Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Digitaler Unterricht in Schulen – Der Grundstein ist gelegt

Stand: 26. September 2022

I. Einführung

Durch die letzten beiden Änderungen des Schulgesetzes Nordrhein-Westfalen (SchulG) hat der Landesgesetzgeber in §§ 120, 121 SchulG die datenschutzrechtlichen Voraussetzungen dafür geschaffen, dass die Schulen digitale Systeme im Schulunterricht einsetzen können. In § 120 Abs. 5 und § 121 Abs. Satz 1 SchulG finden sich nunmehr folgende Regelungen:

> **§ 120 Abs. 5 SchulG** (Daten der Schüler*innen und Eltern):
>
> *„[1]Die Schule darf für den Einsatz digitaler Lehr- und Lernmittel personenbezogene Daten der Schülerinnen und Schüler und der Eltern verarbeiten, soweit dies für die Aufgabenerfüllung der Schule erforderlich ist. [2] Dies gilt entsprechend für den Einsatz von Lehr- und Lernsystemen und Arbeits- und Kommunikationsplattformen einschließlich Videokonferenzsystemen (§ 8 Absatz 2); in diesem Rahmen sind die Schülerinnen und Schüler zur Nutzung verpflichtet.“*
>
> **§ 121 Abs. 1 SchulG** (Daten der Lehrkräfte):
>
> *„[1]Daten der Lehrerinnen und Lehrer dürfen von Schulen verarbeitet werden, soweit dies zur Aufgabenerfüllung bei der Planung und Ermittlung des Unterrichtsbedarfs und der Durchführung des Unterrichts, einschließlich des Einsatzes digitaler Lehr- und Lernmittel, [Maßnahmen der Qualitätsentwicklung und der Qualitätssicherung nach § 3 Absatz 4, wissenschaftlichen Untersuchungen nach § 120 Absatz 4, der Schulmitwirkung sowie in dienstrechtlichen, arbeitsrechtlichen oder sozialen Angelegenheiten] erforderlich ist. [2]Dies gilt entsprechend für den Einsatz von Lehr- und Lernsystemen und Arbeits- und Kommunikationsplattformen einschließlich Videokonferenzsystemen (§ 8 Absatz 2); in diesem Rahmen sind die Lehrerinnen und Lehrer zur Nutzung verpflichtet. […]“*

Diese Regelungen geben den Schulen die Möglichkeit, ihren Unterricht in Zukunft über den analogen Präsenzbetrieb hinaus digital zu gestalten. Vorteile wie die hiermit verbundene Flexibilität, Vermeidung von Unterrichtsausfällen sowie die Vorbereitung der Schüler*innen auf ein Leben im digitalen Zeitalter liegen auf der Hand.

Die Schüler*innen sind in der Regel minderjährig und verpflichtet, die Schule zu besuchen. Deshalb hat die Schule eine besondere Verantwortung dafür, dass die Persönlichkeitsrechte der Schüler*innen auch im digitalen Unterricht gewahrt bleiben.

Der dauerhafte Einsatz von Systemen für den digitalen Unterricht sollte den bestmöglichen Ausgleich zwischen Praxistauglichkeit und Gewährleistung eines angemessenen Datenschutzniveaus bieten. Die Einsatzbedingungen sind datenschutzgerecht zu gestalten. Die nachfolgenden Informationen sollen den verantwortlichen Stellen dabei helfen, diese Ziele umzusetzen.

II. Grundsätzliche Fragen

Unabhängig davon, mit welchen Mitteln die Schulen den digitalen Unterricht bestreiten, stellen sich im Hinblick auf den dabei zu beachtenden Datenschutz die folgenden Fragen:

1. Wer ist wofür zuständig? Wer ist für was verantwortlich?

Gemeint ist damit die datenschutzrechtliche Verantwortlichkeit für die Verarbeitung personenbezogener Daten, die im Zusammenhang mit dem Einsatz digitaler Systeme stattfindet. Die datenschutzgerechte Verarbeitung von Daten der Schüler*innen und Lehrer*innen für Zwecke des digitalen Unterrichts haben die verantwortlichen Stellen – vertreten durch ihre jeweiligen Leitungen – sicherzustellen.

a. Verantwortung der Schule/der Schulleitung; Zuständigkeit der schulischen Datenschutzbeauftragten

Schulen der Gemeinden und Gemeindeverbände gelten, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, nach § 5 Abs. 1 Satz 2 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) als (eigenständige) öffentliche Stellen. Die Erfüllung des Bildungs- und Erziehungsauftrags der Schulen ist eine innere Schulangelegenheit. Damit trägt die Schule die datenschutzrechtliche Verantwortung, wenn personenbezogene Daten für den digitalen Unterricht verarbeitet werden.

Für die Schule stellt die jeweilige Schulleitung **durch technische und organisatorische Maßnahmen** sicher, dass der **Schutz der verarbeiteten Daten** gemäß Art. 32 in Verbindung mit Art. 5 Datenschutz-Grundverordnung (DS-GVO) gewährleistet ist (§ 1 Abs. 3 Satz 1 der Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern – VO-DV I, § 1 Abs. 5 der Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer – VO-DV II).

Das bedeutet zugleich, dass nicht jede einzelne Lehrkraft selbst über den Einsatz von Software-Produkten etc. entscheiden kann. Da der Schulleitung die datenschutzrechtliche Verantwortung zukommt, obliegt diese Entscheidung letztlich ihr. Davon unberührt bleibt selbstverständlich die in der Schulwirklichkeit geübte Praxis, in den Schulen konsensfähige Lösungen zuvor abzustimmen und damit auch die Akzeptanz der Entscheidungen zu erhöhen.

Unterstützung erhalten die Schulleitungen von den behördlichen Datenschutzbeauftragten der Schulen. Hierbei gibt es grundsätzlich eine Besonderheit: Nach § 1 Abs. 6 Satz 3 VO-DV II wählen die Schulämter für Schulen in kommunaler und staatlicher Trägerschaft Personen aus, die in ihrem Bezirk die Aufgaben der*des behördlichen Datenschutzbeauftragten wahrnehmen sollen. Diese sind auch für die Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften in Bezug auf die Daten der Schüler*innen und Eltern zuständig (vgl. § 1 Abs. 3 Satz 2 VO-DV I). Die für die einzelnen Schulamtsbezirke zuständigen Datenschutzbeauftragten können über folgenden Link ermittelt werden: https://www.medienberatung.schulministerium.nrw.de/Medienberatung/Datensicherheit-und-Datenschutz/Datenschutzbeauftragte/. Nach § 1 Abs. 6 Satz 5 VO-DV II können die Schulen stattdessen aber auch schuleigene Datenschutzbeauftragte benennen.

b. Zuständigkeit des Schulträgers

Obwohl in der Praxis häufig die Schulträger die Rahmenverträge, beispielsweise in Bezug auf die Nutzung bestimmter Software-Produkte, vereinbaren, ändert dies nichts daran, dass die Schule bzw. ihre Leitung in ihrem Aufgabenbereich – insbesondere der Bildung und Erziehung der Schüler*innen – bei der Nutzung eines bestimmten Produkts für die damit erfolgende Verarbeitung personenbezogener Daten datenschutzrechtlich verantwortlich ist.

Die Abgrenzung der datenschutzrechtlichen Verantwortlichkeit von Schulträger und Schule ist durch die Aufgabenzuweisung im Hinblick auf innere und äußere Schulangelegenheiten vorgegeben. Für die äußeren Schulangelegenheiten trifft § 79 Abs. 1 SchulG folgende Regelung: „Die Schulträger sind verpflichtet, die für einen ordnungsgemäßen Unterricht erforderlichen Schulanlagen, Gebäude, Einrichtungen und Lehrmittel bereitzustellen und zu unterhalten sowie das für die Schulverwaltung notwendige Personal und eine am allgemeinen Stand der Technik und Informationstechnologie orientierte Sachausstattung zur Verfügung zu stellen.“ Soweit die Schulträger im Zusammenhang mit diesen äußeren Schulangelegenheiten personenbezogene Daten verarbeiten, sind sie als datenschutzrechtlich Verantwortliche anzusehen.

