Bei Beginn des neuen Schuljahres soll allen Eltern eine klasseninterne Telefonliste zur Verfügung gestellt werden. Was ist dabei zu beachten?

Oft wird zum Schuljahresbeginn in den Klassen, meist beim ersten Elternabend, eine Telefonliste/E-Mailliste verteilt, um die Kontaktaufnahme der Eltern untereinander zu ermöglichen bzw. die Weitergabe von Informationen über Stundenausfall oder andere Ereignisse zu erleichtern.

Die Daten für eine solche Kontaktliste werden meistens von den Schulen anhand der Klassenliste erstellt und dann von den Lehrkräften verteilt. Hierbei handelt es sich seitens der Schule um eine Datenübermittlung an private Stellen (die Eltern), die der schriftlichen Einwilligung der Eltern bedarf.

Für eine solche Liste reicht es aus, die Namen der Schülerinnen und Schüler sowie die Telefonnummer(n) und die E-Mail-Adresse zu erfassen. Die Einwilligung der Eltern kann bereits mit der Anmeldung des Kindes zum Schulbesuch eingeholt werden. So ist es der Schulverwaltung möglich, bereits bei der Zusammenstellung der Klasse und der Erstellung der schulverwaltungsinternen Klassenliste die Telefonliste gleich mit anzufertigen.

Wenn eine Schule standardmäßig Vertretungspläne auf der Schulhomepage veröffentlicht und über sonstige unvorhergesehene Ereignisse über die Schulhomepage informiert, ist zu prüfen, ob eine solche Kontaktliste (noch) erforderlich ist. Bei der Prüfung der Erforderlichkeit ist insbesondere der Grundsatz der Datenminimierung (Artikel 5 Absatz 1 Buchstabe c DSGVO) zu beachten. Darüber hinaus wird die Schulverwaltung von Arbeit (Erstellen der Kontaktlisten) entlastet.

Darf die Schule Angaben zur Sorgeberechtigung über die Schülerin oder den Schüler erheben?

§ 30 Abs. 1 Satz 2 Nr. 2 SchulG sieht zwar nicht ausdrücklich vor, dass Angaben zur Sorgeberechtigung erhoben und weiterverarbeitet werden dürfen. Der Elternbegriff im Schulgesetz orientiert sich grundsätzlich an der Sorgeberechtigung des Bürgerlichen Gesetzbuches, zählt aber auch weitere Varianten auf (vgl. § 2 Abs. 5 SchulG). Weil die Zahl der Alleinerziehenden oder der Lebensgemeinschaften ohne Trauschein - aber mit gemeinsamen Kindern - zunimmt, spielt die Frage des Sorgerechtes für die Schule eine immer größere Rolle. Davon hängt ab, an wen Schülerdaten weitergegeben werden dürfen.

Das Sorgerecht ist im Bürgerlichen Gesetzbuch (BGB) geregelt. Es unterscheidet verschiedene Gruppen von Sorgeberechtigten. Die häufigsten Konstellationen - mit Konsequenzen für die Befugnis, Daten des Kindes an diese Personen weiterzugeben - sind:

1. Zusammen lebende Eltern: Gemeinsames Sorgerecht (§ 1626 BGB) = Mitteilung von Daten an beide Elternteile grundsätzlich zulässig

2. Dauernd getrennt lebende Eltern: Grundsätzlich gemeinsames Sorgerecht, es sei denn, gerichtlich ist etwas anderes geregelt (§ 1671 BGB) = Mitteilung grundsätzlich an beide Elternteile zulässig, aber bei gerichtlicher anderer Entscheidung: Übermittlung nur an den festgelegten Sorgeberechtigten

3. Unverheiratete Partner mit gemeinsamen Kindern (§ 1626a BGB): Gemeinsames Sorgerecht bei Abgabe einer Sorgerechtserklärung des Kindesvaters: Übermittlung an beide Elternteile, ansonsten nur an die Mutter.

Im Aufnahmebogen der Schule kann die Frage nach dem Sorgerecht beispielsweise in folgender Form aufgenommen werden:

"Bei Alleinerziehenden: Haben Sie das alleinige Sorgerecht? Ja/Nein (Bitte Gerichtsurteil vorlegen)".

Das Urteil ist keinesfalls zur Schülerakte zu nehmen! Die Vorlage des Nachweises der Sorgeberechtigung kann durch das Schulverwaltungspersonal auf dem Aufnahmebogen vermerkt werden.

"Bei Lebensgemeinschaften: Hat der Vater eine Sorgerechtserklärung abgegeben: Ja/Nein".

In diesen Fällen kann ebenfalls die Vorlage eines entsprechenden Nachweises erbeten werden. Auch dieser

Nachweis ist nicht zur Schülerakte zu nehmen! Liegt keine Sorgerechtserklärung vor, wollen aber beide Lebenspartner über die schulischen Leistungen des gemeinsamen Kindes informiert werden, ist die schriftliche Einverständniserklärung der Mutter erforderlich. Diese ist dann zur Schülerakte zu nehmen.

Darf die Schule Informationen über das Leistungsverhalten volljähriger Schülerinnen und Schüler an deren Eltern übermitteln?

Eine Übermittlung dieser Informationen darf an Eltern volljähriger Schülerinnen und Schüler nur erfolgen, soweit die Schülerinnen und Schüler einer solchen Datenübermittlung nicht generell oder im Einzelfall widersprechen. Die Schülerinnen und Schüler sind auf das Widerspruchsrecht rechtzeitig, im Regelfall zu Beginn des Schuljahres, in dem das 18. Lebensjahr vollendet wird, schriftlich hinzuweisen. Erheben sie Widerspruch, sind die Eltern hierüber zu unterrichten (vgl. § 31 SchulG).

Darf privat beschaffte/bezahlte Software auf Lehrkräfte-Endgeräten eingesetzt werden?

Die von Lehrkräften privat beschaffte und bezahlte Software darf unter bestimmten Voraussetzungen auch weiterhin eingesetzt und auf Lehrkräfte-Endgeräten installiert werden. Im Folgenden wird davon ausgegangen, dass es sich um pädagogisch-didaktische Software handelt. Der Einsatz von Schulverwaltungssoftware unterliegt eigenen Regelungen.

In jedem Fall ist der Einsatz der Software ist nur mit Genehmigung der Schulleitung zulässig. Diese prüft und bewertet vorab, ob ein datenschutzkonformer Einsatz möglich ist.

Unproblematisch zulässig ist dies, soweit mit der Software keine personenbezogenen Daten verarbeitet werden. Etwa, wenn die Software zur Erstellung von Arbeitsblättern genutzt wird.

Wenn mit dieser Software personenbezogene Daten verarbeitet werden, ist darauf zu achten, dass die datenschutzrechtlichen Voraussetzungen für den Einsatz der Software gegeben sind. Die Gesamtverantwortung hierfür trägt gemäß § 2 Abs. 1 SchulDSVO die Schulleitung. Die Einhaltung der datenschutzrechtlichen Vorgaben liegt aber bei allen in der Schule tätigen Personen.

Ein Anspruch auf Erstattung der Kosten für die Software besteht nicht.

Zur Installation der Software wird auf das Endgeräte FAQ der IQSH-Medienberatung verwiesen, da diese vom Gerät und der jeweiligen Software abhängig ist.

Die Schule will für die Schulverwaltung mit Einwilligung der Betroffenen mehr Informationen über Schülerinnen, Schüler oder Eltern erheben, als in § 30 Abs. 1 SchulG in Verbindung mit der Anlage 2 der SchulDSVO vorgesehen. Ist das möglich?

