



Datenschutz in der Schule

Nutzung privater Endgeräte

gew-nrw.de/digitalisierung

**Gewerkschaft
Erziehung und Wissenschaft
Nordrhein-Westfalen
Nünningstr. 11
45141 Essen
TEL.: 0201 29 403-01
FAX: 0201 29 403-51**

info@gew-nrw.de
gew-nrw.de

Redaktion:
AG Digitalisierung
GEW NRW
Stephan Osterhage-Klingler

Titelfoto: shutterstock/Jastki

Stand: Januar 2019

Inhaltsverzeichnis

Vorwort	4
Europäische Datenschutzgrundverordnung (DS GVO) – Was ist das?	6
Was sind überhaupt personenbezogene bzw. personenbeziehbare Daten	7
Was ist mit der „Verarbeitung“ von Daten gemeint?	7
Grundlage der Datenverarbeitung in der Schule	8
Wichtige Grundlage – Datenschutzgesetz NRW	10
Daten von Schüler*innen und Eltern	11
Daten von Lehrer*innen	14
Genehmigung eines privaten Endgeräts – DA ADV	17
Fazit	20

Vorwort

Nicht erst seit des Inkrafttretens der neuen europäischen Datenschutzgrundverordnung (DS GVO) im Mai 2018 ist das Thema Datenschutz in der öffentlichen Wahrnehmung sehr präsent. Im Schulbereich hat die Diskussion hierzu spätestens mit der Neufassung der Dienstanweisung für die automatisierte Verarbeitung von personenbezogenen Daten in der Schule (DA ADV; vgl. BASS 10-41 Nr. 4) im Januar 2018 begonnen.

Viele Schulleitungen und die Kolleg*innen sind verunsichert und es treten zahlreiche Fragen auf. Als Mitglieder der Gewerkschaft Erziehung und Wissenschaft werden wir immer wieder nach der aktuellen Rechtslage gefragt. Außerdem stellen zahlreiche Kolleg*innen Fragen wie

- Darf ich meinen privaten PC für das Schreiben von Zeugnissen benutzen?
- Darf ich Telefonlisten meiner Klasse speichern und weitergeben?
- Wofür darf ich meinen privaten PC überhaupt noch benutzen?
- Sollte ich als Schulleitung die Nutzung privater PCs genehmigen?

Zur Beantwortung dieser Fragen macht es Sinn, sich die derzeit gültige Rechtslage einmal genauer anzusehen. Dies versuchen wir in dieser Broschüre in möglichst einfacher und verständlicher Form zu tun.

Obwohl uns bewusst ist, dass zahlreiche Rechtsverordnungen wie die Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I) und die Verordnung über die zur Verarbeitung zugelassenen Daten von Lehrer*innen (VO-DV II) derzeit überarbeitet werden und im Laufe des Jahres 2019 neu verabschiedet werden, haben wir uns entschieden, die aktuelle Rechtslage schon heute einmal genauer zu beleuchten. Sobald sich die Rechtsvorschriften in NRW geändert haben, werden wir auch diese Broschüre überarbeiten.

Die Frage nach der Nutzung privater Endgeräte stellt zwar nur einen Teil der aktuellen Situation in den Schulen dar, allerdings einen Aspekt, der viele Kolleg*innen in allen Schulformen umtreibt und verunsichert. Aus diesem Grund gehen wir im Rahmen dieser Broschüre auch gerade dieser Fragestellung gesondert nach. Wie der Abschnitt „Fazit“ – Privates Endgerät verwenden oder nicht?“ am Ende dieser Broschüre zeigt, gibt es derzeit allerdings keine einfache und schnelle Lösung für viele Probleme im Bereich der Nutzung von digitalen Endgeräten im Kontext Schule. Aber auch wenn diese Broschüre in vielen Bereichen keine Lösungen für alle Probleme des Datenschutzes im großen Spannungsfeld Schule bieten kann, versucht sie doch über die Rechtslage aufzuklären und zumindest den aktuellen Stand des Datenschutzes deutlich zu machen. Wir hoffen hierdurch zumindest Klarheit in die aktuelle Rechtslage bringen zu können und einige Fragen zu beantworten.

Mit GEWerkschaftlichen Grüßen

Stephan Osterhage-Klingler
(AG Digitalisierung)

Europäische Datenschutzgrundverordnung (DS GVO) – Was ist das?

Seit Mai 2018 ist die „neue“ Europäische Datenschutzgrundverordnung – kurz DS GVO – in aller Munde. Dabei gilt sie eigentlich bereits seit dem 24. Mai 2016, da trat die Neufassung der DS GVO in Kraft. Bis zum 25. Mai 2018 galt jedoch eine Übergangsfrist für alle Mitgliedsstaaten der EU.

Im Vergleich zu anderen vorher gültigen Regelungen der EU, muss die DS GVO nicht erst in nationales Recht umgesetzt werden, sondern gilt direkt in allen Mitgliedsstaaten. Diese sind nun lediglich aufgefordert, ihre nationalen Gesetzgebungen anzupassen bzw. im Bereich einiger „Öffnungsklauseln“ zusätzliche nationale Regelungen zu treffen. Was dazu führt, dass die DS GVO sowohl den Charakter einer Verordnung als auch den einer Richtlinie hat.

In Deutschland sind bereits zahlreiche Gesetze wie das Bundesdatenschutzgesetz oder in Nordrhein-Westfalen das Datenschutzgesetz NRW neugefasst und an die DS GVO angepasst worden.

Die DS GVO versucht dabei, die Regelungen für die Nutzung privater Daten durch Unternehmen und Behörden europaweit zu vereinheitlichen. Viele Passagen der DS GVO sind jedoch relativ unspezifisch, so dass davon auszugehen ist, dass es in den kommenden Jahren zahlreiche Gerichtsverfahren geben wird, um die Auslegung einzelner Passagen zu regeln.