Hingegen gelten die Schulen der Gemeinden und Gemeindeverbände, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, wie oben dargestellt, als (eigenständige) öffentliche Stellen, für die die jeweilige Schulleitung durch technische und organisatorische Maßnahmen sicherzustellen hat, dass der Schutz der verarbeiteten Daten gewährleistet ist. Sie ist insofern datenschutzrechtlich Verantwortliche.

c. Verantwortung des Schulministeriums NRW (MSB NRW)

Gemäß § 2 DSG NRW haben die obersten Landesbehörden im Rahmen ihrer **Ressortverantwortung** jeweils für ihren Bereich die Ausführung der Vorschriften über den Datenschutz sicherzustellen. Oberste Landesbehörde für den Schulbereich ist das MSB NRW.

Da nicht jede Schule über die fachlichen Ressourcen verfügt, um datenschutzgerechte Lösungen für den digitalen Unterricht zu entwickeln, stellt das MSB NRW eigene Systeme für den digitalen Unterricht bereit (Näheres hierzu vgl. Ziffer III) und unterstützt die Schulen im Digitalisierungsprozess.

d. Zuständigkeit der Landesbeauftragten für Datenschutz und Informationsfreiheit NRW (LDI NRW)

Die LDI NRW ist bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse eine von der Landesregierung unabhängige Landesbehörde (vgl. Art. 77a Abs. 2 Satz 1 Verfassung für das Land Nordrhein-Westfalen, Art. 52 Abs. 1 DS-GVO, § 25

Abs. 2 Satz 1 DSG NRW). Sie überwacht als Aufsichtsbehörde die Einhaltung der datenschutzrechtlichen Vorschriften bzw. berät und informiert die öffentlichen Stellen in Belangen des Datenschutzes und der Datensicherheit (vgl. Art. 57 Datenschutz-Grundverordnung – DS-GVO, §§ 26, 27 DSG NRW). Darüber hinaus nimmt sie sich insbesondere auch der Beschwerden und Anfragen von Bürger*innen an.

Die Aufsichtsfunktion der LDI NRW umfasst allerdings weder eine Genehmigung noch eine Zertifizierung von Datenverarbeitungsprozessen oder Softwareprodukten. Wir geben den für die konkrete Datenverarbeitung verantwortlichen Schulen nicht die Gestaltung der Datenverarbeitungsprozesse in den Schulen vor. Anders als beispielsweise das Bundesamt für die Sicherheit in der Informationstechnik ist die LDI NRW auch nicht auf ein laufendes Monitoring von Datensicherheitsfragen ausgerichtet.

Unsere Beratungsaufgabe erstreckt sich auf Hinweise, die wir aufgrund des Rechtsrahmens und der technischen Erkenntnisse geben können. Außerdem bearbeiten wir Beschwerden über Datenverarbeitungen im Schulbereich, die jede Person, die sich in ihren Datenschutzrechten verletzt fühlt, bei uns als Datenschutzaufsichtsbehörde einreichen kann (Art. 77 Abs. 1 DS-GVO, § 29 Satz 1 DSG NRW).

2. Welche rechtlichen Rahmenbedingungen sind im Schulbereich zu beachten?

Nach Art. 6 Abs. 1 Satz 1 DS-GVO ist eine Verarbeitung personenbezogener Daten durch öffentliche Stellen vor allem dann rechtmäßig, wenn entweder eine Einwilligung vorliegt oder eine Rechtsgrundlage im nationalen Recht nach Art. 6 Abs. 1 Satz 1 Buchstabe c oder e DS-GVO in Verbindung mit Art. 6 Abs. 3 DS-GVO die Verarbeitung erlaubt. Jeder Datenverarbeitungsschritt muss also auf einer wirksamen Rechtsgrundlage – einer Rechtsvorschrift oder einer Einwilligung – beruhen, weil die Verarbeitung personenbezogener Daten der betroffenen Personen ansonsten unzulässig ist.

a. Rechtsgrundlagen im nationalen Recht

Für die Schulen finden sich Rechtsgrundlagen im nationalen Recht vor allem in §§ 120 f. SchulG (und ggf. den sie konkretisierenden Vorschriften der VO-DV I und der VO-DV II). Sie gehen als bereichsspezifische Rechtsgrundlagen, die spezielle Regelungen für die Verarbeitung der Daten von Schüler*innen, Eltern und Lehrkräften treffen, der allgemeinen (Auffang-) Rechtsgrundlage des § 3 DSG NRW vor. Die allgemeinen Datenschutzregelungen des DSG NRW finden ggf. ergänzend Anwendung (vgl. § 122 Abs. 1 Satz 3 SchulG).

Maßgeblich für den Einsatz digitaler Unterrichtsanwendungen sind die oben wörtlich zitierten § 120 Abs. 5 und § 121 Abs. 1 Satz 1 und 2 SchulG. Danach dürfen Schulen für den Einsatz von digitalen Lehr- und Lernsystemen sowie Arbeitsplattformen personenbezogene Daten der Schüler*innen und der Eltern sowie der Lehrer*innen verarbeiten, soweit dies für ihre Aufgabenerfüllung erforderlich ist.

Schulen müssen immer betrachten, welche Aufgabe sie zu erfüllen haben und welche Datenverarbeitungen dafür erforderlich sind. Schwierigkeiten bereiten in der Regel Anwendungen, die neben den für schulische Zwecke erforderlichen Datenverarbeitungen von den Anbietern voreingestellte Datenverarbeitungen vorsehen, die nicht den schulischen Zwecken dienen. Lassen sich diese Voreinstellungen nicht durch die Schule abstellen, sind diese Anwendungen für den digitalen Unterricht nicht geeignet.

b. Einwilligung

Art. 6 Abs. 1 Satz 1 DS-GVO sieht die Möglichkeit vor, eine Datenverarbeitung (über die Grenzen der gesetzlichen Rechtsgrundlagen hinaus) auch auf eine **Einwilligung** der betroffenen Person zu stützen. **Für Schulen** kann die Einwilligung im Zusammenhang mit dem Unterrichtsgeschehen **regelmäßig keine Rechtsgrundlage** für die Datenverarbeitung bieten. Wesentlich für eine wirksame Einwilligung ist, dass sie freiwillig erteilt wird. Diese Freiwilligkeit ist in aller Regel bei Datenverarbeitungen, die den digitalen Unterricht ermöglichen sollen, nicht gegeben, weil die Schüler*innen am Unterricht teilnehmen müssen und keine freie Wahl haben.

Damit eine Einwilligung wirksam ist, müssen bestimmte Voraussetzungen erfüllt sein (vgl. Art. 4 Nr. 11, Art. 7 DS-GVO, §§ 120 Abs. 2 Satz 3, § 121 Abs. 1 Satz 8 und 9 SchulG, Art. 8 Abs. 1 DS-GVO).

Wie sich aus Erwägungsgrund (EG) 42 DS-GVO ergibt, ist eine Einwilligungserklärung unter anderem nur dann wirksam, wenn die einwilligende Person in geeigneter Weise zuvor über die Bedeutung der Einwilligung **informiert** wurde. Die Stelle muss die betroffene Person über den gesamten Prozess der geplanten Datenverarbeitung und auch über die Person des Verantwortlichen und den Verwendungszweck informieren, für den die Daten verarbeitet werden.