In § 30 Abs. 1 Satz 2 SchulG ist präzise und abschließend aufgeführt, welche Kategorien von Daten von der Schule verarbeitet werden dürfen. Die Details zu den einzelnen Kategorien finden sich in der Anlage 2 der SchulDSVO. Weitere Daten können nur mit Einwilligung des oder der Betroffenen erhoben werden (Artikel 6 Absatz 1 Buchst. a DSGVO). Dies ist aber nur im Einzelfall zulässig. Die Einwilligung darf allerdings nicht genutzt werden, um ein bestehendes Verbot zu umgehen. Eine regelmäßige Erhebung von Daten, die über das Datenprofil

von § 30 Abs. 1 SchulG i. V. m. Anlage 2 SchulDSVO hinausgehen, ist unzulässig. Zwar ist die Schriftlichkeit von Einwilligungen nicht mehr explizit vorgeschrieben. Artikel 7 Absatz 1 EU-Datenschutz-Grundverordnung (DSGVO) verlangt jedoch vom Verantwortlichen den Nachweis, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Dies ist im Grundsatz jedoch nur - wie bisher - mit einer Einwilligung in Schriftform möglich. Die Einwilligung kann in papierener oder in elektronischer Form (z. B. per E-Mail) eingeholt werden. Wichtig ist, dass mit der Einholung der Einwilligung auch eine umfassende Information der betroffenen Person nach Artikel 13 DSGVO erfolgt.

Hinweise zur Gestaltung einer Einwilligung sind unten als Download verfügbar. Hinweise zur Erfüllung der Informationspflichten sind auf den Seiten des Unabhängigen Landeszentrums für Datenschutz (ULD) unter der Bezeichnung „Datenschutz-Steckbrief“ herunterladbar.
[Datei] Hinweise zur Gestaltung + Mustereinwilligung

Dürfen die Noten von Klassenarbeiten von den Lehrkräften öffentlich vor den Schülerinnen und Schülern verkündet werden?

Bei den Ergebnissen von Klassenarbeiten handelt es sich um personenbezogene Daten. Das Verlesen der einzelnen Noten vor der versammelten Klasse stellt eine Datenübermittlung an Einzelpersonen dar. Die Übermittlung von personenbezogenen Daten an Einzelpersonen ist jedoch nur mit Einwilligung der oder des Betroffenen zulässig. Das Einholen pauschaler Einwilligungen für diesen Zweck, z. B. bereits bei der Aufnahme der Schülerinnen und Schüler, ist unzulässig. Einwilligungen sind für den Einzelfall einer Datenverarbeitung (in diesem Falle einer Datenübermittlung) einzuholen. Dabei sind Betroffene auch auf ihr jederzeitiges Widerrufsrecht hinzuweisen (Widerrufsrecht nach Art. 7 Abs. 3 DSGVO). Soll die Notenverkündung aus pädagogischen Gründen erfolgen, ist es ausreichend einen Notenspiegel zu erstellen. Jede/r Schülerin/Schüler kann damit für sich feststellen, wo sie/er leistungsmäßig in der Klasse steht. In bestimmten Fällen kann es aus pädagogischer Sicht möglicherweise ratsam sein, statt des Notenspiegels auch nur die Durchschnittsnote einer Klassenarbeit bekannt zu geben. Auch in diesem Fall können sich Schülerinnen und Schüler leistungsmäßig einordnen.

Dürfen die Schulen private Telefonnummern ihrer Lehrkräfte ohne deren Einwilligung an die Eltern weitergeben?

Eltern müssen die Möglichkeit haben, Kontakt zu den Lehrkräften herzustellen, die ihre Kinder unterrichten. Die Schule muss deshalb sicherstellen, dass dies möglich ist.

Allerdings ist eine Übermittlung von Adressdaten der Lehrkräfte (wozu auch die Telefonnummern gehören) nach § 9 Abs. 4 SchulDSVO nur an die Klassenelternbeiräte zulässig und nur dann, wenn die Lehrkräfte in die Übermittlung vorher eingewilligt haben (idealerweise schriftlich - Nachweisbarkeit). Es empfiehlt sich deshalb seitens der Schulleitung unmittelbar nach der Zusammenstellung der Klassen, die unterrichtenden Lehrkräfte zu fragen, ob sie mit der Übermittlung ihrer privaten Adress- und Telefondaten einverstanden sind. Nach der Wahl der Elternvertretung können diese Daten unmittelbar an den Klassenelternbeirat übermittelt werden, von dem die Eltern die Informationen dann bei Bedarf erhalten.

Dürfen Klassenelternbeiräte an Zeugniskonferenzen teilnehmen und hierfür im Vorwege Kenntnis von den Zeugnisnoten aller Kinder der Klassengemeinschaft erhalten?

Die Tätigkeit als Elternvertretung wird ehrenamtlich ausgeübt. Bei der Erfüllung ihrer Aufgaben sind die Elternvertretungen zur Verschwiegenheit verpflichtet (§ 76 Abs. 1 SchulG i. V. m. §§ 95 und 96 des Landesverwaltungsgesetzes). Weitere Informationen zur Elternmitwirkung und auch zu den datenschutzrechtlichen Pflichten hat das Institut für Qualitätsentwicklung an Schulen SH (IQSH) in einer Broschüre veröffentlicht. Dort findet sich auch ein Muster für die erforderliche Verschwiegenheitserklärung.

Diese Verpflichtung erstreckt sich auch auf die Zeit nach Beendigung dieser Aufgabe. Die Schule muss also die Elternbeiräte auf deren Verschwiegenheitspflicht hinweisen. Es empfiehlt sich, dies in Form eines Merkblattes vorzunehmen, dessen Erhalt von jedem Elternbeiratsmitglied schriftlich zu bestätigen ist. Diese Bestätigung ist von

der Schule zu den Akten zu nehmen.

Die oder der Vorsitzende des Klassenelternbeirates nimmt nach § 65 Abs. 4 SchulG mit beratender Stimme an der Zeugniskonferenz teil. Die Teilnahme erfolgt im Rahmen der Aufgabe, das Interesse und die Verantwortung der Eltern für die Erziehung zu wahren und zu pflegen (§ 70 Abs. 3 Nr. 2 SchulG). Dazu kann es erforderlich sein, dass ihr oder ihm die Noten aller Kinder der Klassengemeinschaft bekannt gemacht werden.

Dabei ist es ausreichend, wenn ihr oder ihm unmittelbar zu Beginn der Konferenz eine Notenliste zur Einsichtnahme ausgehändigt wird. Es gibt keine sachliche Notwendigkeit und auch keine rechtliche Rechtfertigung dafür, vor der Konferenzeröffnung entsprechende Listen auszulegen, damit dem Elternbeirat eine angemessene Zeit zur Vorbereitung bleibt. Es besteht auch keine Notwendigkeit, dass diese Listen und/oder andere mit der Konferenz in Zusammenhang stehende personenbezogene Unterlagen bei den Elternvertretern verbleiben. Nach Abschluss der Konferenz sind diese Unterlagen deshalb wieder an die Konferenzleiterin oder den Konferenzleiter auszuhändigen.

Dürfen Streaming-Dienste im unterrichtlichen Kontext eingesetzt werden?

Ob ein Musik- oder Videostreamingdienst für pädagogische Zwecke genutzt werden darf, hängt einerseits vom Dienst selbst ab, aber auch vom konkreten Nutzungsszenario. Das Geschäftsmodell vieler Streamingdienste basiert auf dem Sammeln personenbezogener Daten der Nutzenden, um Profile zu bilden und die Daten für eigene Zwecke zu verarbeiten oder an Werbetreibende zu verkaufen. Diese Daten werden zudem je nach Anbieter häufig in sogenannten Drittländern, also Ländern außerhalb der EU und des Europäischen Wirtschaftsraums (EWR), verarbeitet. Hierfür existiert im schulischen Kontext i.d.R. keine gültige Rechtsgrundlage. Ein rechtskonformer Einsatz gängiger Streamingdienste ist daher, mit Ausnahme eng begrenzter Nutzungsszenarien, nicht möglich.