In insgesamt 99 Artikeln regelt die DS GVO sowohl Definitionen als auch Verfahrensabläufe, Sanktionsmöglichkeiten und Verantwortlichkeiten. Den 99 Artikeln sind insgesamt 173 Erwägungsgründe vorausgestellt, die zur besseren Auslegung der Artikel dienen sollen.

In vielen Bereichen haben sich durch die Datenschutzgrundverordnung keine großen Veränderungen ergeben, sondern die bereits vor 2018 geltende Rechtslage gilt weiter. Gleichwohl ist aber durch die DS GVO und die damit einhergehenden öffentlichen Diskussionen der Fokus auf den Datenschutz deutlich erhöht worden und viele Aspekte des Datenschutzes werden deutlicher eingefordert.

Was sind überhaupt personenbezogene bzw. personenbeziehbare Daten?

Die Regelung, was alles zu den personenbezogenen Daten gehört, ist in Artikel 4 der DS GVO geregelt. Demnach sind dies ...

„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“

Neben den offensichtlichen Informationen wie Namen, Anschrift und Geburtsdatum sind also auch Daten als personenbezogen zu bezeichnen, die im wahrsten Sinne des Wortes auf eine Person bezogen werden können bzw. durch die eine Person identifizierbar wird, also personenbeziehbare Daten.

Damit gehören auch z.B. die Beschreibungen eines familiären Umfeldes oder die Beschreibung des Sozialverhaltens einer Schüler*in zu den personenbezogenen Daten, aber natürlich auch Fotos.

Was ist mit der „Verarbeitung“ von Daten gemeint?

Ähnlich wie die Definition des Begriffs der personenbezogenen Daten ist in Artikel 4 der DS GVO im unter Punkt 2 auch geregelt, was unter die Verarbeitung von Daten fällt:

„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“

Der Verarbeitungsbegriff ist also sehr weit gefasst. Grundsätzlich kann man also unter Datenschutzgesichtspunkten sagen, dass

jegliche Verwendung von Daten auch schon in den Bereich der Verarbeitung von Daten fällt.

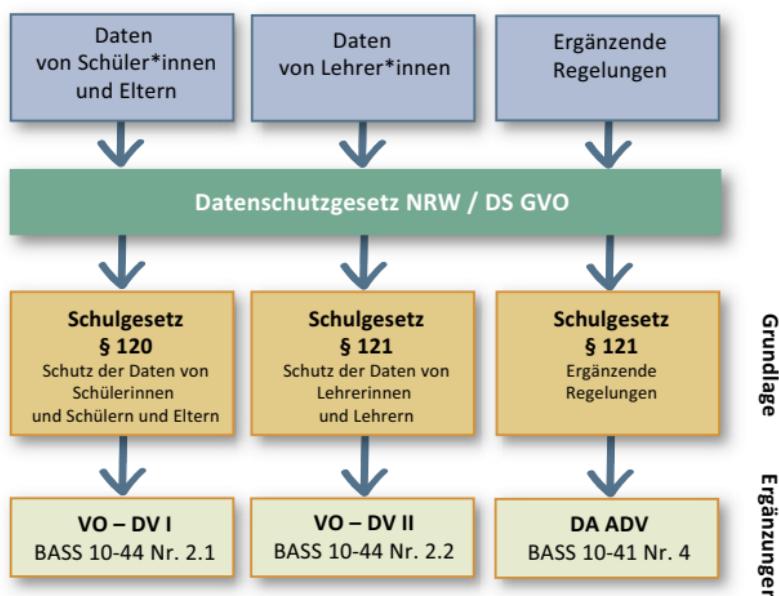
Sobald man also z.B. Daten auf dem Bildschirm eines Endgeräts (PC, Tablet oder Smartphone) sehen kann, wurden diese Daten also nach DS GVO auch verarbeitet, ganz unabhängig davon, ob man mit ihnen auch im eigentlichen Wortsinn „gearbeitet“ hat. Bereits durch das Aufrufen von Daten wurden diese ja im Sinne der DS GVO abgefragt oder ausgelesen.

Hier stellt sich jetzt die Frage nach der Verwendung sogenannter „Datensafes“, wie es sie z.B. in der neu an den Start gehenden Onlineplattform LOGINEO NRW gibt. Nach DS GVO ist davon auszugehen, dass Daten aus dem Datensafe / sensible Daten schon auf dem privaten PC verarbeitet wurden, wenn diese lediglich aus dem Datensafe aufgerufen werden – unabhängig davon, dass man sie nicht im umgangssprachlichen Sinne verarbeitet und man sich vorher durch eine doppelte Authentifizierung sicher angemeldet hat. Das heißt in der Konsequenz, dass auch die Einführung von LOGINEO NRW nach aktueller Rechtslage das Problem der fehlenden dienstlichen Endgeräte nicht lösen kann.

Grundlage der Datenverarbeitung in der Schule

Der Ausgangspunkt der rechtlichen Regelungen zum Datenschutz ist das Grundrecht auf informationelle Selbstbestimmung. Hierunter wird das Recht jedes Einzelnen verstanden, selbst über die Preisgabe und Verwendung der eigenen personenbezogenen Daten zu bestimmen. Auch wenn dieses Recht im Grundgesetz nicht explizit verankert ist, hat es trotzdem den Status eines Grundrechts. Im Rahmen des Volkszählungsurteils von 1983 hat das Bundesverfassungsgericht festgelegt, dass das Grundrecht auf informationelle Selbstbestimmung eine besondere Ausprägung des in Artikel 22 Absatz 1 des Grundgesetzes verankerten allgemeinen Persönlichkeitsrechts ist.