Vor allem muss die Entscheidung für oder gegen die Erteilung der Einwilligung freiwillig sein. Nach EG 42 DS-GVO sollte nur dann davon ausgegangen werden, dass die betroffene Person ihre Einwilligung **freiwillig** gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Um sicherzustellen, dass die Einwilligung freiwillig erfolgt, sollte diese gemäß EG 43 DS-GVO darüber hinaus keine gültige Rechtsgrundlage liefern, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt und deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde.

Aufgrund des durch die Schulpflicht, die Leistungsbewertung oder die Möglichkeit der Sanktionierung nach § 53 SchulG bestehenden Ungleichgewichts zwischen den Protagonist*innen ist gerade im Schulbereich wenig Spielraum für Einwilligungserklärungen, die tatsächlich freiwillig sind und damit geeignete Rechtsgrundlage für eine Verarbeitung personenbezogene Daten sein können. Werden Daten von Schüler*innen im Zusammenhang mit digitalem Unterricht erhoben, ist es den Schüler*innen oder deren Eltern in aller Regel nicht möglich, sich frei und ohne Nachteile für die Schüler*innen gegen die Verarbeitung ihrer Daten zu entscheiden, weil sie ansonsten von der Nutzung der konkreten Anwendung und damit zumindest teilweise vom Unterricht ausgeschlossen wären.

Die vorstehenden Erwägungen gelten regelmäßig auch für Daten von Lehrer*innen, die zur Durchführung des digitalen Unterrichts verarbeitet werden. Hier darf das strukturelle Ungleichgewicht des Dienstverhältnisses keinen Einfluss auf die Freiwilligkeit einer Einwilligung haben. Dabei sind die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Personen sowie die Umstände zu berücksichtigen, unter denen die Einwilligung erteilt worden ist.

Eine Einwilligung kann nur dann eine Rechtsgrundlage für die Datenverarbeitung sein, wenn sich die Betroffenen frei von sozialem Druck oder Zwang für oder gegen die Verarbeitung ihrer personenbezogenen Daten entscheiden können.

3. Welche weiteren Anforderungen müssen erfüllt werden?

Eingesetzte Datenverarbeitungssysteme müssen den **datenschutzrechtlichen Anforderungen insbesondere aus Art. 5, 24, 25 und 32 DS-GVO** genügen. Zum anderen muss die von der Schule verantwortete Datenverarbeitung gemäß dem Wortlaut der §§ 120 Abs. 5, 121 Abs. 1 SchulG durch sie **selbst oder durch einen Auftragsverarbeiter** erfolgen.

a. Technische Sicherheit

Digitale Lehr- und Lernformen, die zu Unterrichtszwecken an den Schulen genutzt werden sollen, müssen zum Schutz der personenbezogenen Daten der Schüler*innen und Lehrer*innen die Anforderungen aus Art. 32 DS-GVO an die Datensicherheit erfüllen. Hiernach haben die Verantwortlichen u.a. unter Berücksichtigung der Umstände und der Zwecke der Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und vor allem die Vertraulichkeit und Integrität der Daten sicherzustellen.

b. Auftragsverarbeitung

Soweit sich die Verantwortlichen bei dem Betrieb digitaler Lehr- und Lernformen externer Dienstleister als Auftragsverarbeiter bedienen, haben sie Art. 28 DS-GVO zu beachten. Charakteristisch für eine Auftragsverarbeitung ist, dass der Auftragsverarbeiter nicht selbst Verantwortlicher für die in Rede stehende Datenverarbeitung, sondern weisungsgebunden gegenüber dem Verantwortlichen ist (vgl. Art. 29 DS-GVO).

Die Verarbeitung durch einen Auftragsverarbeiter wird grundsätzlich dem Verantwortlichen zugerechnet. Es ist ein zuverlässiger Anbieter auszuwählen, der die technisch-organisatorischen Anforderungen der DS-GVO gewährleisten kann (Art. 28 Abs. 1 DS-GVO). Die Schule muss als Verantwortliche für die Datenverarbeitung die Umstände der Auftragsverarbeitung durch vertragliche Regelungen so festlegen, dass personenbezogene Daten nur entsprechend ihrer Weisung sowie ausschließlich für ihre Zwecke (vgl. § 2 Abs. 3 Satz 1 VO-DV I, § 3 Satz 2 VO-DV II) verarbeitet werden und die Vertraulichkeit im Zusammenhang mit der Verarbeitung sichergestellt ist.

c. Datentransfer in Drittstaaten

Einige große Auftragsverarbeiter und Produkthersteller, die Techniken für den digitalen Unterricht anbieten, übermitteln personenbezogene Daten z.B. zu Wartungs- oder Supportzwecken an Drittländer. Das ist nur unter den in Art. 44 ff. DS-GVO festgelegten Voraussetzungen zulässig. Eine solche Übermittlung liegt auch dann vor, wenn der Dienstleister oder dessen Auftragnehmer aus dem Drittland heraus auf in der EU gehaltene Daten zugreift.

Die DS-GVO stellt in ihrem Kapitel V besondere Anforderungen an die Übermittlung personenbezogener Daten in Nicht-EU/EWR-Staaten ohne adäquates Datenschutzniveau bzw. an einen entsprechenden Zugriff aus derartigen Ländern. Selbst wenn die Datenverarbeitung und auch der Einsatz eines Dienstleisters daher grundsätzlich zulässig sein sollte, müssen zusätzlich noch die Voraussetzungen für die Datenübermittlung in Drittstaaten erfüllt sein. Weitere Informationen und Handlungsempfehlungen dazu finden sich unter https://www.ldi.nrw.de/datenschutz/internationaler-datenverkehr/geeignete-garantien/ und zu den bei Bedarf zu ergänzenden Maßnahmen unter https://www.ldi.nrw.de/datenschutz/internationaler-datenverkehr/geeignete-garantien/ergaenzende-massnahmen.

d. Daten der Lehrkräfte

Beim Einsatz digitaler Medien im Unterricht geht es nicht nur um den Schutz der Daten von Schüler*innen. Regelmäßig werden auch die Daten der mittels digitaler Anwendung unterrichtenden Lehrkräfte verarbeitet. Wenn ein genutztes Medium Rück-

schlüsse auf Verhalten oder Leistung der Lehrer*innen zulässt, muss betrachtet werden, wie sich der Einsatz auf das Dienstverhältnis auswirkt. Hier sind die behördlichen Datenschutzbeauftragten und Personalvertretungen einzubeziehen, um den Interessen der Beschäftigten Rechnung zu tragen.

4. Dürfen Lehrkräfte ihre privaten PCs zur Verarbeitung von Daten der Schüler*innen einsetzen, und wie sollen Schüler*innen die Daten digital verarbeiten?

Mit privaten Endgeräten der Lehrer*innen einerseits und auch der Schüler*innen andererseits, sind dauerhafte und tragfähige Lösungen nicht erreichbar, weil Datenschutz und Datensicherheit im gebotenen Maße nur durch Geräte gewährleistet werden können, die von der Schule administriert werden. Ein voller administrativer Zugriff der Schulen auf private Endgeräte scheitert an einem damit verbundenen unzulässigen Eingriff in die Privatsphäre der Eigentümer*innen der Geräte. Für den digitalen Unterricht ist es mittelfristig daher erforderlich, dass sowohl Lehrende als auch Lernende mit schulischen Endgeräten ausgestattet werden.

a. Einsatz privater Endgeräte durch Lehrkräfte

Die LDI NRW hat bereits in ihrem 23. Datenschutz- und Informationsfreiheitsbericht 2017 unter Ziffer 7 (S. 44 ff.) auf die Probleme für den Schutz der Daten der Schüler*innen aufmerksam gemacht, die sich daraus ergeben, dass Lehrkräfte mangels dienstlich zur Verfügung gestellter Geräte ihre eigenen nutzen. Der entsprechende Beitrag kann über den folgenden Link abgerufen werden: https://www.ldi.nrw.de/berichte.