Das Vorführen (per Beamer/Smartboard) eines gestreamten Videos, idealerweise mit einem schulischen (nicht personalisierten Endgerät), kann aus Datenschutzsicht als unkritisch angesehen werden. Wenn ein privates Endgerät verwendet wird, sollte der Lehrkraft je nach Anbieter das Risiko des Datenabflusses in Drittländer bewusst sein.

Beim Aufrufen eines Streamingdienstes durch die Schülerinnen und Schüler über einen Browser im privaten (inkognito) Modus, mit schuleigenen, nicht personalisierten Endgeräten im Netz der Schule besteht kein signifikantes datenschutzrechtliches Risiko. Der Browser muss so konfiguriert sein, dass keine Werbung angezeigt wird (s.u.). Außerdem dürfen die Schülerinnen und Schüler nicht zeitgleich bei diesem oder einem anderen Dienst des gleichen Anbieters angemeldet sein, da der Streamingdienst hierdurch i.d.R. Zugriff auf personenbezogene Daten der Schülerinnen und Schüler erhält. Dies gilt ebenso für Webseiten, die Streamingdienste, z.B. über einen embedded Player, einbinden.

Die Aufforderung an Schülerinnen und Schüler, ein gestreamtes Video oder Musikstück (bspw. über einen Link in einem digitalen Arbeitsblatt) im Rahmen des Unterrichts (in Präsenz und insbesondere auch im Homeschooling oder als Hausaufgabe) über ein personalisiertes Endgerät anzusehen, ist datenschutzrechtlich unzulässig. Die Bereitstellung von Musik/Videos über Plattformen, die personenbezogene Daten in Drittländern verarbeiten, z.B. durch die Lehrkraft und die Aufforderung, diese anzuschauen, ist aus den genannten Gründen ebenfalls unzulässig.

Wenn unterstützende Videos auf profilbildenden Plattformen zur freiwilligen Betrachtung empfohlen werden, muss

der Fürsorgepflicht der Schule dadurch Rechnung getragen werden, dass die Schülerinnen und Schüler bzw. deren Eltern darauf hingewiesen werden, dass mit dem freiwilligen Aufrufen der Videos eine unbemerkte und nahezu unkontrollierbare Datensammlung einhergeht.

Darüber hinaus gilt, dass neben dem Datenschutz auch immer sonstige rechtliche Regelungen wie das Urheberrecht und das Werbeverbot in Schule (§29 SchulG SH) zu beachten sind. Bei browserbasierten Diensten können Werbeverbot und Datenschutz ggf. durch den Einsatz entsprechender AddOns unterstützt werden, sofern die Nutzungsbedingungen des jeweiligen Dienstes dies nicht untersagen. Eine in den Nutzungsbedingungen ggf. aufgeführte Altersgrenze ist für den unterrichtlichen Einsatz nicht relevant, solange die Auswahl der Inhalte, durch die Lehrkräfte erfolgt und damit bspw. der Jugendschutz gewährleistet wird und ansonsten die oben aufgeführten Rahmenbedingungen berücksichtigt sind.

Dürfen Vertretungspläne auf der Homepage der Schule veröffentlicht werden?

Vertretungspläne dienen der Organisation des Schulbetriebes. Sie informieren die Schülerinnen und Schüler über Veränderungen in den Stundenplänen. Vertretungspläne werden üblicher Weise in den Räumlichkeiten der Schulen ausgehängt und sind damit im Grundsatz nur den Adressaten (Schülerinnen, Schülern, ggf. Eltern und den Lehrkräften) zugänglich. Diese Veröffentlichung von Vertretungsplänen ist zur Organisation des Schulablaufes erforderlich. In diesem Fall ist es datenschutzrechtlich grundsätzlich zulässig, dass die Vertretungspläne Namen von Lehrkräften oder deren entsprechende Kürzel enthalten. Die Gestaltung der Vertretungspläne liegt letztlich im organisatorischen Entscheidungsbereich der Schulleitung. Dabei muss im Einzelfall bewertet werden, ob auf die Angabe des Namens einer Lehrkraft verzichtet werden kann. Ist die Schulleitung der Auffassung, dass die Namensnennung unverzichtbar ist, so müssen es sich die Lehrkräfte gefallen lassen, dass ihre Namen genannt werden, da diese im Zusammenhang mit ihrer (Lehr-)Funktion stehen.

Die Veröffentlichung von Vertretungsplänen auf der schuleigenen Homepage mit Nennung der Namen der Lehrkräfte ist hingegen aus schulorganisatorischen Gründen in der Regel zunächst nicht erforderlich, weil die Schülerinnen und Schüler anhand der Vertretungspläne nur Informationen erhalten müssen, ob sich Fächer verschieben oder sich der Stundenplan verändert hat.

Darüber hinaus ist zu bedenken, dass durch die Veröffentlichung von Vertretungsplänen auf der Schulhomepage nicht nur der eingeschränkte Adressatenkreis der Schulöffentlichkeit Zugang zu diesen Informationen hat, sondern jeder Nutzer des Internets weltweit. Wegen der fehlenden Erforderlichkeit und des unbestimmten Adressatenkreises ist eine Veröffentlichung von Namen der Lehrkräfte daher unzulässig.

Idealerweise sollten die Vertretungspläne in einem gesonderten Bereich der Schulhomepage untergebracht werden, der nur befugten Nutzenden unter Eingabe eines Passwortes zugänglich ist und der nicht für die Web-Öffentlichkeit zur Verfügung steht. Auf diese Weise ließe sich der Zugriff auf solche Daten im Ansatz auf die Schulöffentlichkeit beschränken. Allerdings sollten auch hier maximal die Namenskürzel der Lehrkräfte angegeben werden.

Beabsichtigt die Schulleitung dennoch, zusammen mit den Vertretungsplänen auch personenbezogene Daten der Lehrkräfte zu veröffentlichen, so muss eine Einwilligung der Betroffenen eingeholt werden.

Eine Kirche möchte die Eltern mit ihren Kindern zum (Einschulungs-)Gottesdienst einladen. Dürfen die Schulen deren Namen und Adressen für diesen Zweck an die Kirche weitergeben?

Nein. Die Religionsgemeinschaften zählen nicht zu den öffentlichen Stellen im Sinne des Landesdatenschutzgesetzes und des Schulgesetzes (vgl. § 2 Abs. 1 LDSG). Sie sind insofern wie private Stellen zu behandeln, auch wenn sie einen öffentlich-rechtlichen Status haben. Eine Datenübermittlung an die Kirchengemeinden ist nur zulässig, wenn die Betroffenen im Einzelfall ihre Einwilligung erteilt haben.

Viele Schulen pflegen gute Kontakte zu den Kirchengemeinden und der Einschulungsgottesdienst hat vielerorts Tradition. Datenschutz soll hier kein Hinderungsgrund sein: Die Schulen können die Einladungen der Kirchengemeinden zu den Gottesdiensten für diese versenden. In diesem Falle erfolgt keine Datenübermittlung; das Ergebnis der Einladung wird trotzdem erreicht.

Gehören sonderpädagogische und andere schulärztliche Gutachten in die Schülerakte?