Dieses Recht hat also den Status eines Grundrechtes, was in der Konsequenz dazu führt, dass Gesetze und Verordnungen dieses Recht sicherstellen müssen. Nach Artikel 30 des Grundgesetzes fällt der Bereich der Bildung dabei in die Zuständigkeit der Bundesländer. Hier müssen daher die Gesetze und Verordnungen für jedes einzelne Bundesland in Bezug auf den Datenschutz erlassen



werden, die sich am Bundes- und Europarecht orientieren. Die Ausführungen dieser Broschüre beziehen sich daher ausschließlich auf die rechtliche Situation in Nordrhein-Westfalen.

Diese gesetzliche Grundlage der gesamten Verarbeitung von personenbezogenen Daten in der Schule (sowohl von Schüler*innen und Eltern als auch von Lehrer*innen) ist im Schulgesetz in den Paragraphen 120 bis 122 geregelt. Gleichzeitig findet natürlich beim Umgang mit Daten immer auch das Datenschutzgesetz NRW sowie die Datenschutzgrundverordnung (DS GVO) Anwendung.

Die Bestimmungen des Datenschutzgesetzes NRW (DSG NRW) legen auf der Grundlage der Datenschutzgrundverordnung (DSGVO) die Rahmenbedingungen der Datenverarbeitung und des Datenschutzes allgemein fest.

Für den Bereich der Schule regelt dabei das Schulgesetz die Regelungen, die nicht allgemeingültig sind, sondern extra für diesen Bereich getroffen werden. Während die Paragraphen 120 und 121 Schulgesetz die Grundlage für die Verarbeitung von Daten von Schüler*innen und Eltern (§120) sowie von Lehrer*innen (§121) bilden, legt §122 weitere datenschutzrechtliche Vorschriften fest, die bei der Datenverarbeitung in der Schule berücksichtigt werden müssen.

Diese rechtlichen Grundlagen des Datenschutzes in der Schule, die im Schulgesetz festgeschrieben sind, werden durch weitere, ergänzende Gesetze und Rechtsverordnungen ergänzt (siehe Übersicht oben).

Wichtige Grundlage – Datenschutzgesetz NRW

Auch im Schulgesetz wird in §122 darauf verwiesen, dass natürlich die allgemeinen datenschutzrechtlichen Bestimmungen Gültigkeit behalten und eingehalten werden müssen. Diese Grundlagen regelt das Datenschutzgesetz NRW, das dabei im Rahmen der Vorgaben der europäischen Datenschutzgrundverordnung (DS GVO) ergänzende Regelungen festlegt und Begriffe definiert.

So regelt das Datenschutzgesetz zum Beispiel in §15, dass geeignete „technische und organisatorische Maßnahmen“ ergriffen werden müssen, um Daten auf digitalen Endgeräten zu schützen. Dabei verweist das Datenschutzgesetz auf die Regelungen in Artikel 32 DS GVO. Dort werden allerdings primär die Datenschutzziele formuliert und nicht mehr die konkreten Datenschutzmaßnahmen.

Man kann aber davon ausgehen, dass die folgenden technischen und organisatorischen Maßnahmen zum Datenschutz nach DS GVO und dem Datenschutzgesetz NRW eingehalten werden müssen, die auch in der Anlage zur Dienstanweisung zur automatisierten Verarbeitung von personenbezogenen Daten in der Schule (DA ADV; BASS 10-41 Nr. 4) aufgeführt sind. Auch wenn es dort ausschließlich um die Nutzung privater Endgeräte geht, stellt die Auflistung sowohl technische als auch organisatorische Maßnahmen dar, die grundsätzlich für digitale Endgeräte eingehalten werden müssen, um Vertraulichkeit, Integrität und Verfügbarkeit der Daten sicherstellen zu können:

- Zugriffsschutz der eingesetzten Endgeräte durch ein adäquates Verfahren (z.B. ein ausreichendes Passwort)
- Automatische Sperre der Endgeräte nach maximal 15 Minuten
- Anlegen eines eigenen Benutzerkontos für dienstliche Zwecke
- Verschlüsselung der gespeicherten Daten durch ein geeignetes Verfahren (z.B. bei einem externen Datenträger)
- Einsatz eines Betriebssystems für das aktuelle Sicherheits-updates verfügbar sind
- Einsatz einer aktuellen Virenschutz-Software
- Einsatz einer Firewall
- Regelmäßige Aktualisierung der Betriebssysteme
- Regelmäßige Aktualisierung eingesetzter Anwendungen (z.B. Virendefinitionen)
- Regelmäßige Backups der verarbeiteten Daten

Diese Auflistung – die sicherlich nicht abschließend ist – zeigt schon, wie schwer es für einen Laien ist, alle Maßnahmen zu ergreifen und einzuhalten. Gerade Maßnahmen zum Schutz eines Endgeräts in einem Netzwerk mit Internetzugang wie z.B. Port-freigaben o.ä. sind noch gar nicht mit aufgenommen.

Daten von Schüler*innen und Eltern

Wann die Verarbeitung von Daten von Schüler*innen und Eltern in der Schule und der Schulaufsichtsbehörde zulässig ist, regelt §120 Schulgesetz: „§120 Absatz 1 Schulgesetz NRW: Schulen und Schulaufsichtsbehörden dürfen personenbezogene Daten der Schülerinnen und Schüler, der in § 36 genannten Kinder sowie der Eltern verarbeiten, soweit dies zur Erfüllung der ihnen durch Rechtsvorschrift übertragenen Aufgaben erforderlich ist. Die gespeicherten personenbezogenen Daten dürfen in der Schule nur den Personen zugänglich gemacht werden, die sie für die Erfüllung ihrer Aufgaben benötigen.“

Pflichtdaten

Für die Verarbeitung von Schüler*innen- und Elterndaten ist in §120 Absatz 1 Schulgesetz geregelt, dass in der Schule bzw. in der Schulaufsichtsbehörde alle Daten verarbeitet werden dürfen, die für die Erfüllung der Aufgaben benötigt werden. Diese Aufgaben ergeben sich auch aus den jeweiligen Ausbildungsordnungen für die einzelnen Schulformen.