Vor diesem Hintergrund ist es gut, dass das Land verstärkt in die Digitalisierung der Schulen investiert. Mit der Aushändigung eines dienstlichen digitalen Gerätes erlischt eine in der Vergangenheit erteilte Genehmigung für die Verarbeitung personenbezogener Daten von Schüler*innen für dienstliche Zwecke auf privaten Geräten von Lehrkräften nach § 2 Abs. 2 Satz 5 VO-DV I.

Mit Aushändigung persönlicher dienstlicher Geräte ist **grundsätzlich kein Erfordernis mehr** erkennbar, **auf die privaten Geräte zurückzugreifen**. Die in § 2 Abs. 2

Satz 6 VO-DV I eingeräumte vierwöchige Frist dient gerade dazu, dem Risiko zu begegnen, dass die Lehrkräfte unter dem Druck des sofortigen Erlöschens der Genehmigung auf nicht datenschutzgerechte Lösungen für eine Zwischenspeicherung der auf ihren privaten Geräten abgelegten Daten (beispielsweise die Speicherung auf USB-Sticks) zurückgreifen. Hierdurch sollen sie die Möglichkeit haben, die auf den privaten Endgeräten verarbeiteten Daten in datenschutzgerechter Weise auf die dienstlichen Geräte zu übertragen und von den privaten Endgeräten zu löschen.

Die für die Beschaffung der dienstlichen Geräte zuständigen Stellen, in der Regel die Schulträger, müssen dafür Sorge tragen, dass die beschafften Geräte und die zur Verfügung gestellte Software den von den Lehrer*innen benötigten Funktionsumfang und eine angemessene Leistungsfähigkeit aufweisen. Um die unter Ziffer II. 3. genannten Anforderungen zu erfüllen, müssen die Geräte und die Software entsprechend konfiguriert sein und betrieben werden. Hierzu ist ein Betriebskonzept umzusetzen, das insbesondere die regelmäßige Aktualisierung hinsichtlich technischer Sicherheitslücken und die Prüfung der datenschutzfreundlichen Konfiguration der Endgeräte umfasst.

§ 2 Abs. 2 Satz 7 VO-DV I bietet den Schulleitungen die Möglichkeit, in begründeten Einzelfällen unter den dort genannten Voraussetzungen - für die mit dem digitalen dienstlichen Gerät nicht möglichen Nutzungen - **ausnahmsweise** die **vorübergehende Nutzung von Privatgeräten** zuzulassen. Neben dem in § 2 Abs. 2 Satz 2 VO-DV I vorgesehenen technischen Zugangsschutz sind organisatorische Maßnahmen zu ergreifen, um ein angemessenes Schutzniveau im Sinne von Art. 32 DS-GVO zu gewährleisten. Hierzu gehört u.a., dass für den Schulbetrieb genutzte private digitale Geräte der Lehrkräfte für die Dauer des Einsatzes keinen Dritten, einschließlich Haushaltsangehörigen, zur Verfügung stehen dürfen, das Sicherheitsniveau der Geräte u.a. durch aktuelle Updates und den Einsatz von Software nur aus vertrauenswürdigen Quellen auf einem vertretbaren Niveau ist und ein Speichern personenbezogener Daten auf den Geräten möglichst vermieden wird. Weiterhin sollten grundsätzlich nur digitale Geräte genutzt werden, auf denen ein separates Benutzerkonto eingerichtet werden kann, so dass die private und dienstliche Nutzung des Geräts weitgehend getrennt stattfindet. Darüber hinaus sind die Einschränkungen der

Anlage 3 zur VO-DV I zu beachten, die u.a. Regelungen zur Verarbeitung zeugnisrelevanter Leistungsangaben, von Aussagen zum Arbeits- und Sozialverhalten, der Angabe von Fehlzeiten oder Zeugnisbemerkungen auf privaten digitalen Geräten enthalten.

b. Ausstattung der Schüler*innen mit digitalen Geräten

Auch die Ausstattung von Schüler*innen mit schulischen Endgeräten, die die Sicherstellung eines angemessenen Datenschutzniveaus mit Hilfe technischer Maßnahmen ermöglicht, wurde durch die Corona-Pandemie deutlich vorangetrieben.

Häufig wird für die Verwaltung und Aktualisierung von schulischen Endgeräten ein Mobile Device Management eingesetzt. Dieses bietet den Schulen auch die technische Möglichkeit, die Endgeräte hinsichtlich ihrer Nutzung zu überwachen, d.h. beispielsweise den Bildschirminhalt live zu verfolgen oder aus der Ferne Screenshots zu machen.

Soweit dies zur Wahrnehmung ihres Bildungs- und Erziehungsauftrags erforderlich ist, kann eine Einsichtnahme der Lehrer*innen in die Bildschirme der Schüler*innen ebenso wie die Fertigung von Screenshots mit Hilfe eines **Mobile Device Managements,** beispielsweise zum Nachweis einer unzulässigen Nutzung des Geräts im Unterricht, nach § 120 Abs. 5 SchulG gerechtfertigt sein. Dabei muss die Schule sicherstellen, dass die Betroffenen zuvor über die möglichen Maßnahmen und die dabei erfolgende Verarbeitung ihrer personenbezogenen Daten informiert werden.

Was in einem Mobile Device Management möglich ist oder wie Rechte konkret vergeben werden können, hängt vom jeweiligen Produkt ab. Für den Einsatz in Schulen sind nur solche Mobile Device Managements geeignet, in denen Rollen mit bestimmten Rechten festgelegt werden können. Über diesen Mechanismus sollten die den Lehrer*innen zur Verfügung stehenden Möglichkeiten auf das für die Aufgabenwahrnehmung der Schule erforderliche Maß beschränkt sein.

Der **Einsatz privater Endgeräte** der Schüler*innen kann bereits unter dem Aspekt sozialer Teilhabe und Chancengleichheit nicht verpflichtend erfolgen. Sofern über-

gangsweise auch private Endgeräte eingesetzt werden, muss die Schule sicherstellen, dass diese regelmäßig mit Sicherheitsupdates versorgt und zumindest die Sicherheitshinweise des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für mobile, internetfähige Geräte berücksichtigt werden:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basisschutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/schutz-fuer-mobilgeraete_node.html

Dauerhafte und tragfähige Lösungen sind allerdings nur durch die Ausstattung mit schulischen Endgeräten möglich, die verpflichtende Regelungen erlauben.

III. Systeme für den digitalen Unterricht an Schulen

Um den Schulunterricht digital zu gestalten, greifen die Schulen vor allem auf digitale Lehr- und Lernsysteme/ Arbeitsplattformen, Videokonferenz- und Messengerdienste zurück.

1. Digitale Lehr- und Lernsysteme/ Arbeitsplattformen

Neben eigentlichen Lehr- und Lernsystemen werden an Schulen häufig Arbeitsplattformen für den digitalen Informationsaustausch genutzt.

a. Rechtlicher Rahmen

Wie zu Beginn erläutert, dürfen die Schulen nur die Datenverarbeitungen durchführen, die für die schulischen Zwecke erforderlich sind. Als ein Beispiel sei die Protokollierung der Systemzugriffe genannt. Diese ist erforderlich, um die Sicherheit der für schulische Zwecke eingesetzten Systeme zu gewährleisten. Nicht erforderlich und damit unzulässig ist dagegen, dass Lehrkräfte Zugriff auf die Protokolldaten erhalten, um feststellen zu können, wann und wie lange die Schüler*innen die Systeme genutzt haben. Diese Feststellung ist von dem von ihnen wahrzunehmenden Bildungs- und Erziehungsauftrag nicht erfasst. Für die Leistungsbewertung kommt es allein auf die fristgerechte Erledigung einer gestellten Aufgabe an.