Grundsätzlich werden Gutachten und Befunde nicht in der Schülerakte abgelegt. Bei einer Pflichtuntersuchung (bspw. Schuleingangsuntersuchung, Feststellung sonderpädagogischer Förderbedarf) darf die untersuchende Stelle der Schule zunächst nur das Ergebnis mitteilen (§ 27 Abs. 4 S. 1 SchulG). Wenn es im Einzelfall für die Beschulung, insbesondere für die individuelle Förderung, erforderlich ist, weitere Daten über Entwicklungsauffälligkeiten und gesundheitliche Beeinträchtigungen zu verarbeiten, dürfen diese Daten dann ergänzend in der Schülerakte gespeichert werden (§ 30 Abs. 1 Nr. 1 SchulG).

Besteht ein sonderpädagogischer Förderbedarf, muss vom Förderzentrum eine separate "sonderpädagogische Schülerakte" angelegt werden. In dieser Akte werden die Gutachten und die weiteren Unterlagen gespeichert. Diese Akte wird ausschließlich im Förderzentrum geführt (§ 7 Abs. 2 SchulDSVO). In der Schülerakte wird nur der von Schule und Förderzentrum erarbeitete Lern-/Förderplan abgelegt (§ 7 Abs. 1 Nr. 5 SchulDSVO).

Im Falle einer inklusiven Beschulung führt diese Schule nur die "normale Schülerakte". Bei einem Schulwechsel verbleibt diese Schülerakte in der bisher besuchten Schule (§ 9 Abs. 1 SchulDSVO).

Wenn ein Wechsel von einem Förderzentrum zum nächsten erfolgt (bei Förderzentren mit eigenen Schülerinnen und Schülern bzw. bei Wechsel der Zuständigkeit), wird die komplette "sonderpädagogische Schülerakte" an das neu zuständige Förderzentrum übergeben (§ 9 Abs. 1 letzter Satz SchulDSVO).

Haben ehemalige Schülerinnen und Schüler ein Recht auf Einsicht in ihre Abschlussarbeiten und ab wann steht ihnen dieses Recht zu?

Nach Artikel 15 Abs. 1 DSGVO hat die betroffene Person ein Recht auf Auskunft. Gemäß § 9 Abs. 4 Landesdatenschutzgesetz (LDSG) kann der betroffenen Person (z. B. Abiturientin oder Abiturient) anstelle einer Auskunft auch Akteneinsicht gewährt werden, wenn die Daten in Akten (also in Papierform) enthalten sind.

Abschlussarbeiten werden in papierener Form gespeichert. Somit findet diese Vorschrift Anwendung. Ehemalige Schülerinnen und Schüler können somit nach Abschluss des (Prüfungs-)Verfahrens, also nach Aushändigung des Abschlusszeugnisses, dieses Akteneinsichtsrecht geltend machen.

Darüber hinaus verpflichtet Artikel 15 Abs. 3 DSGVO den Verantwortlichen (die Schule), der betroffenen Person eine (kostenfreie) Kopie der personenbezogene Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen, wenn die betroffene Person dies verlangt.

In welcher Weise sind externe Mitarbeitende, die die schulische Arbeit unterstützen sollen, zur Verschwiegenheit zu verpflichten?

Zunehmend werden die schulischen Aufgaben nicht mehr nur von den Lehrkräften und dem Verwaltungspersonal (Schulsekretärinnen und Hausmeister) wahrgenommen, sondern auch von externen Kräften unterstützt.

Mittlerweile werden in vielen Schulen Schulassistentinnen und Schulassistenten eingesetzt. Diese Personen sind entweder beim Land, bei Schulträgern oder bei anderen Trägern angestellt. In diesen Fällen, sind diese bereits im Rahmen dieser Anstellung arbeitsvertraglich zur Verschwiegenheit verpflichtet. Die Schulleiterin oder Schulleiter hat diese Assistenzkräfte daneben unmittelbar nach Dienstbeginn in der Schule gem. § 3 SchulDSVO über die Pflicht zur Beachtung des Datenschutzes zu belehren. Gleiches gilt für Schulbegleiterinnen und Schulbegleiter.

Die Schulsozialarbeiterinnen und Schulsozialarbeiter, die in den Schulen zum Einsatz kommen, müssen nicht belehrt werden. Für diese gelten in der Regel die Verschwiegenheitspflichten aus § 203 StGB (sog. Patientengeheimnis). Daneben sind sie durch ihre Anstellungsträger zur Verschwiegenheit verpflichtet.

Ferner sind Personen zur Durchführung schulischer Veranstaltungen außerhalb des lehrplanmäßigen Unterrichts (z. B. offener Ganztag) und Unterstützungskräfte bei schulischen Veranstaltung im Einsatz (§ 34 Abs. 6 und 7 SchulG). dieser Personenkreis ist ebenfalls nach § 3 SchulDSVO förmlich zu belehren.

In vielen Schulen sind daneben aber auch Honorarkräfte tätig, die z. B. den Musikunterricht wahrnehmen. Ferner sind in den Schulen Praktikantinnen und Praktikanten sowie Studierende zu Gast, die am Unterricht teilnehmen und dabei auch Kenntnis von personenbezogenen Daten der Schülerinnen und Schüler erhalten.

Dieser Personenkreis steht in keinem Beschäftigungsverhältnis mit dem Land oder dem Schulträger. Arbeitsvertraglich vereinbarte Verschwiegenheitsverpflichtungen, wie sie für Landesbedienstete oder kommunale Mitarbeiter üblich sind, existieren demnach in der Regel nicht.

Es muss jedoch sichergestellt werden, dass dieses Personal die bekannt werdenden personenbezogenen Daten vertraulich behandelt. Aus diesem Grund sind sie von der Schulleitung schriftlich zur Verschwiegenheit zu verpflichten. Ein entsprechendes Muster einer solchen Verschwiegenheitserklärung steht zum Download bereit.
[Datei] Muster Verschwiegenheitserklärung

In welcher Weise sind nicht mehr benötigte personenbezogene Unterlagen über Schülerinnen und Schüler (z.B. Klausurenhefte, Klassenlisten, Zeugnislisten usw.) datenschutzgerecht zu vernichten?

§ 10 SchulDSVO schreibt vor, dass personenbezogene Schülerdaten zu bestimmten Fristen zu vernichten sind. Die Vernichtung papierener Unterlagen hat dabei so zu erfolgen, dass Unbefugte keine Kenntnis von diesen Daten erlangen können. Eine Entsorgung über Altpapiercontainer ist nicht zulässig. Vor einer Vernichtung sind allerdings alle Unterlagen dem zuständigen Archiv zur Übernahme anzubieten (§ 10 SchulDSVO).

Für eine datenschutzgerechte Vernichtung dieser Unterlagen gibt es folgende Möglichkeiten:

1. Beauftragung eines nach DIN 66399 zertifizierten Betriebes, der sich auf die Vernichtung solcher Unterlagen spezialisiert hat. Diese Firmen stellen sicher, dass die Unterlagen vor ihrer Vernichtung (Verbrennung, Zerkleinerung u. ä.) nicht durch eigene Mitarbeiter oder andere unbefugte Dritte zur Kenntnis genommen werden können. Hierbei handelt es sich datenschutzrechtlich um Auftragsverarbeitung. Hierfür sind die Vorgaben des Art. 28 DSGVO zu beachten. Die Auftragsverarbeitung verlangt eine sorgfältige Auswahl des Auftragnehmers sowie die schriftliche Festlegung der Art und Weise der Aktenvernichtung und deren Kontrolle.
2. Vernichtung der Unterlagen durch eigene Mitarbeiterinnen oder Mitarbeiter der Schule oder des Schulträgers mittels vorhandener Papierschredder. In diesem Falle muss sichergestellt sein, dass bis zur endgültigen Vernichtung zwischengelagerte Unterlagen nicht für Unbefugte zugänglich sind und die Schredder die erforderliche Schutzklasse und Sicherheitsstufe nach DIN 66399 erfüllen. Empfehlung: Schutzklasse 2, Sicherheitsstufe 4-5.
3. Vernichtung über vom Schulträger bereitgestellte Sammelcontainer ("Silberlinge").