Hierzu gehören sicherlich Daten wie Namen, Anschriften und Erreichbarkeiten im Notfall. Die Erziehungsberechtigten sowie die Schüler*innen sind zur Angabe dieser Daten gesetzlich verpflichtet. Aber natürlich gehören auch Daten, die für den Unterrichtsalltag benötigt werden, wie z.B. Noten, Leistungsstandbeschreibungen u.ä. zu den Daten die aufgrund der durch Rechtsvorschriften übertragenen Aufgaben in der Schule benötigt werden und damit verarbeitet werden dürfen.

Freiwillige Daten

Andere Daten, wie Fotos oder Hobbies u.ä., sind nicht für die Erledigung der durch Rechtsvorschriften übertragenen Aufgaben notwendig und dürfen damit nur auf freiwilliger Basis erhoben und verarbeitet werden, wie Absatz 2 des §120 Schulgesetz regelt.

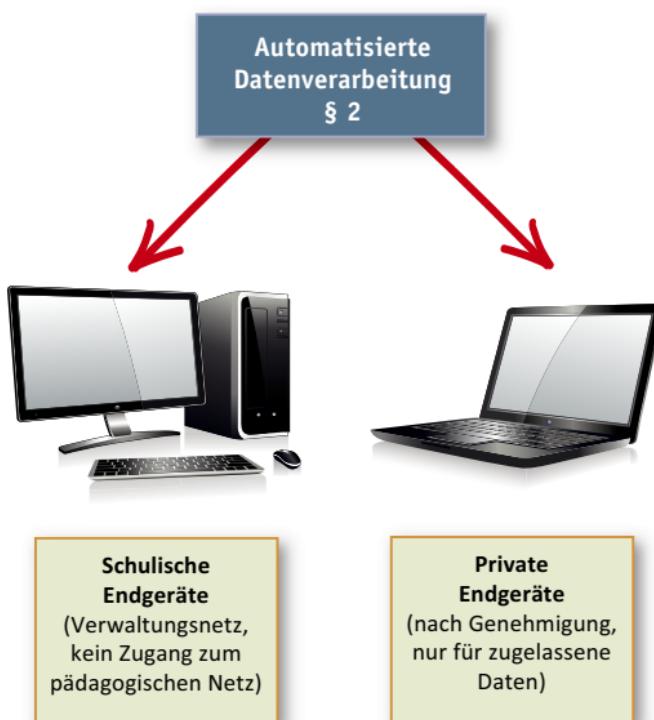
Fotos

Fotos, die in der Schule für Ausstellungen, Dokumentationen o.ä. erstellt werden, sind also nicht grundsätzlich durch das Schulgesetz gedeckt, sondern bedürfen der vorherigen, schriftlichen Genehmigung durch die betroffene Person bzw. die Erziehungsberechtigten. Hier gilt das Prinzip der Freiwilligkeit. Niemand kann dazu gezwungen werden, sein Einverständnis zu geben, dass z.B. Fotos von ihr/von ihm in der Schule gemacht und verwendet werden.

VO-DV I

Gleichzeitig gibt es weitere Rechtsverordnungen, die die Verarbeitung dieser Daten und die zu treffenden Datenschutzmaßnahmen näher erläutern. Für den Bereich der Daten von Schüler*innen und Schülern sowie Eltern ist dies die Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I; vgl. BASS 10-44 Nr. 2.1).

Gerade die in 2017 neugefasst VO-DV I bestimmt hier genau, was wo verarbeitet werden darf. So wird zum einen festgelegt, welche Daten überhaupt in der Schule verarbeitet werden dürfen (§4) und welche Daten auf welchen Geräten verarbeitet werden dürfen (§2).



Es dürfen also Daten nur auf dienstlichen Endgeräten verarbeitet werden, die abgekoppelt sind vom schulischen, pädagogischen Netz und die die technischen und organisatorischen Maßnahmen des Datenschutzes aufweisen. Verantwortlich für die Einhaltung der technischen und organisatorischen Maßnahmen zum Datenschutz ist dabei die Schulleiterin / der Schulleiter (§1 VO DV I).

Private Endgeräte

Auf privaten Endgeräten dürfen Daten von Schüler*innen und Eltern nur verarbeitet werden, wenn diese Geräte im Vorfeld durch die Schulleitung genehmigt wurden (siehe DA ADV, Seite 17). Aber auch nach der Genehmigung der Nutzung eines privaten Endgeräts legt die VO DV I in der Anlage 3 fest, welche Daten auf einem privaten Endgerät verarbeitet werden dürfen. Alle Daten, die nicht in der Liste der Anlage 3 auftauchen, dürfen damit auch grundsätzlich nicht auf einem privaten Endgerät verarbeitet werden. Gleichzeitig wird festgelegt, dass diese Daten nicht durch alle Lehrkräfte verarbeitet werden dürfen, sondern lediglich durch die, die die Schüler*in auch wirklich unterrichten.