Alle von der Datenverarbeitung betroffenen Personen müssen zudem vorab darüber informiert werden, ob die Nutzung der eingesetzten Produkte an der Schule verpflichtend oder freiwillig erfolgt. Ausführungen zur Wirksamkeit von Einwilligungen finden sich unter Ziffer II.2 b.

Die Schulen dürften im Hinblick auf ihren Bildungsauftrag ein nachvollziehbares Interesse an einer verpflichtenden Nutzung haben. Diese ist aber nur mit schulischen Geräten und im Umfang des datenschutzrechtlich Zulässigen (siehe dazu II.2, 3 und 4) möglich.

b. Einzelne Produkte

Wie unter Ziffer II.1.d bereits angesprochen, zertifiziert die LDI NRW keine Softwareprodukte oder Datenverarbeitungsprogramme. Ob ein Produkt datenschutzkonform eingesetzt werden kann, muss die Schule prüfen, die das Produkt nutzen will. Zweifellos ist ein dem Stand der Technik entsprechender Betrieb eines Lehr- und Lernsystems, das auch den Anforderungen des Art. 32 DS-GVO genügt, mit hohem Aufwand verbunden. Schulen die das nicht leisten können, sollten die Angebote nutzen, die das MSB NRW bereithält.

Das MSB NRW stellt allen öffentlichen Schule und Ersatzschulen die digitale Lernplattform **LOGINEO NRW LMS** kostenlos zur Verfügung. Laut den auf seiner Homepage zu findenden Informationen soll das Lernmanagementsystem LOGINEO NRW LMS Unterricht auf Distanz erleichtern und dazu beitragen, Lehr-Lern-Prozesse digital zu unterstützen, sei es in Phasen des Lernens auf Distanz wie anlässlich der Corona-Pandemie oder im Rahmen des Präsenzunterrichts. Schulen könnten ihren kostenfreien Zugang zu LOGINEO NRW LMS auch unabhängig von der Schulplattform LOGINEO NRW beantragen. Das Angebot von LOGINEO NRW werde fortlaufend weiterentwickelt und ergänzt. Nähere Informationen finden Sie unter dem folgenden Link: https://www.schulministerium.nrw.de/lehrkraefte/schule-nrw-amtsblatt/schulpoltik-aktuell-logineo-nrw-lms-das-lernmanagementsystem-fuer.

2. Videokonferenztools

Für den Distanzunterricht sind Videokonferenztools ein verbreitetes Mittel.

a. Verantwortungsbereich der Schulen

Seit Inkrafttreten des neuen Telekommunikationsgesetzes (TKG) und Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) am 1. Dezember 2021 sind in der Regel gegen Entgelt erbrachte Videokonferenzsysteme grundsätzlich als **Telekommunikationsdienste** zu qualifizieren. Dies hat Auswirkungen auf die Verantwortlichkeit der Schulen.

Für die Verarbeitung der bei der Nutzung von Telekommunikationsdiensten anfallenden **Metadaten** (hierzu gehören z.B. IP-Adressen, die übertragene Datenmenge, der Browsertyp, das Betriebssystem und Informationen darüber, wer wann mit wem kommuniziert) sind nicht die Schulen selbst verantwortlich, sondern die Anbieter der Telekommunikationsdienste. Dasselbe gilt für die technischen Übertragungsdaten, d.h. den Transport der Inhaltsdaten (Fernmeldegeheimnis). Die Telekommunikationsdienste unterliegen – soweit sie geschäftsmäßig erbracht werden – nach § 29 Abs. 1 TTDSG der aufsichtsbehördlichen Zuständigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI).

Die Schulen sind aber nach wie vor für die in ihrem Einflussbereich stattfindende Verarbeitung personenbezogener Daten verantwortlich. Ihre Verantwortung erstreckt sich auf die Verarbeitung personenbezogener Daten im Zusammenhang mit der **Herstellung der Kommunikation** (beispielsweise Verwendung von E-Mail-Adressen zur Übersendung des Besprechungslinks), die **Inhaltsdaten** an sich (also z. B., welche Inhalte zum Gegenstand der Videokonferenzen und der im Rahmen der Videokonferenzen stattfindenden Chats gemacht werden und wie damit umgegangen wird, z. B. ob sie gespeichert oder anderweitig verarbeitet werden) sowie auf die **datenschutzfreundlichen Voreinstellungen**. Dabei unterliegen sie in NRW meiner Datenschutzkontrolle. Sie sollten bereits bei der **Auswahl des Videokonferenzdienstes** darauf achten, dass Inhalte angemessen verschlüsselt sind und ein Löschkonzept vorliegt.

b. Rechtlicher Rahmen

Die o.g. Regelungen in §§ 120 Abs. 5, 121 Abs. 1 Satz 1 und 2 SchulG erlauben den Schulen für den Einsatz von Videokonferenzsystemen (§ 8 Absatz 2 SchulG) personenbezogene Daten der Schüler*innen und der Eltern sowie der Lehrer*innen zu verarbeiten, soweit dies für ihre Aufgabenerfüllung erforderlich ist.

c. Verarbeitung von Inhaltsdaten

Die Verarbeitung von Bild- und Tondaten ist nur so weit zulässig, als sie für schulische Zwecke erforderlich ist.

Dieser Maßstab gilt sowohl für die Frage, ob eine Videokonferenz zulässig ist, als auch für die, wie sie konkret durchzuführen ist. Eine Nutzung der Videokonferenzsysteme im häuslichen Umfeld ist unter verschiedenen Aspekten besonders datenschutzrelevant. Sie kann einen Einblick in die Privatsphäre der Teilnehmenden (Wohn- und Familienverhältnisse) ermöglichen. Da dieser für die Aufgabenwahrnehmung der Schule nicht erforderlich ist, ist er so weit wie möglich zu beschränken. Anders als in einer „normalen“ Unterrichtssituation gibt die Nutzung von Videokonferenzsystemen im häuslichen Umfeld auch Familienangehörigen oder sonstigen Dritten die Möglichkeit, vom Unterrichtsgeschehen Kenntnis zu nehmen. Auch dies ist im Rahmen des zu Unterrichtszwecken erfolgenden Videokonferenzaustauschs grundsätzlich nicht zulässig. Die Schulleitungen sind im Rahmen ihrer datenschutzrechtlichen Verantwortung gefordert, Eltern, Schüler*innen und Lehrkräfte entsprechend zu sensibilisieren, über mögliche Datenschutzeinstellungen und –funktionen (s. hierzu auch Ziffer III.2.d – Datenschutzgerechte Voreinstellungen) zu informieren sowie Nutzungsregeln festzulegen und auf ihre Einhaltung hinzuwirken.

In Bezug auf die Erforderlichkeit der Verarbeitung von Inhaltsdaten sind darüber hinaus die Aufzeichnung von Bild- und Tondaten sowie die Verpflichtung, die Kamera einzuschalten, von besonderem Interesse.

i. Keine Aufzeichnung von Bild- und Tondaten

Sollen dauerhafte Bild- und Tonaufzeichnungen vom Unterricht erfolgen, bedarf es hierzu gemäß § 120 Abs. 6 SchulG (in Bezug auf die Daten der Schüler*innen) bzw.

§ 121 Abs. 1 Satz 3 SchulG (in Bezug auf die Daten der Lehrer*innen) der Einwilligung der betroffenen Personen (zur Wirksamkeit von Einwilligungen im Zusammenhang mit dem eigentlichen Unterrichtsgeschehen s. Ziffer II.2 b). Ohne Einwilligung aller Betroffenen dürfen die Teilnehmenden den Inhalt des per Videokonferenz stattfindenden Unterrichts nicht aufzeichnen. Auch insoweit hat die Schulleitung geeignete technische und/oder organisatorische Maßnahmen zu treffen.