In jedem Falle ist die Zuständigkeit für die Aktenvernichtung innerhalb der Schule durch die Schulleitung schriftlich zu regeln (wer sortiert die zu vernichtenden Unterlagen aus, wer erteilt den Auftrag zur Vernichtung, wer kontrolliert die ordnungsgemäße Durchführung).

Kann SchulCommSy auch für Schulverwaltungszwecke (digitales Lehrerzimmer, Austausch von Informationen, Protokolle) genutzt werden?

Schulen benötigen technische Verfahren für eine schnelle Kommunikation sowie den Austausch von Dokumenten für Unterrichtszwecke zwischen Schulleitung, Lehrkräften, Schülerinnen und Schülern. Immer mehr wird es daneben erforderlich, dass Lehrkräfte für dienstliche Zwecke auch Zugang zu Informationen (z.B. Klassenlisten,

Konferenzprotokollen usw.) erhalten, die ansonsten nur auf den Schulverwaltungsrechnern (LanBSH-Rechner) gespeichert werden dürfen.

Das IQSH stellt mit dem Verfahren SchulCommSy allen Schulen als Landeslösung eine über das Internet erreichbare technische Lösung kostenfrei zur Verfügung. Das IQSH übernimmt für die Schulen die Aufgabe, die Datensicherheit des Gesamtverfahrens (Anwendung und Server) zu gewährleisten. Dies hat für die Schulen gegenüber anderen im Einsatz befindlichen Verfahren den Vorteil, dass sie von dieser ihnen ansonsten obliegenden Aufgabe entlastet werden.

Unter der Voraussetzung, dass die Vorgaben zur strikten Trennung von Schulverwaltungsdaten (Instanz I) und Daten für pädagogisch-didaktische Zwecke (Instanz II) eingehalten werden, ist ein datenschutzkonformer Einsatz und eine Verarbeitung personenbezogener Daten im in der Nutzungsordnung festgelegten Umfang möglich. Für die Einhaltung der Vorgaben ist die Schulleitung verantwortlich.

Das IQSH hält ein mit dem ULD und dem Datenschutzbeauftragten für die öffentlichen Schulen abgestimmtes Dokumentenpaket vor. Dieses Paket enthält alle Unterlagen, die für den datenschutzrechtlich einwandfreien Betrieb von SchulCommSy erforderlich sind.

Die für die Datenverarbeitung verantwortliche Schulleitung kann somit das Verfahren mit wenigen noch notwendigen Maßnahmen ohne großen eigenen Aufwand in datenschutzkonformer Weise einführen.

Für die Beratung zum Verfahren und der Bereitstellung des Dokumentenpakets steht das IQSH zur Verfügung: https://www.secure-lernnetz.de/helpdesk/ (Bereich Schulportal -> SchulCommSy SH)

Kindergeldkassen (der Arbeitsämter) und Rentenversicherungsträger fordern bei der Schule personenbezogene Daten über Schulbesuchszeiträume bzw. über die Tatsache des Schulbesuchs an. Darf die Schule diese Daten übermitteln?

Nein. Kindergeld und Renten werden von Sozialleistungsträgern gezahlt, die die Regelungen des Sozialgesetzbuches zu beachten haben. Nach diesen Vorschriften sind die für die Leistungsgewährung erforderlichen Informationen direkt bei den Leistungsempfängern zu erheben. Diese haben eine Mitwirkungspflicht. Daher besteht grundsätzlich keine Erforderlichkeit für die Datenübermittlung seitens der Schule. § 30 Abs. 3 S. 1 SchulG findet somit keine Anwendung. Allerdings kann es in Ausnahmefällen durchaus keine andere Möglichkeit für die genannten Stellen geben, als die Daten von der Schule anzufordern. Die anfordernde Stelle ist dann jedoch verpflichtet zu begründen, warum es nicht möglich ist, die Daten beim Betroffenen zu erheben. Darüber hinaus muss die Schule die Übermittlung aktenkundig machen (§ 30 Abs. 3 letzter Satz SchulG).

Lehrkräfte im Vorbereitungsdienst und Lehramtsstudierende wollen zu eigenen Ausbildungszwecken Schülerdaten verwenden. Was ist dabei zu beachten?

§ 6 Abs. 1 SchulDSVO erlaubt dem genannten Personenkreis die Einsichtnahme in die in der Schule gespeicherten Daten. Dies kann aber nur gelten, soweit diese Personen "aktiv" im Unterrichtsbetrieb eingebunden sind. Werden darüber hinausgehend Informationen aus Schülerakten zur Anfertigung von Prüfungsarbeiten o. ä. verwendet, so sollten die Daten der Schülerinnen und Schüler nur mit Einwilligung der Eltern oder der volljährigen Schülerinnen und Schüler personenbezogen genutzt werden. Der § 32 SchulG regelt, dass für Praktika und Prüfungsarbeiten im Rahmen der Lehrkräfteausbildung personenbezogene Daten der Schülerinnen und Schüler sowie Eltern verarbeitet werden dürfen. Hierbei sind die datenschutzrechtlichen Vorgaben zur Einwilligung (Artikel 7 DSGVO), zur Information der Betroffenen (Artikel 13 DSGVO) und hinsichtlich der Datensicherheit (Artikel 32 DSGVO) zu beachten.

Muss ich für jeden digitalen Dienst eine umfangreiche Dokumentation erstellen?

Entsprechend § 2 SchulDSVO trägt die Schulleitung die Verantwortung für die Organisation und Einhaltung des Datenschutzes in der Schule. Dazu gehört auch das Anfertigen bzw. Inkraftsetzen der datenschutzrechtlichen Dokumentation. Die digitalen Dienste, die in der Schule genutzt werden, lassen sich aus Datenschutzperspektive in

drei Kategorien unterteilen.

Kategorie 1 - kein Personenbezug

Ein digitaler Dienst muss nur datenschutzrechtlich dokumentiert werden, wenn das Datenschutzrecht anzuwenden ist, d.h. wenn personenbezogene Daten verarbeitet werden. Der Begriff Verarbeitung umfasst u.a. das Erfassen, Übertragen, Speichern und Löschen von Daten. Personenbezogene bzw. personenbeziehbare Daten sind bspw. Name, Kontaktdaten, IP-Adressen und Leistungsdaten.

Kategorie 2 - geringes Schadensrisiko

Das mit der Verarbeitung personenbezogener Daten einhergehende Risiko für die Rechte und Feiheiten der betroffenen Personen, kann durch das Ergreifen geeigneter technischer und/oder organisatorischer Maßnahmen (TOM) reduziert werden. Erfordert beispielsweise eine Lernanwendung nur sehr wenige personenbezogene Daten (z. B. ein Pseudonym und die IP-Adresse), dann kann der Personenbezug gegenüber dem Anbieter verschleiert werden, indem die ausschließliche Nutzung der Anwendung über das Schul-WLAN, auf schuleigenen, nicht-personalisierten Geräten vorgeschrieben wird. Digitale Dienste, die aufgrund eines solchen konkreten Nutzungsszenarios nur ein geringes datenschutzrechtliches Risiko bergen, bezeichnen wir als „Anwendungen mit geringem Datenschutzrisiko“. Für diese Dienste steht ein Dokumentenpaket zur Verfügung, welches mit wenigen Basis-Dokumenten eine Liste von Anwendungen abdeckt. Die Schulleitung kann mit Hilfe der im Dokumentenpaket beigefügten Orientierungshilfe prüfen und entscheiden, ob ein digitaler Dienst unter die Anwendungen mit geringem Datenschutzrisiko fällt. Dabei ist es ausreichend, wenn entsprechende Dienste in die schulinterne Liste übernommen und die Dokumentation an wenigen Stellen angepasst wird. Somit entfällt der Aufwand für jeden Dienst eine eigene Dokumentation anzufertigen.