Daten, die auf einem privaten Endgerät durch die Schüler*in unterrichtende Lehrkraft verarbeitet werden dürfen (Anlage 3, VO-DV I):

- Vorname, Name, Geburtsname
- Geschlecht, Geburtsdatum, Konfession
- Klasse/Jahrgangsstufe, Kurs
- Schülernummer
- Ausbildungsrichtung bzw. Ausbildungsberuf
- Fächer, in denen die Lehrkraft Schüler*in unterrichtet
- Leistungsbewertungen in diesen Fächern
- Zeiten des Fernbleibens in diesen Fächern
- Vermerk über Benachrichtigung nach §50 SchulG Abs. 4 (Minderleistung, die zu einer Nichtversetzung führen kann)
- Erreichbarkeit der zuständigen Personen

Klassenlehrer*in / Schulleitung

Über diese Auflistung hinaus, dürfen Schulleiter*innen, deren Stellvertretungen sowie Klassenlehrer*innen oder Jahrgangsstufenleiter*innen auch noch die folgenden Daten auf einem privaten Endgerät verarbeiten, wenn dieses im Vorfeld genehmigt wurde:

- Halbjahresnoten in allen Fächern
- alle zeugnisrelevanten Leistungsangaben
- eugnisbemerkungen
- Vermerk über Benachrichtigung nach §50 SchulG Abs. 4 (Minderleistung, die zu einer Nichtversetzung führen kann)

Neben der Anlage 3 regeln die weiteren Anlagen 1 und 2 noch, welche Daten auf dienstlichen Endgeräten verarbeitet werden dürfen und welche Daten damit zum Datenbestand der Schule gehören.

Daten von Lehrer*innen

Analog zur Verarbeitung der Daten von Schüler*innen und Eltern ist die Verarbeitung der Daten von Lehrer*innen, Referendar*innen und Lehrkräften in Ausbildung geregelt. §121 Schulgesetz regelt die Grundlagen und die Verordnung über die Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrer, die Verordnung über die zur Verarbeitung zugelassenen Daten der Lehrerinnen und Lehrern (BASS 10-41 Nr. 6.1) spezifiziert diese. Allgemein wird in §121 Schulgesetz geregelt, welche Daten von Lehrer*innen grundsätzlich in der Schule und welche grundsätzlich durch die Schulaufsicht verarbeitet und gespeichert werden dürfen. Hierbei erfolgt keine dezidierte Aufzählung, sondern es werden Zwecke definiert, für deren Durchführung benötigte Daten verarbeitet werden dürfen. Eine Spezifizierung erfolgt dann in der VO-DV II. Alle anderen Daten bedürfen der Einwilligung durch die betroffene Lehrkraft. Alle Daten, die den folgenden Zwecken dienen, dürfen also in der Schule oder in der Schulaufsichtsbehörde verarbeitet werden:

Schule	Schulaufsichtsbehörden
Planung und Ermittlung des Unterrichtsbedarfs	Unterrichtsbedarf und Personalmaßnahmen
Durchführung des Unterrichts	Lehrerausbildung und Lehrerfortbildung
Maßnahmen der Qualitätsentwicklung und der Qualitätssicherung	Aufstellung des Haushalts und Bewirtschaftung der Haushaltsmittel
wissenschaftlichen Untersuchungen	Betreuung von Bewerber*innen für die Einstellung in den Schuldienst
Schulmitwirkung	
dienstrechtlichen, arbeitsrechtlichen oder sozialen Angelegenheiten	Sonstige schulaufsichtliche Zwecke

Es gibt aber auch besonders geschützte Daten von Lehrkräften:

§121 Absatz 2 Satz 2 Schulgesetz NRW:

„Verhaltensdaten von Lehrerinnen und Lehrern, Daten über ihre gesundheitlichen Auffälligkeiten mit Ausnahme des Grades einer Behinderung, Ergebnisse von psychologischen und ärztlichen Untersuchungen sowie Daten über soziale und therapeutische Maßnahmen und deren Ergebnisse dürfen nicht automatisiert verarbeitet werden.“

Die in §121 Absatz 2 Satz 2 genannten Daten stellen dabei Ausnahmen dar, die grundsätzlich nicht automatisiert verarbeitet, gespeichert und übermittelt werden dürfen. Deswegen erhält der Arbeitgeber (die Schule) z.B. auch bei einer Krankschreibung keine Diagnose, sondern lediglich die attestierte Dauer der Krankschreibung.

In der VO-DV II ist die Verarbeitung der Daten, die zur Erfüllung der in der Tabelle oben aufgeführten Tatbestände erforderlich sind, genauer geregelt.

So legt der §5 VO-DV II den genauen Datenbestand fest, der in der Schule bzw. durch die Schulleitung verarbeitet und gespeichert werden darf. Eine dezidierte Auflistung dieser Daten findet sich in den Anlage 1 und 2 zur VO-DV II.

Die Verarbeitung von Daten von Lehrkräften auf privaten Endgeräten ist grundsätzlich ausgeschlossen. Sie darf lediglich auf dienstlichen Endgeräten erfolgen.

Einige Ausnahme hiervon ist die Verarbeitung von Daten von Lehramtsanwärter*innen, wie in §2 Absatz 4 VO-DV II festgelegt:

„Die Verarbeitung personenbezogener Daten von Lehramtsanwärterinnen und Lehramtsanwärtern und Lehrkräften in Ausbildung in privaten ADV-Anlagen der mit der Ausbildung beauftragten Personen bedarf der schriftlichen, ein Verfahrensverzeichnis gemäß § 8 DSG NRW enthaltenden Genehmigung durch die Leiterin oder den Leiter des Zentrums für schulpraktische Lehrerausbildung. Die Genehmigung darf nur erteilt werden, wenn die Verarbeitung der Daten nach Art und Umfang für die Ausbildung erforderlich ist und ein angemessener technischer Zugangsschutz nachgewiesen wird. Die für die Verarbeitung zugelassenen Daten ergeben sich aus der Anlage 6. Für die nach Satz 1 genehmigte Verarbeitung personenbezogener Daten in privaten ADV-Anlagen ist das Zentrum für schulpraktische Lehrerausbildung öffentliche Stelle im Sinne des § 2 Absatz 1 DSG NRW. Die mit der Ausbildung beauftragten Personen sind verpflichtet, der Leiterin oder dem Leiter des Zentrums für schulpraktische Lehrerausbildung alle Auskünfte zu erteilen, die für die Wahrnehmung der datenschutzrechtlichen Verantwortung erforderlich sind.“

Es bedarf also auch hier wieder einer vorherigen Genehmigung des privaten Endgeräts, um dieses nutzen zu können, was besonders für Fachleiter*innen wichtig ist.