Dauerhafte „Bild- und Tonaufzeichnungen des Unterrichts“ im Sinne dieser Vorschriften stellen eine spezielle Form der Datenverarbeitung dar. Hiervon zu unterscheiden ist die bei der Durchführung einer Videokonferenz stattfindende Verarbeitung von Bild- und Tondaten. Bei deren digitaler Übertragung ist zwar eine äußerst vorübergehende Zwischenspeicherung üblich und in den meisten Fällen auch technisch erforderlich, um den digitalen Dienst überhaupt bereit zu stellen. Sie können jedoch zu einem späteren Zeitpunkt nicht mehr wiedergegeben werden. Diese Verarbeitung liegt in der Verantwortung des Videodienstanbieters. Hierauf erstreckt sich die schulische Verantwortung für die Datenverarbeitung nicht.

ii. Verpflichtung, die Kamera einzuschalten

Die Schule muss entscheiden, inwieweit sie Schüler*innen und Lehrer*innen dazu verpflichtet, während des per Videokonferenz stattfindenden Unterrichts die Kamera einzuschalten. In datenschutzrechtlicher Hinsicht hat sie dabei zu berücksichtigen, ob die mit dem permanenten Einschalten der Kamera verbundene Verarbeitung von Bilddaten für den von ihr zu erfüllenden gesetzlichen Bildungs- und Erziehungsauftrag erforderlich ist und ob bzw. inwieweit hiervon Ausnahmen zugelassen werden können. Über eventuell berechtigte Ausnahmen in Einzelfällen sollten sich Lehrkräfte, Schüler*innen und Eltern gegebenenfalls miteinander verständigen.

iii. Livestreams des Präsenzunterrichts/ sog. Hybridunterricht

Nicht nur pandemiebedingt kann es vorkommen, dass nicht alle Schüler*innen am Präsenzunterricht teilnehmen können. Wie dem Begründungstext zum 16. Schulrechtsänderungsgesetz zu § 120 zu entnehmen ist, sollen die Neuregelungen in § 120 Abs. 5 Satz 2 und § 121 Abs. 1 Satz 2 SchulG nicht nur einen für alle Beteiligten mittels Videokonferenz durchgeführten Unterricht umfassen. Nach dem Willen des

Gesetzgebers sollte vielmehr auch die Möglichkeit geschaffen werden, „Schüler*innen, die nicht am Präsenzunterricht teilnehmen können (z.B. Quarantäne, Wechsel von Präsenz- und Distanzphasen, Krankheit etc.), zum Unterricht vor Ort „zuzuschalten“ und somit am Unterricht teilhaben zu lassen“. In diesen Fällen hat die Schule im Rahmen ihrer Aufgabenerfüllung zu entscheiden, ob dabei eine Videoübertragung des stattfindenden Präsenzunterrichts an die Schüler*innen, die nicht hieran teilnehmen können, oder sog. Hybridunterricht für den von den Schulen zu erfüllenden gesetzlichen Bildungs- und Erziehungsauftrag erforderlich ist und inwieweit hiervon Gebrauch gemacht wird. Beim sog. Hybridunterricht befindet sich eine Gruppe im Präsenzunterricht in der Schule, während die zweite Gruppe per Videokonferenz aktiv am Unterricht teilnimmt. Charakteristisch für Videokonferenzen an sich ist die bidirektionale Kommunikation, d.h. der Austausch zwischen „Sender“ und „Empfänger(n)“, sowie das Bewusstsein, Teil einer Kommunikation zu sein. Dies ist bei einem Livestream, d.h. einer reinen Videoübertragung, bei der die Schüler*innen und die Lehrkraft, die sich im Präsenzunterricht befinden, nur Objekt einer audio(-visuellen) Beobachtung sind, anders als auch beim sog. Hybridunterricht nicht der Fall.

iv. Einsatz sog. Telepräsenzroboter

Sog. Telepräsenzroboter eröffnen Schüler*innen, die aufgrund einer Langzeiterkrankung nicht regelmäßig am Präsenzunterricht teilnehmen können, die Möglichkeit, sich zum Unterricht „zuzuschalten“. Die Geräte werden im Klassenzimmer auf dem Platz des*der betroffenen Schüler*in aufgestellt. Sie haben eine eingebaute Kamera und ein Mikrofon, um per Live-Stream den Präsenzunterricht zu übertragen. Über eine App und ein Tablet oder ein großes Smartphone steuert der*die Schüler*in den sog. Telepräsenzroboter, dreht seinen Kopf, sieht den Stream und hört, was um das Gerät herum geschieht. Über eine Leuchtfunktion am Gerät ist erkennbar, ob der*die betroffene Schüler*in verbunden bzw. online ist.

Die Einsatzbedingungen sog. Telepräsenzroboter entsprechen damit grundsätzlich denen eines Videokonferenzsystems. Sie unterfallen damit dem Anwendungsbereich der §§ 120 Abs. 5, 121 Abs. 1 SchulG. Die Schule hat im Rahmen ihrer Aufgabenerfüllung zu entscheiden, ob ihr Einsatz für den von ihr zu erfüllenden gesetzlichen Bil-

dungs- und Erziehungsauftrag erforderlich ist und inwieweit hiervon Gebrauch gemacht wird. Dabei sind in jedem Fall auch die gesundheitlichen Belange des*der betroffenen erkrankten Schüler*in in den Blick zu nehmen.

Anders als bei einer reinen Videoübertragung des Unterrichts sind die Schüler*innen und die Lehrkraft, die sich im Präsenzunterricht befinden, beim Einsatz sog. Telepräsenzroboter nicht nur Objekt einer audio(-visuellen) Beobachtung. Dadurch, dass die Nutzer*innen ebenfalls die Möglichkeit haben, sich mit ihrer Stimme am Unterricht zu beteiligen, ist bidirektionale Kommunikation wie bei einer Videokonferenz möglich. Zwar ist beim Einsatz sog. Telepräsenzroboter nicht vorgesehen, dass Bilddaten der Nutzer*innen an die Schüler*innen und die Lehrkraft im Präsenzunterricht übertragen werden, was angesichts der speziellen Situation, in der sich die Nutzer*innen befinden (Langzeiterkrankung) nachvollziehbar ist. Durch die vorgesehene Leuchtfunktion ist für die Anwesenden im Präsenzunterricht dennoch erkennbar, ob das Gerät aktiv ist und die Nutzer*innen online sind oder nicht. Hierdurch ist sichergestellt, dass den Schüler*innen und der Lehrkraft bewusst ist, wann das Gerät aktiv ist und sie Teil einer Kommunikation sind. Auch in Bezug auf die Möglichkeit der Nutzer*innen, das Gerät zu steuern, d.h. seinen Kopf zu drehen, ist die Vergleichbarkeit mit dem Einsatz eines Videokonferenzsystems gegeben. Während die Teilnehmenden – im Fall der Verpflichtung, die Kamerafunktion zu aktivieren – dort alle im Bild zu sehen sind, haben die Nutzer*innen hier nur die Möglichkeit, sich auszusuchen, wohin sie die Kamera des auf ihrem Platz aufgestellten Geräts steuern. Sofern dies in Einzelfällen zu einer Belastung für Mitschüler*innen (beispielsweise Sitznachbar*innen) führen sollte, haben die Lehrkräfte die Möglichkeit, – wie im Präsenzunterricht – ausgleichend einzugreifen und den sog. Telepräsenzroboter an anderer Stelle zu positionieren.