Kategorie 3 - erhöhtes Schadensrisiko

Wird ein digitaler Dienst, der personenbezogene Daten verarbeitet, in nicht unerheblichem Umfang in der Schule verwendet, so muss für diesen eine spezifische datenschutzrechtliche Dokumentation angefertigt bzw. in Kraft gesetzt werden. Dies ist beispielsweise der Fall, wenn der Einsatz mit einer Auftragsverarbeitung einher geht. Für die Landeslösungen und für einige häufig angefragte Dienste stehen fertige Musterdokumentenpakete zur Verfügung. Für die Neuerstellung noch nicht dokumentierter Dienste können diese als Vorlagen genutzt werden. Allgemeine Hinweise zum Erstellen der datenschutzrechtlichen Dokumentation gibt es in diesem FAQ-Eintrag.

Nutzung privater Endgeräte - Was ist bei der Beantragung, Genehmigung und Nutzung zu beachten?

Vorbemerkung:

Private Endgeräte dürfen für die **dienstliche Verarbeitung personenbezogener Daten** nur verwendet werden, wenn hierfür eine **Genehmigung auf Antrag der Lehrkraft durch die Schulleitung** erteilt wurde. Eine solche Genehmigung stellt nach der Neuerung der SchulDSVO im Juli 2022 **nur noch die Ausnahme** dar. Durch die vom Land sukzessive **Bereitstellung dienstlicher Endgeräte** für die Arbeitsverrichtung werden zunehmend keine Genehmigungen mehr für private Endgeräte erteilt. Des Weiteren **erlischt die bisher erteilte Genehmigung** nach

§14 Abs. 7 SchulDSVO sobald ein dienstliches Endgerät zur Verfügung steht. Für den Ausnahmefall bleibt das alte Verfahren vorerst dennoch bestehen. Die Antragstellung erfolgt eigenverantwortlich durch die Lehrkraft (Bringschuld). Die Genehmigung ist maximal 4 Jahre gültig. Sie muss erneut beantragt werden, wenn sich Änderungen am Antragsgegenstand ergeben (neue Programme, neues Endgerät).

Antrags- und Genehmigungsverfahren:

Die Rahmenbedingungen zur Nutzung privater Endgeräte ergeben sich formal aus dem § 14 SchulDSVO. Die Lehrkraft sichert in Ihrem Antrag (Musterformular im Anhang) verschiedene organisatorische Maßnahmen (nur dienstliche Verarbeitung, keine Offenlegung gegenüber Dritten, Wahrung der Vertraulichkeit, Ermöglichung der Einsichtnahme zu Kontrollzwecken gegenüber der Datenschutzaufsichtsbehörde und der Schulleitung, Mitteilung bei Änderungen des Antragsgegenstands) zu und verpflichtet sich darüber hinaus, angemessene Sicherheitsmaßnahmen (Artikel 32 DSGVO und § 30 Absatz 10 Schulgesetz) zu ergreifen und nur Programme zu verwenden, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten das erforderliche und angemessene Maß an Vertraulichkeit sicherstellen.

Damit beschränkt sich der Prüfaufwand durch die Schulleitung für die Erteilung der Genehmigung auf die im Antrag angegebenen Programme, mit denen die Lehrkraft **personenbezogene Daten** verarbeiten möchte (bspw. Office-Anwendungen für Listen, Zeugnisentwürfe, Gutachten etc., digitale Lehrerkalender) und das Betriebssystem des Endgerätes. Weitere Programme, die die Lehrkraft bspw. zur Unterrichtsvor- und Nachbereitung (Erstellung von Arbeitsblättern, Präsentationen, Klassenarbeiten etc.) oder im Unterricht (bspw. Simulationen, Visualisierung) einsetzen möchte und in denen **keine personenbezogenen Daten** bearbeitet werden, sind davon ausgenommen.

Prüfung folgender Punkte durch die Schulleitung auf Grund des Antrags:

- die installierte Betriebssystemversion muss aktuell sein
  - Windows 10 (https://docs.microsoft.com/de-de/windows/release-health/release-information)
  - Apple-macOS (https://support.apple.com/de-de/HT201260)
  - Apple iPad-OS (https://support.apple.com/de-de/guide/ipad/ipad213a25b2/ipados)
- die installierte Office Anwendung muss aktuell sein, damit sie noch mit Sicherheitsupdates versorgt wird. Sie muss lokal installiert sein.
- Beispiele:
  - LibreOffice (de.libreoffice.org)
  - OpenOffice (openoffice.org/de)
  - Microsoft Office 2013 (Ende des Supports am 11.04.2023)
  - Microsoft Office 2016 (14.10.2025)
  - Microsoft Office 2019 (14.10.2025)
  - Microsoft Office 2019 for Mac (10.10.2023)
- -> Quelle: https://docs.microsoft.com/de-de/lifecycle/products/?products=office&terms=Microsoft%20Office
- Office 365/Microsoft 365 darf für die **Verarbeitung personenbezogener Daten** nicht verwendet werden, da die Dokumentenbearbeitung/-speicherung bei Clouddiensten nicht zulässig ist (§14 Absatz 6 SchulDSVO). Hier muss die Lehrkraft dann parallel bspw. LibreOffice installieren.
- ältere Betriebssystemversionen (bspw. Windows 7) oder Officeanwendungen (bspw. MS Office 2010) dürfen nicht mehr eingesetzt werden, da hier der Support mit wichtigen Sicherheitsupdates ausgelaufen ist und somit auf Grund von Sicherheitslücken ein erhöhtes Risiko besteht.
- Bei Internetbrowsern, die bspw. für den Zugang zum E-Mailpostfach (@schule-sh.de -> verpflichtend zu nutzen für dienstliche Kommunikation), Schulportal, Lernmanagementsystem oder für Videokonferenzen eingesetzt werden, ist ebenfalls darauf zu achten, dass eine aktuelle Version installiert ist und aktuell gehalten wird:
  - Beispiele:

  - Edge (https://www.microsoft.com/de-de/edge)
  - Firefox (https://www.mozilla.org/de/firefox/new/)
  - Chrome (https://www.google.com/intl/de/chrome/)
- weitere von der Lehrkraft angegebene Programme müssen ebenfalls hinsichtlich der Aktualität und Sicherheit bewertet werden.
- Insbesondere für digitale Lehrerkalender gelten die in der Ergänzung zum Antragsformular aufgeführten Rahmenbedingungen/Einschränkungen.

Hinweise zur Nutzung privater Endgeräte für Lehrkräfte, die geeignet sind, die Forderungen des §14 SchulDSVO zu erfüllen und insgesamt, auch bei der privaten Nutzung, ein erhöhtes Sicherheitsniveau zu erreichen:

- Das Endgerät muss mit einem Zugangsschutz versehen sein (Fingerabdruck, Passwort mit min. 8 Zeichen -> Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen).
- Das Gerät muss auch bei kurzfristiger Abwesenheit gesperrt werden (Tastenkombination Windows+L, [ctrl]+Touch-ID-Sensor).
- Idealerweise wird ein zweites Benutzerkonto (dienstlich) angelegt, um die Vermischung privater und dienstlicher Daten zu verhindern.