Fachleiter*innen und Ausbildungslehrkräfte

Nach der Anlage 6 zur VO-DV II dürfen damit Fachleiter*innen, Ausbildungslehrer*innen und Schulleitungen folgende Daten von Lehramtsanwärter*innen auf einem privaten Endgerät verarbeiten, wenn dies zuvor genehmigt wurde:

- Name, Vorname
- E-Mail (soweit erforderlich, sonst nur mit Einwilligung)

- Beurteilungen der Leistungen
- Dienstliche E-Mail-Adresse

Gleichzeitig muss darauf hingewiesen werden, dass der Verweis in §2 Absatz 4 auf das Datenschutzgesetz NRW sich auf die alte Fassung bezieht und noch nicht auf die aktuell gültige Neufassung des Datenschutzgesetzes NRW.

Genehmigung eines privaten Endgeräts – DA ADV

Im Januar 2018 wurde durch das Ministerium für Schule und Bildung die Dienstanweisung für die automatisierte Verarbeitung von personenbezogenen Daten in der Schule (DA ADV; BASS 10-41 Nr. 4) neu gefasst und beschlossen.

Auch wenn sich grundsätzlich hierdurch an der rechtlichen Grundlage nichts geändert hat, wurde ein enormer Fokus auf das Thema Datenschutz und besonders auf den Gebrauch von privaten Endgeräten gelegt.

Außerdem wurde mit der Neufassung der DA ADV auch die Grundlage gelegt, um eine Basis-IT-Infrastruktur – also eine webbasierte Arbeitsplattform wie z.B. LOGINEO NRW – zu nutzen und gleichzeitig Daten auf kommunalen Servern wie z.B. im kommunalen Rechenzentrum zu speichern.

Ansonsten fasst die DA ADV zahlreiche Vorschriften aus den oben bereits beschriebenen Verordnungen (VO-DV I und VO-DV II) noch mal zusammen und verweist darauf.

Trennung der Netze in der Schule

Besonders weist die DA ADV noch einmal auf den bereits oben erwähnten Sachverhalt hin, dass das pädagogische Netz und das Verwaltungsnetz in der Schule zu trennen sind (VO-DV II, Absatz 1).

„Schuleigene ADV-Anlagen, zu denen Schülerinnen und Schüler Zugang haben, dürfen nicht für die lokale Verarbeitung der unter Nummern 4.3.2.1 bis 4.3.2.4 sowie 4.3.3 genannten Dokumente eingesetzt werden. Die lokale Verarbeitung von Zeugnissen, sonderpädagogischen Gutachten gemäß § 19 Absatz 5 SchulG (BASS 1-1), Lern- und Förderempfehlungen gemäß § 50 Absatz 3

SchulG und Benachrichtigungen gemäß § 50 Absatz 4 SchulG ist auf diesen Anlagen untersagt. Dieses bezieht sich in der Regel auf Anlagen außerhalb des Verwaltungsnetzes.“

Während also gewisse Daten auch auf Endgeräten im pädagogischen Netz verarbeitet werden dürfen, sind die folgenden Daten hier ausgeschlossen:

- Berichte an die Schulaufsichtsbehörden in dienstrechtlichen Angelegenheiten und in Angelegenheiten der Lehrerversorgung
- Berichte zur Vorbereitung von Dienstleistungszeugnissen, Beratung der Schulaufsichtsbehörden zur dienstlichen Beurteilung, Fertigen von dienstlichen Beurteilungen, Berichte in disziplinarrechtlichen Angelegenheiten
- Beantwortung von Anfragen und Erhebungen der Schulaufsichtsbehörden
- Beantwortung von Anfragen und Erhebungen des Schulträgers (in äußeren Schulangelegenheiten) sowie anderer Behörden aus dem Geschäftsbereich des Ministeriums für Schule und Bildung und wissenschaftlicher Einrichtungen
- Aktualisierung der Amtlichen Schuldaten und der Stellendatei des Ministeriums für Schule und Bildung.

Außerdem ist die Verarbeitung von Zeugnissen, sonderpädagogischen Gutachten, Lern- und Förderempfehlungen sowie Benachrichtigungen nach §50 Absatz 4 Schulgesetz (Benachrichtigung über Minderleistungen, die die Versetzung gefährden können) auch grundsätzlich auf Endgeräten im pädagogischen Netz der Schule ausgeschlossen.

Hierfür bleiben nur Endgeräte im Verwaltungsnetz, da nach VO-DV I auch die Nutzung eines privaten Endgeräts für einen Großteil dieser Punkte ausgeschlossen wurde (siehe Seite 13).

Genehmigung privater Endgeräte

Mit der Neufassung der DA ADV wurde in der Anlage auch ein Genehmigungsformular für die Nutzung privater Endgeräte vorgelegt, das nun verpflichtend zu verwenden ist und das in Zukunft alte, bereits bestehende Genehmigungsformulare ersetzen soll.