Im Übrigen gelten die vorstehenden Ausführungen zur Verarbeitung von Inhaltsdaten (insbesondere in Bezug auf die Grenzen der Bild- und Tonübertragung sowie Bild- und Tonaufzeichnungen). Um zu verhindern, dass unbefugte Dritte Zugriff auf den Audio-/Videostream erhalten oder die Steuerung des Gerätes übernehmen, muss die Schule auch für eine ausreichende Sicherheit bei dem von den betroffenen Schüler*innen eingesetzten mobilen Endgeräten (Tablet, Smartphone) sorgen. Idealerweise sollten die betroffenen Schüler*innen auch hier von der Schule bereitgestellte

und verwaltete Endgeräte nutzen, die verpflichtende Regelungen erlauben. Hierauf lässt sich die Umsetzung der erforderlichen Sicherheitsmaßnahmen am effektivsten sicherstellen.

v. Exkurs: Elternsprechtag per Videokonferenz

Soweit die Schulen Videokonferenztools für den Elternsprechtag einsetzen möchten, ist die hierbei stattfindende Verarbeitung personenbezogener Daten der Eltern nur auf der Basis ihrer wirksamen Einwilligungen zulässig.

Zwar erlaubt § 120 Abs. 5 Satz 1 i.V.m. Satz 2 SchulG den Schulen für den Einsatz von Videokonferenzsystemen (§ 8 Abs. 2 SchulG) auch, personenbezogene Daten der Eltern zu verarbeiten, soweit dies für ihre Aufgabenerfüllung erforderlich ist. § 8 Abs. 2 SchulG erlaubt den Schulen zur Erfüllung des Bildungs- und Erziehungsauftrags bereitgestellte Arbeits- und Kommunikationsplattformen in digitaler Form zu nutzen. Auch wenn die Regelungen in § 8 SchulG im Übrigen nur den Unterricht betreffen, ist dem Begründungstext zum 16. Schulrechtsänderungsgesetz zu § 8 SchulG zu entnehmen, dass § 8 Abs. 2 SchulG nicht nur eine ausdrückliche Rechtsgrundlage für die Nutzung von digitalen Lehr- und Lernsystemen etc. für pädagogisch-didaktische Zwecke, sondern auch für schulinterne Verwaltungstätigkeiten sowie interne und externe Kommunikationsprozesse schaffen soll. Allerdings sind nach § 120 Abs. 5 Satz 2, 2. Halbsatz SchulG in diesem Rahmen nur Schüler*innen zur Nutzung verpflichtet. Für die Eltern kommt lediglich eine freiwillige Nutzung in Betracht, so dass die in diesem Zusammenhang stattfindende Verarbeitung personenbezogener Daten eine Einwilligung erfordert.

Da die Einwilligungen in den hier in Rede stehenden Fällen nicht in unmittelbarem Zusammenhang mit dem eigentlichen Unterrichtsgeschehen stehen und sofern die Eltern bzw. volljährigen Schüler*innen alternativ die Möglichkeit haben, mit den betroffenen Lehrkräften auf andere Weise ein Gespräch durchzuführen (beispielsweise telefonisch oder in Präsenz), bestehen keine Bedenken gegen die Freiwilligkeit der Entscheidung.

d. Datenschutzfreundliche Voreinstellungen

Videokonferenzsysteme sollten grundsätzlich so konfiguriert sein, dass Funktionalitäten zur Aufzeichnung von Bild- und Tondaten deaktiviert sind und zusätzlich zu einer obligatorischen Transportverschlüsselung eine Ende-zu-Ende-Verschlüsselung zwischen den Teilnehmenden erfolgt, so dass auf dem Server nur verschlüsselte Daten verarbeitet werden. Weiterhin sollten die Kamera, das Mikrofon und das Teilen des Bildschirms von Teilnehmenden vor Eintritt in die Konferenz standardmäßig ausgeschaltet sein und nur von den Teilnehmenden selbst aktiviert werden können.

Die Teilnehmenden sollten zudem vor der Durchführung von Videokonferenzen über ihrerseits mögliche Datenschutzeinstellungen und -funktionen informiert werden. Hierzu zählt beispielsweise das Einblenden eines virtuellen Hintergrunds, sofern dies vom eingesetzten System unterstützt wird. Weitere Beispiele für Datenschutzeinstellungen und -funktionen sind:

- **Aufmerksamkeitsanzeige**
  Einige Videokonferenzlösungen bieten Aufmerksamkeitsanzeigen an, die es ermöglichen sollen, zu erkennen, ob Teilnehmende der Videokonferenz folgen. Diese Überwachung ist ein Eingriff in die Persönlichkeitsrechte der Teilnehmenden. Wir empfehlen Schulen, diese Funktion zu deaktivieren.
- **Integration sozialer Medien**
  Bei der Einbindung von Social-Media-Inhalten durch Schulen ist Vorsicht geboten. Werden beispielsweise Inhalte von Plattformen eingebunden, bei denen die Übertragung der Nutzungsdaten der Schüler*innen in ein Drittland außerhalb der EU nicht ausgeschlossen werden kann, kann dies gegen geltendes Datenschutzrecht verstoßen und sollten die Schüler*innen nicht verpflichtet sein oder sich verpflichtet fühlen, die entsprechenden Links selbst zu öffnen. Denkbar ist jedoch z. B. die Einbindung von Social-Media-Inhalten im Rahmen der Präsentation einer Lehrkraft über das schulische Internet.
- **Passwortschutz/Anklopfen**
  Wenn die Videokonferenzlösung die Möglichkeit bietet, einen Konferenzraum zu sperren und eine Teilnahme erst nach einer Eingabe eines Passworts bzw. nach einem „Anklopfen“ (auch: Warteraum) und der Freigabe der Teilnahme

durch die Moderation zu erlauben, sollte diese Funktion genutzt werden, um sicherzustellen, dass nur berechtigte Personen an der Videokonferenz teilnehmen.

- Um die Transparenz der Datenverarbeitung in ihrer Videokonferenz zu gewährleisten bzw. die Teilnehmenden über die Verwendung ihrer Daten zu informieren, sollte den Teilnehmenden an der Videokonferenz die datenschutzfreundliche Verwendung der Funktionen vor Beginn der Videokonferenz erläutert oder die Chatfunktion genutzt werden, um die datenschutzrelevanten Informationen bereitzustellen.
- Vorbereitung auf mögliche Datenschutzprobleme, die im Laufe der Videokonferenz auftreten können, beispielsweise:
    - falls die Videokonferenz nicht durch ein Passwort o. ä. geschützt ist, schnelle Reaktion darauf, dass eine unberechtigte Person an der Konferenz teilnimmt,
    - schnelle Reaktion darauf, dass einzelne Teilnehmende unerlaubt personenbezogene Daten verwenden oder veröffentlichen.

e. Auswahl von Videokonferenzdiensten/ Einzelne Produkte

Soweit die Betreiber der Telekommunikationsdienste nach § 29 Abs. 1 TTDSG in die aufsichtsbehördliche Zuständigkeit des BfDI fallen, ist dieser für die datenschutzrechtliche Prüfung einzelner Systeme zuständig.

Wenn datenschutzrechtliche Probleme in Bezug auf einen Videokonferenzdienst allgemein bekannt sind, sollten die Schulen gerade als öffentliche Stellen dies nach Art. 5, 24, 25 und 32 DS-GVO im Rahmen der Auswahl der in ihrem Verantwortungsbereich eingesetzten Videokonferenzdienste berücksichtigen und gegebenenfalls auf ihren Einsatz verzichten.

Nicht in die Zuständigkeit des BfDI fallen von den Schulen oder den Gebietsrechenzentren im Auftrag der Schulen selbst betriebene Videokonferenzdienste (wie beispielsweise Jitsi oder BigBlueButton), die ausschließlich in ihrem Zuständigkeitsbereich eingesetzt und nicht Dritten zur Nutzung angeboten werden. Zwar sind die Be-

treiber dieser Dienste Telekommunikationsdiensteanbieter, die den spezifischen Regeln des TKG und des TTDSG unterworfen und damit insbesondere verantwortlich für die Verarbeitung der im Rahmen der Videokonferenz anfallenden Metadaten sind. Als nicht geschäftsmäßig erbrachte Telekommunikationsdienste unterliegen sie jedoch der Datenschutzaufsicht der LDI NRW.