- Dateien mit personenbezogenen Inhalten, das können auch E-Mailanhänge sein, sollten auf einem verschlüsselten, externen Datenträger (USB-Stick, Wechselfestplatte) abgelegt werden. Alternativ kann ein separater Ordner (verschlüsselter Container) auf dem Endgerät angelegt werden (bspw. der kostenlosen Open-Source-Verschlüsselungssoftware VeraCrypt -> https://www.veracrypt.fr/en/Downloads.html).
- Wenn vorhanden, sollte eine Festplattenverschlüsselung (bspw. Bitlocker bei Windows 10, FileVault bei MacOS) aktiviert sein.
- Eine Speicherung personenbezogener Daten bei Clouddiensten (insb. ICloud, GoogleDrive, Dropbox, OneDrive) ist nicht zulässig (vgl. §14 Abs. 6 SchulDSVO).

- Die installierte oder im Betriebssystem integrierte Antiviren-/Malware-/Firewallsoftware (bspw. Windows Defender) sollte regelmäßig, automatisch vollständige Scans des Rechners durchführen.
- Automatische Updates für das Betriebssystem, die Schutzsoftware und die genutzten Programme müssen aktiviert sein.
- Die Verbindung zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk der Schule, das eigene WLAN zuhause oder einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zur Verfügung stehenden Netzwerke (z.B. öffentliche Netzwerke in Bahnhöfen oder Städten), sollte keine Internetverbindung aufgebaut werden.
- Die Datenschutzeinstellungen des Betriebssystems sollten überprüft und angepasst werden (Tipps: https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/datenschutz-bei-windows-10-erhoehen-12154).
- Gleiches gilt für die Sicherheitseinstellungen des Internetbrowsers.

- Dateien sollten unter Beachtung des § 15 SchulDSVO regelmäßig gelöscht werden – auch aus dem Papierkorb.
- Für aufbewahrungspflichtige Daten (bspw. persönliche Notizen zur Dokumentation von Leistungsbewertungen) sollten regelmäßig Sicherungskopien auf verschlüsselten Wechseldatenträgern angefertigt werden.
- Digitale Lehrerkalender dürfen nur wie im Antrag vorgegeben genutzt werden (insb. Datenminimierung, Backups, Aufbewahrungspflichten, Verbot von Cloudspeicherung, keine Mehrgerätenutzung)
- Weitere Informationen zum Schutz von Endgeräten erhalten Sie beim Bundesamt für Sicherheit in der Informationstechnik (BSI) in der Rubrik „Basistipps zur IT-Sicherheit“.
- Wenn das Endgerät entsorgt werden soll, dann sollte sichergestellt sein, dass alle Daten auf der Festplatte sicher gelöscht sind. Ein einfaches Löschen in den „Papierkorb“ oder im Windows Explorer ist hierfür nicht ausreichend. Auf der BSI-Webseite „BSI für Bürger“ finden Sie Hilfestellungen und kostenfreie Werkzeuge zum sicheren Löschen Ihrer Daten: https://www.bsi-fuer-buerger.de/BSIFB/richtig_loeschen.

[Datei] Antrag zur Genehmigung der Nutzung privater Endgeräte durch Lehrkräfte

Private Nachhilfeeinrichtungen wollen von den die Schülerinnen und Schüler unterrichtenden Lehrkräften Informationen zum Lernverhalten erheben. Unter welchen Bedingungen wäre dies datenschutzrechtlich zulässig?

Schülerinnen und Schüler nehmen Nachhilfestunden bei privaten Anbietern in Anspruch, um ihre Leistungen in der Schule zu verbessern. Diese Anbieter wenden sich häufig direkt an die diese Schülerinnen und Schüler unterrichtenden Lehrkräfte, ohne die Anfrage über die Schulleitung zu stellen. Die Lehrkräfte werden gebeten, Informationen z. B. über bestehende Wissenslücken, das Lernverhalten, die Unterrichtsbeteiligung und das Verhalten im Unterricht an die private Einrichtung zu übermitteln. Die Kontaktaufnahme findet dabei entweder telefonisch oder mittels eines Formblattes statt.

Für die Übermittlung solcher Daten existiert im SchulG keine Rechtsgrundlage, so dass eine Übermittlung an eine private Einrichtung oder an eine Einzelperson in diesen Fällen nur mit der Einwilligung der oder des Betroffenen zulässig ist.

Somit ist die Übermittlung nur mit einer Einwilligung nach den Vorgaben des Artikel 7 DSGVO der oder des Betroffenen (in diesem Fall der Eltern) zulässig. Die Einwilligung ist von der Nachhilfeeinrichtung einzuholen und der Schule vorzulegen. Die Übermittlung der Informationen von der Schule an die Nachhilfeeinrichtung sollte ebenso wie das Vorliegen der Einwilligung aktenkundig gemacht werden. Erst nach der Entscheidung der Schulleitung zur Datenübermittlung, dürfen die Lehrkräfte der Schülerin oder des Schülers die Daten, für deren Übermittlung die Einwilligung erteilt wurde, an die Nachhilfeeinrichtung übermitteln. Ohne Genehmigung der Schulleitung würde die Lehrkraft gegen ihre Amtsverschwiegenheit verstoßen.

Stellt die Videoüberwachung in Schulen ein zulässiges Mittel dar, um Sachbeschädigungen und Diebstähle zu verhindern?

Nach § 14 Landesdatenschutzgesetz (LDSG) darf eine öffentliche Stelle u. a. zur Ausübung des Hausrechts öffentlich zugängliche Räume beobachten und auch unter bestimmten Voraussetzungen Videoaufzeichnungen vornehmen.

Immer häufiger wollen Schulen Videoüberwachung einsetzen, um Sachbeschädigungen oder Diebstähle in und an den Schulgebäuden einzudämmen. Unter datenschutzrechtlichen Gesichtspunkten stellt die Videoüberwachung jedoch einen schweren Eingriff in die Persönlichkeitsrechte der Betroffenen dar.

Aus diesem Grunde sollten vor dem Einsatz solcher Überwachungsanlagen zunächst alle anderen Möglichkeiten geprüft werden, um schädigende Handlungen zu unterbinden. Wenn z. B. immer wieder Diebstähle und Sachbeschädigungen an Fahrrädern auf dem Schulhof festgestellt werden, sollte zunächst geprüft werden, ob die Fahrräder nicht in einem anderen Bereich, beispielsweise unter Fenstern von Unterrichtsräumen, abgestellt werden können, also im Blickfeld der Lehrkräfte, Schülerinnen und Schüler. Finden Diebstähle innerhalb des Schulgebäudes statt, beispielsweise von Kleidungsstücken, die auf den Fluren hängen, so wäre es denkbar, dass die Schülerinnen und Schüler diese mit in die Unterrichtsräume nehmen. Bei vermehrten Vorkommnissen könnte unter pädagogischen Aspekten überlegt werden, die Polizei zu bitten, in den Klassen über die strafrechtlichen Konsequenzen solchen Verhaltens Vorträge zu halten. Auch "Kontrollgänge" im Schulgebäude während der Unterrichtszeit (von Lehrkräften mit Freistunden oder des Gebäudemanagements) dürften nicht ohne Wirkung sein.

Diese Maßnahmen sind datenschutzfreundlicher als die Videoüberwachung und zudem kostengünstiger als die Anschaffung und Wartung von Videoüberwachungsanlagen. Für den Fall einer trotzdem angedachten Videoüberwachung hat das Bildungsministerium eine Bekanntmachung hinsichtlich der Anforderungen herausgegeben (Bekanntmachung vom 25. Juni 2018, NBl. MBWK. Seite 289).
[Datei] Checkliste zur Bewertung einer Videoüberwachung

Unter welchen Voraussetzungen darf ich einen digitalen Lehrkräftekalender nutzen?

