfung wird entsprechend den Standards und Regeln der Aufsichts- oder Akkreditierungsstellen für die jeweils anwendbaren Kontrollstandards oder Rahmenbestimmungen durchgeführt.

Diskurs der Hauptbedrohungen

g. Art der Zusicherungen (einseitig/ vertraglich)

Die Zusicherungen von Microsoft sind vertraglich und durch ein zweiseitiges Rechtsgeschäft zustande gekommen.

h. Keine Änderung der Standardvertragsklauseln

Es wird von Microsoft zugesichert, dass die SCC nicht verändert wurden:

“The SCC have not been adapted or otherwise changed. However, Microsoft is (i) constantly evaluating the robustness of its services from a customer security perspective and (ii) currently in the process of identifying the potential necessity for implementing additional measures following Schrems II. In this evaluation of potential additional measures, Microsoft will take into account the guidance of data protection authorities and feedback we receive from customers.”

i. Zugriff auf personenbezogene Daten durch Mitarbeiterinnen und Mitarbeiter von Microsoft

„Microsoft employs least privilege access mechanisms to control access to Customer Data (including any Personal Data therein). Role-based access controls are employed to ensure that access to Customer Data required for service operations is for an appropriate purpose, for a limited time, and approved with management oversight.“

j. Schadenersatz bei Offenlegung

Microsoft gewährt im Falle der Offenlegung von Daten auf Anordnung einer Regierungsstelle oder Strafverfolgungsbehörde den betroffenen Personen einen Anspruch auf materiellen wie immateriellen Schadensersatz der aufgrund dieser Offenlegung entstanden ist.

Maßnahmen der Schule

Um die Risiken/Bedrohungen für die Schuler und Schülerinnen sowie des Lehrpersonals so gering wie möglich zu halten, hat die Gemeinschaftsschule Wartbergsschule Niederndodeleben folgende Regelungen getroffen.

Maßnahmen zur Eindämmung der Risikoquellen:

1. Verschlüsselung des internen Schulnetzwerkes
2. konfiguriertes Personenverzeichnis
3. Einwilligungserklärung der Erziehungsberechtigten für die Anmeldevoraussetzungen (Vor- und Nachname des Schüler/-in und der Domain der Schule)
4. keine Speicherung besonderer Kategorien personenbezogener Daten (" Stammdaten")
5. diese werden gesondert in den Schülerakten hinterlegt (Einsehen wird dokumentiert)
6. Handlungsanweisung sowie Belehrung der SuS im privaten Einsatzbereich wird dokumentiert
7. ständige Evaluation des Geschehens, um auf Risiken sofort entgegenzuwirken

weitere Abschätzungsgegenstände

Für die Abschätzung der Risikostufe, ob eine DSFA durchzuführen ist, werden nun weitere Kategorien herangezogen und untersucht.

Abschätzungsgegenstand	Ja	Nein	Bemerkung
Allgemeines			
Handelt die Firma AIXconcept nach den Regelungen der DS-GVO (EU)	X		
Identifizierung des Drittstaatentransfers: Steht der Server außerhalb der EU?		X	
Identifizierung des Drittstaatentransfers: Steht der Server in der EU?	X		<u>Standort:</u> Microsoft Ireland Operations Limited 70 Sir Rogerson's Quay Dublin 2 Irland --> Unterliegen der DS-GVO (EU)
Systematische Bewertung von AIXconcept			
Werden Leistungsbeurteilung damit erhoben?	X		Allgemeine unterrichtsbezogene Sachen (Vorträge, Hausaufgaben etc.) nur eine weitere Möglichkeit Leistungen der SuS zu beurteilen
Werden damit Zeugnisse erstellt?		X	Schulinternes Programm vorhanden, Zugriff nur durch Lehrer

weitere Abschätzungsgegenstände

Abschätzungsgegenstand	Ja	Nein	Bemerkung
Verarbeitung von personenbezogenen Daten			
Religiöse Überzeugung der SuS?		X	
Weltanschauung der SuS?		X	
Gesundheitsstatus der SuS		X	
Vor- und Nachname	X		Anmeldung (Einwilligungserklärung)
Videoüberwachung der SuS?		X	
Videokonferenzen mit den SuS?	X		Erfolgt nur Lehrerzentriert keine Aufzeichnungen von SuS keine Aufzeichnungen vom Unterricht Anwendung der Methode eher selten, außer bei Schulschließung (Lockdown) oder ähnlich gravierenden Situationen
Videokonferenzen mit den SuS durch Microsoft Teams?	X	X	Laut LSA zur Zeit nicht zulässig Bei Änderungen, wird darauf zurückgegriffen Alternative "Big Blue Button"

Einschätzung des Risikoschweregrades

Auf Grundlage der derzeitigen Erkenntnisse aus Gesprächen mit der Firma AIXconcept (Ingo Goblirsch, Steffen Janitza), dem Datenschutzbeauftragten Sachsen-Anhalt Nord (Herr Andreas Merkel) und den uns zugekommen Informationen der Firma Microsoft Ltd. sowie der internen Analyse der Risikoabschätzung kommen wir zu folgendem Ergebnis:

*

Bei der Offenlegung von personenbezogenen Daten ist das Risiko überschaubar, da es sich um keine besonderen Kategorien personenbezogener Daten, hier „Stammdaten“, der Betroffenen handelt. Das Risiko ist jedoch nicht "geringfügig", da es sich um besonders schützenswerte Betroffene handelt, nämlich Minderjährige und abhängig Beschäftigte.

Es bestehen nach Umsetzung der Maßnahmen aus Sicht des Verantwortlichen keine hohe Restrisiken für die Rechte und Freiheiten der Schüler und Schülerin sowie dem Lehrpersonal. Es besteht lediglich ein geringes Zugriffsrisiko von Behörden. Die Restrisiken von allen Betroffenen sind nach ausführlicher Untersuchung als „niedrig“ bis „mittel“ bewertet wurden. Damit ist aus unserer Sichtweise - analog zu den Grundgedanken der DSGVO - eine Datenübermittlung in Drittstaaten auf Basis von EU-Standardvertragsklauseln mit den skizzierten Maßnahmen und genannten zusätzlichen Garantien verhältnismäßig.

Dementsprechend kommen wir zu dem Entschluss, in dieser Schwellenwertanalyse, dass die Bedingungen für eine Durchführung einer Datenschutz-Folgenabschätzung nicht gegeben sind, sofern sich an diesen Regelungen und Gesetzmäßigkeiten nichts ändert. Diese Aussagen wurde nach besten Wissen und Gewissen getroffen.

*

R. Schöndube

Herr Schöndube
(Direktor)

11



R. Schulze

Herr Schulze
(IT- Beauftragter/ Datenschutz)