„Die Verarbeitung personenbezogener Daten für dienstliche Zwecke auf privaten ADV-Anlagen von Lehrkräften ist nur mit schriftlicher Genehmigung der Schulleiterin oder des Schulleiters zulässig. Es gilt § 2 Absatz 2 mit Anlage 3 der VO-DV 1. Für die Genehmigung ist der als Anlage beigefügte Genehmigungsvordruck zu verwenden.“ (DA ADV, Punkt 11.1)

Private Endgeräte können also für die Verwendung dienstlicher Tätigkeiten eingesetzt werden, wenn die Geräte zum einen durch die Schulleitung genehmigt wurden und es sich zum anderen um Daten handelt, die nach VO-DV I oder II für die Verarbeitung auf privaten Endgeräten zugelassen sind. Voraussetzung ist dabei immer die Erfordernis, dass in der Schule nicht ausreichend dienstliche Endgeräte zur Verfügung stehen.

Hierbei muss auch berücksichtigt werden, dass zu den privaten Endgeräten nicht nur der heimische PC, sondern natürlich auch Laptops, Tablets und vor allem auch Smartphones u.ä. zählen.

Smartphone und WhatsApp

Gerade die Nutzung eines Smartphones, das in erster Linie für den privaten Bereich genutzt wird, bringt datenschutzrechtlich zahlreiche Schwierigkeiten mit sich. Genau wie für alle anderen – auch für dienstliche Zwecke genutzten – Endgeräte, bedarf es einer Genehmigung des Smartphones mittels des Genehmigungsformulars durch die Schulleitung. Gleichzeitig sind die einzuhaltenden technischen und organisatorischen Maßnahmen bei der Nutzung eines Smartphones kaum einzuhalten. Besonders schwierig wird dies, wenn auf dem Gerät auch Instant-Messaging-Dienste wie z.B. WhatsApp genutzt werden. Bei der Nutzung von z.B. WhatsApp genehmigt man der App die im Handy gespeicherten Kontaktdaten auszulesen und zu speichern. Diese Speicherung erfolgt dann auf den Servern von Facebook (Mutterkonzern zu dem WhatsApp gehört) in Kalifornien. Diese Server unterliegen aber weder der DS GVO noch dem deutschen Datenschutzrecht, sondern dem amerikanischen.

Man kann also festhalten, dass die Speicherung von personenbezogenen, dienstlichen Daten (Kontaktdaten, Noten, ...) und die gleichzeitige Nutzung von z.B. WhatsApp auf dem gleichen Gerät sich datenschutzrechtlich ausschließt.

Entscheidend bei der Genehmigung von privaten Endgeräten aller Art ist der Punkt, dass die Genehmigung durch die Schulleiterin bzw. den Schulleiter erfolgt. Sie bzw. er trägt damit auch einen großen Teil die Verantwortung sowie ist verpflichtet, die Einhaltung der Datenschutzbestimmungen sicher zu stellen (DA ADV Nr. 3).

Gleichzeitig trägt auch jeder selbst die Verantwortung für den Datenschutz. Spätestens mit der Unterzeichnung des Genehmigungsformulars versichert man, alle dort aufgeführten Maßnahmen (vgl. „technische und organisatorische Maßnahmen“; Seite 10) auf seinem privaten Endgerät auch einzuhalten. Damit ist man selber also auch in der Haftung, sollte man die Maßnahmen trotz erteilter Unterschrift nicht einhalten.

Fazit

Insgesamt bleibt festzuhalten, dass die „neue“ Rechtslage nach dem Inkrafttreten der DS GVO zwar nicht viele Neuerungen bzw. Änderungen des Datenschutzes gebracht hat, aber einen enormen Fokus auf diese Thematik gelenkt hat.

So wurde durch die aktuelle Rechtslage und ein erstes Urteil vom Oberlandesgericht (9.3.2018; I-11U/2517) zum Thema Schließanlagen z.B. die Rolle der Schulleitung als datenverarbeitende Stelle deutlich betont. Damit wird der Schulleitung im Bereich des Datenschutzes eine deutlich höhere Verantwortung auferlegt als noch zuvor. Während die Schulträger mehr zu „Beschaffern“ von Hard- und Software gemacht werden, liegt die datenschutzrechtliche Verantwortung bei den Schulleitungen.

Dies hat auch gerade auf die Genehmigung von privaten Endgeräten der Kolleg*innen Auswirkungen.

Wie kompliziert und umfassend die Frage nach dem Datenschutz in Schulen aussieht, zeigt auch eine FAQ-Liste, die das Schulministerium Ende 2018 auf seiner Homepage veröffentlicht hat. Auf vielen Seiten werden hier über 40 Fragen zu den Themengebieten Schulhomepage, zur Genehmigung und Nutzung privater Endgeräte sowie weitere allgemeine Fragen des Datenschutzes erläutert.

Auch wenn es sinnvoll erscheint alle diese Fragen durch offizielle Stellen beantworten zu lassen, sind viele der Antworten noch fragwürdig. So wird zum Beispiel für Gutachten darauf hingewiesen, dass diese sehr wohl auf privaten Endgeräten verfasst werden dürfen, wenn sie dort anonymisiert (ohne Klarnamen und Daten aber natürlich auch ohne personenbeziehbare Daten – wie Beschreibung von Lerngruppen oder Lernbiografien) verfasst werden. In der Realität ist dies sicherlich kaum umsetzbar. Die GEW geführten Personalräte befinden sich hier noch in weiterführenden Gesprächen mit dem MSB.

Grundsätzlich bleibt festzuhalten, dass niemand zur Beantragung der Nutzung seines privaten Endgerätes verpflichtet werden kann. Die Beantragung ist vollständig freiwillig. Genauso wenig ist die Schulleitung im Anschluss verpflichtet die Genehmigung zur Nutzung eines privaten Endgeräts zu erteilen, da sie rechtlich für die Einhaltung der Datenschutzbestimmungen der dienstlich erhobenen personenbezogenen Daten (mit)verantwortlich ist.