Wie der unter dem folgenden Link zu findenden Pressemitteilung des MSB NRW vom 21. Januar 2021 zu entnehmen ist, stellt das Land NRW allen öffentlichen sowie den privaten Ersatzschulen für die Organisation und Gestaltung des Distanzunterrichts **ein in den LOGINEO NRW Messenger integriertes Videokonferenztool** kostenfrei zur Verfügung: https://www.land.nrw/de/pressemitteilung/ministerin-gebauer-wir-unterstuetzen-die-lehrkraefte-mit-einem-wichtigen-update

3. Messengerdienste

Die Neuregelungen in § 120 Abs. 5 und § 121 Abs. 1 SchulG ermöglichen den Schulen auch die mit dem Einsatz von Messengerdiensten – als Kommunikationsplattformen – verbundene Datenverarbeitung.

Bei Messengerdiensten handelt es sich um Telekommunikationsdienste. Wie unter Ziffer III.2.a dargestellt, sind für die Verarbeitung der bei der Nutzung von Telekommunikationsdiensten anfallenden **Metadaten** (hierzu gehören z.B. IP-Adressen, die übertragene Datenmenge, der Browsertyp, das Betriebssystem und Informationen darüber, wer wann mit wem kommuniziert) nicht die Schulen, sondern die Betreiber der Telekommunikationsdienste verantwortlich. Dasselbe gilt für die technischen Übertragungsdaten, d.h. den Transport der Inhaltsdaten (Fernmeldegeheimnis).

Die Telekommunikationsdienste fallen nach § 29 Abs. 1 TTDSG grundsätzlich in die aufsichtsbehördliche Zuständigkeit des BfDI.

Die Schulen sind für die in ihrem Einflussbereich stattfindende Verarbeitung personenbezogener Daten zuständig. Ihre Verantwortung erstreckt sich auf die für die **Herstellung der Kommunikation** benötigten Daten, die **Inhaltsdaten an sich (als die**

Inhalte der Kommunikation) sowie auf die **datenschutzfreundlichen Voreinstellungen**. Sie sollten bereits bei der **Auswahl des Messengerdienstes** darauf achten, dass die Inhalte angemessen verschlüsselt sind und ein Löschkonzept vorliegt.

Messengerdienste, die im Zusammenhang mit der Herstellung der Kommunikation Daten verarbeiten, die für die Erbringung der Telekommunikationsleistung nicht erforderlich sind, sind für den Einsatz in Schulen nicht geeignet. Ein Beispiel hierfür ist die im Zusammenhang mit der Anmeldung bei einem Messengerdienst vorgesehene **Übermittlung von Daten unbeteiligter Dritter im Rahmen des Adressbuchabgleichs**.

Dabei wird, nachdem sich die Nutzer*innen mit ihrer Mobilfunknummer registriert haben, regelmäßig ihr Adressbuch ausgelesen, und es werden mindestens die von den Nutzer*innen gespeicherten Namen und Mobilfunknummern an die Server des Messengerdienstes übermittelt. Dieser Adressbuchabgleich wird unter anderem dazu genutzt, den Nutzer*innen anzuzeigen, welche ihrer Kontakte ebenfalls diesen Messengerdienst nutzen. Hierbei werden immer auch die Daten von Personen an den Messengerdienst übermittelt, die diesen nicht nutzen.

Über die Nutzung für rein private oder familiäre Zwecke hinaus sind, mangels einer gesetzlichen Erlaubnis für die Weitergabe der Daten, grundsätzlich die Einwilligungen aller Personen einzuholen, deren Telefonnummern im Adressbuch gespeichert sind. Wenn die Nutzer*innen dies nicht leisten können, sollten sie bei der Installation der entsprechenden App zumindest darauf achten, dass der App, soweit dies technisch möglich ist, keine Zugriffsrechte auf das Adressbuch des Endgerätes eingeräumt werden. Alternativ sollten Nutzer*innen ein Endgerät oder ein Benutzerprofil auf ihrem Endgerät verwenden, in dessen Adressbuch außer der eigenen Telefonnummer keine weiteren vorhanden sind. Dies dürfte in den meisten Fällen nicht praktikabel sein.

Der Einsatz eines Messengerdienstes, bei dem ein solcher Adressbuchabgleich stattfindet, ist unzulässig, wenn eine Einwilligung der Betroffenen nicht vorliegt, da die Schule ansonsten die Verarbeitung von personenbezogenen Daten veranlasst, die

über das für ihre Aufgabenwahrnehmung erforderliche Maß im Sinne von §§ 120 Abs. 5, 121 Abs. 1 Satz 1 SchulG hinausgeht.

Wenn datenschutzrechtliche Probleme in Bezug auf einen Messengerdienst allgemein bekannt sind, sollten Schulen gerade als öffentliche Stellen dies aufgrund von Art. 5, 24, 25 und 32 DS-GVO im Rahmen der Auswahl eines in ihrem Verantwortungsbereich eingesetzten Messengerdienstes berücksichtigen und gegebenenfalls auf ihren Einsatz verzichten.

Das MSB NRW hat die LDI NRW im August 2020 darüber informiert, dass es allen öffentlichen Schulen und Ersatzschulen den **LOGINEO NRW Messenger** zur Verfügung stellt.

IV. Ausblick: Erwartungen für die Zukunft…

In der pandemiebedingten Ausnahmesituation eingesetzte Lösungen, die nicht datenschutzkonform waren, sind nun von den Verantwortlichen anzupassen oder auszutauschen, wenn sie dauerhaft zum Einsatz kommen. Hier sind die Verantwortlichen gefordert, sobald wie möglich ein den aktuellen Umständen angemessenes Schutzniveau zu gewährleisten. Die LDI NRW setzt hierbei schwerpunktmäßig auf Überzeugungsarbeit bei den Verantwortlichen, nicht auf Untersagungen und Verbote. Selbstverständlich behalten wir uns vor, in Einzelfällen auch prüfend und kontrollierend tätig zu werden. Darüber hinaus raten wir den Schulen die Belange des Datenschutzes bei der Weiterentwicklung der digitalen Unterrichtsangebote von vornherein zu berücksichtigen. Eine umsichtige Planung von Anfang an ist meist besser und auch kostengünstiger als die spätere Nachbesserung unzureichender Systeme.

Eine weitere Entlastung der verantwortlichen Stellen sieht die LDI NRW auch in der Schaffung einheitlicher datenschutzrechtlicher Kriterien sowie entsprechender Prüf- und Zertifizierungsverfahren für die digitalen schulischen Systeme. Diesen Ansatz verfolgt das vom Bundesministerium für Bildung und Forschung initiierte Projekt „Data Protection Certification for Educational Information Systems“ (DIRECTIONS). Ziel dieses Förderprojekts ist die Konzeptionierung, exemplarische Umsetzung und

Erprobung einer nachhaltig anwendbaren Datenschutzzertifizierung von Informationssystemen im Bildungssektor. Dabei stehen insbesondere Lernanwendungen sowie Content-Plattformen im Fokus, aber auch notwendige Lerninfrastrukturen wie virtuelle Klassenzimmer, Videokonferenzsysteme oder Systeme zur Unterstützung des Unterrichts finden Berücksichtigung.

Daneben haben die Bundesländer das Projekt „eduCheck digital“, ein gemeinsames Prüfverfahren für digitale Bildungsmedien, initiiert. Beide Projekte sollen den verantwortlichen Stellen dabei helfen, durch eine verbesserte Informationslage, fundierte und vereinfachte Auswahlentscheidungen zu treffen und die Einhaltung der (datenschutz-) rechtlichen Vorgaben nachweisen zu können. Nähere Informationen zu beiden Projekten können unter den folgenden Links abgerufen werden:

- https://directions-cert.de/
- https://educheck.schule/impressum/