Die Entscheidung, die Nutzung eines privaten Endgeräts zu beantragen, bleibt also jedem selbst überlassen. Häufig entsteht in den Schulen Druck dies zu tun, da keine bzw. bei weitem nicht ausreichend dienstliche Endgeräte zur Verfügung stehen. Nichtsdestotrotz sollte sich jeder gut überlegen, wie er vorgeht bzw. ein Kollegium sollte gemeinsam mit der Schulleitung im Rahmen einer Lehrerkonferenz beraten wie es vorgehen möchte.

Es gibt aktuell leider keine einfache und schnelle Lösung für das Problem der fehlenden dienstlichen Endgeräte.

Es bleiben nach aktueller Rechtslage und bei aktueller Ausstattung der Schulen also derzeit nur die folgenden – alle unbefriedigenden – Lösungen:

- Das Genehmigungsformular nicht unterschreiben und keine personenbezogenen Daten mehr auf dem privaten Endgerät verarbeiten.

Dies würde in vielen Fällen bedeuten: zurück zu Papier und Stift. Hierbei wäre zumindest die Haftungsfrage geklärt und niemand liefe Gefahr persönliche für Datenschutzverstöße haftbar gemacht zu werden. Ob diese Vorgehensweise allerdings wirklich praktikabel ist, bleibt dahingestellt. Unbequem und mit Mehrarbeit verbunden wäre sie allemal.

- Das Genehmigungsformular nicht unterschreiben und trotzdem weiter machen wie bisher und alle Daten auf dem privaten Endgerät verarbeiten.

Hier von ist definitiv abzuraten. Bei der Nutzung des privaten Endgeräts ohne vorherige Genehmigung durch die Schulleitung, macht sich jede*r Einzelne zum einen persönlich haftbar in Bezug auf Datenschutzverstöße zum anderen könnte dies auch dienst- bzw. arbeitsrechtliche Konsequenzen haben.

- Das Genehmigungsformular unterschreiben und das private Endgerät weiter für die Verarbeitung personenbezogener Daten verwenden.

Ein Haftungsausschluss wird nur erreicht, wenn alle geforderten Maßnahmen auch vollständig und ohne Ausnahme eingehalten werden. Sollte man dies nicht sicherstellen können, macht man sich erneut haftungstechnisch angreifbar.

Selbst, wenn jemand in der Lage sein sollte, alle geforderten Maßnahmen zu ergreifen, die im Genehmigungsformular für die Nutzung des privaten Endgeräts gefordert werden, bleibt immer noch das Problem, dass zahlreiche Daten trotzdem nicht auf dem privaten Gerät verarbeitet werden dürfen (vgl. Liste der zur Verarbeitung auf privaten Endgeräten zugelassenen Daten, Seite 13).

Das Land NRW ist jetzt gefordert, Lösungen zu finden. Aus Sicht der GEW können diese nur darin bestehen, die Lehrkräfte zeitnah mit einer ausreichenden Anzahl an dienstlichen Endgeräten auszustatten.

Diese Auffassung vertritt auch die Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI) Hella Block, die bereits 2016 darauf hinwies, dass der Datenschutz in der Schule ausschließlich mit der Stellung von dienstlichen Endgeräten gewährleistet werden kann.

Das Ministerium für Schule und Bildung muss jetzt zeitnah eine gemeinsame Lösung mit den Kommunen als Schulträgern finden, um die Lehrkräfte in NRW in die Lage zu versetzen, datenschutzkonform zu arbeiten und ihre vom Land übertragenen Aufgaben erledigen zu können.

Die GEW wird diesen Prozess aktiv begleiten und sich immer wieder mit Aktionen, Forderungen und Diskussionsbeiträgen einbringen.

Seit November 2018 liegt ein Rechtsgutachten des Parlamentarischen Gutachterdienstes des Landtages Nordrhein-Westfalen mit dem Titel „Ausstattung von Lehrkräften mit digitalen Arbeitsgeräten an Schulen in Nordrhein-Westfalen“ vor.

In diesem Gutachten werden die aktuelle Rechtslage und die Erfordernisse der Schulen in NRW von Prof. Dr. Michael Wräse (Wissenschaftszentrum für Sozialforschung Berlin) genauer in den Blick genommen. Im Ergebnis stellt Prof. Dr. Wräse fest, dass eine angemessen Ausstattung der Schulen mit Computern und digital zugänglichen Medien nach dem Schulgesetz zur Umsetzung von Bildungszielen notwendig ist. Gleichzeitig sieht er hier sowohl die Schulträger als Beschaffer benötigter Ausstattung in der Pflicht als auch im Rahmen der Fürsorgepflicht das Land NRW als Arbeitgeber der Lehrer*innen.

„Zwar verbleibt dem Schulträger nach § 79 SchulG NRW ein erheblicher Spielraum, wie er seiner Verpflichtung nachkommt. Er schuldet lediglich eine am allgemeinen Stand der Technik und Informationstechnologie „orientierte“ Sachausstattung. Allerdings gibt es faktisch nur zwei Möglichkeiten: Der Schulträger kann entsprechend ausgestattete Arbeitsplätze für die Lehrkräfte in genügender Anzahl im Schulgebäude vorhalten.

Stattdessen kann er die Lehrkräfte auch mit (Dienst-)Computern ausstatten, welche diese (auch) zu Hause nutzen können. Wird keine der genannten Optionen umgesetzt, so verstößt der Schulträger gegen seine Verpflichtung aus § 79 SchulG NRW.“

(Wräse, Prof. Dr., Michael; 2018; Rechtsgutachten zur Ausstattung von Lehrkräften mit digitalen Arbeitsgeräten an Schulen in Nordrhein-Westfalen; S. 52)

Aus Sicht der GEW kann die Lösung nur die Ausstattung aller Lehrkräfte mit mobilen dienstlichen Endgeräten sein, da in den Schulen nicht ausreichend Arbeitsplätze zur Verfügung stehen.

gew-nrw.de/digitalisierung