Für die Zulässigkeit eines digitalen Lehrkräftekalenders ist zwischen Angeboten zu unterscheiden, bei denen die Daten lokal auf dem dienstlich bereitgestellten Endgerät der Lehrkraft gespeichert werden und Angeboten, bei

denen die Daten online bei einem Auftragsverarbeiter gespeichert werden.

Lokale Speicherung

Lehrkräftekalender, die die Daten lokal auf dem Endgerät der Lehrkraft speichern, können von der Schulleitung genehmigt werden. Die Schulleitung prüft, ob der Lehrkräftekalender datenschutzkonform eingesetzt werden kann und erlässt eine entsprechende Dienstanweisung, die den Umfang und die Grenzen der Nutzung regelt.

Damit die Schulleitung ihrer Prüfpflicht nachkommen kann, ist die Lehrkraft verpflichtet, vor Einsatz des Lehrkräftekalenders die Schulleitung zu informieren und sich die Nutzung genehmigen zu lassen.

Da der Einsatz eines digitalen Lehrkräftekalenders mit einem hohen Prüf- und Dokumentationsaufwand verbunden ist, kann die Schulleitung die Nutzung des Lehrkräftekalenders auf eine bestimmte Anwendung beschränken.

In jedem Fall ist die Nutzung eines Lehrkräftekalenders nur zulässig, wenn der Kalender auf dem dienstlich bereitgestellten oder dienstlich genehmigten Gerät eingesetzt wird und die Speicherung lokal auf dem Gerät erfolgt. Eine Sicherung der Daten bei Onlinediensten ist unzulässig.

Dafür ist sicherzustellen, dass

- ein Cloud-Backup,
- die Synchronisation zwischen Endgeräten und
- die Möglichkeit der Datenweitergabe an andere Lehrkräfte

ausgeschlossen sind.

Zudem müssen dem Schutzbedarf der Daten angemessene Sicherheitsmaßnahmen getroffen werden. Dazu gehören:

- ein zusätzlicher Passwortschutz für den Lehrkräftekalender
- die Zugangsdaten für das Endgerät und den Lehrkräftekalender müssen sich unterscheiden
- Daten der Anwendungen, Exportdateien und Backups müssen verschlüsselt werden

Der zulässige Umfang der personenbezogenen Daten, die hierfür verarbeitet werden dürfen, ergibt sich aus § 30 Abs. 10 S. 1 SchulG i.V.m. § 13 Abs. 3 bis 5 SchulDSVO.

Hierzu gehören:

- Kontaktdaten,
- Name, Vorname, Geburtsdatum, Geschlecht und ein rechtmäßig erhobenes Lichtbild,
- Adressdaten, E-Mail-Adressen, Telefon- und vergleichbare Telekommunikationsverbindungen,
- Angaben über für die Beschulung relevante gesundheitliche Beeinträchtigung in codierter Form,
- Angaben zu Nachteilsausgleich, Notenschutz oder einer zurückhaltenden Gewichtung der Rechtschreibleistung,
- persönliche Zwischenbewertungen von Unterrichtsbeiträgen und des allgemeinen Lernverhaltens sowie Zwischennoten für schriftliche Leistungsnachweise,
- Angaben zum Sozialverhalten,
- Namen, Telefonnummern, E-Mail-Adressen der Eltern,
- Adressdaten von Ausbildungsbetrieben,
- entschuldigte und unentschuldigte Fehlzeiten des laufenden Schuljahres,
- eine bestehende Attestpflicht,
- die Unterrichtsdokumentation.

Die Fehlzeiten, die Attestpflicht und die Unterrichtsdokumentation gehören grundsätzlich ins Klassenbuch und dürfen im Lehrkräftekalender nur zusätzlich gespeichert werden.

Sofern der Lehrkräftekalender die Möglichkeit bietet, ein Lichtbild der Schülerinnen und Schüler zu verarbeiten, ist zu beachten, dass dies erforderlich sein muss und die Lichtbilder rechtmäßig, d.h. mit Einwilligung gegenüber der Schule, erhoben wurden.

In allen Fällen ist zu beachten, dass nur die Daten verarbeitet werden, die für die Aufgabenerfüllung erforderlich sind (Grundsatz der Datenminimierung).

Für die im Lehrkräftekalender verarbeiteten Daten sind Aufbewahrungs- und Löschfristen zu beachten. Diese sind in § 15 SchulDSVO geregelt. Grundsätzlich gilt, dass Daten gelöscht werden müssen, sobald sie nicht mehr erforderlich sind um einer Aufgabe nachzukommen. Eine Ausnahme gilt für Daten, die für die Dokumentation einer Leistungsbewertung in einem gerichtlichen Verfahren erforderlich sein könnten. Diese müssen nach Ablauf des Schuljahres für zwei Jahre aufbewahrt werden und können auf Aufforderung der Schulleitung auch in der Schulverwaltung gespeichert werden.

Online-Speicherung

Unter sehr engen Voraussetzungen ist es zulässig, einen Lehrkräftekalender zu nutzen, bei dem die Daten online bei einem Auftragsverarbeiter gespeichert werden.

Grundsätzlich gelten hier dieselben Rahmenbedingungen wie bei lokal abgespeicherten Lehrkräftekalendern. Insoweit wird zu den Erläuterungen zur lokalen Speicherung verwiesen.

Darüber hinaus ist zu beachten, dass online genutzte Lehrkräftekalender immer eine Auftragsverarbeitung darstellen, soweit der Kalender nicht auf Servern der Schule gehostet wird.

Für die Auftragsverarbeitung muss die Schulleitung einen Auftragsverarbeitungsvertrag unterschreiben. Da es sich bei den Daten in einem Lehrkräftekalender zumindest teilweise um Schulverwaltungsdaten handelt, ist für den Abschluss der Auftragsverarbeitung eine Genehmigung des für Bildung zuständigen Ministeriums erforderlich. Einen Mustergenehmigungsantrag finden Sie auf der Medienberatungswebseite des IQSH.

Diese Genehmigung wird erteilt, wenn die Voraussetzungen des § 13 Abs. 2 und 3 SchulDSVO vorliegen. Dafür muss gewährleistet werden, dass nur die Lehrkraft Zugriff auf den Lehrkräftekalender hat, der er gehört und die Nutzung nur auf dienstlichen Geräten bzw. dienstlich genehmigten Geräten erfolgt. Zudem darf der Zugang zu den in § 13 Abs. 4 SchulDSVO aufgeführten Daten nur unter Nutzung einer 2-Faktor-Authentifizierung erfolgen.

Zu diesen in § 13 Abs. 4 SchulDSVO aufgeführten Daten gehören:

- Name, Vorname, Geburtsdatum, Geschlecht und ein rechtmäßig erhobenes Lichtbild,
- Adressdaten, E-Mail-Adressen, Telefon- und vergleichbare Telekommunikationsverbindungen,
- Angaben über für die Beschulung relevante gesundheitliche Beeinträchtigung in codierter Form,
- Angaben zu Nachteilsausgleich, Notenschutz oder einer zurückhaltenden Gewichtung der Rechtschreibleistung,
- persönliche Zwischenbewertungen von Unterrichtsbeiträgen und des allgemeinen Lernverhaltens sowie Zwischennoten für schriftliche Leistungsnachweise,
- Angaben zum Sozialverhalten,
- Namen, Telefonnummern, E-Mail-Adressen der Eltern,
- Adressdaten von Ausbildungsbetrieben.

Unter welchen Voraussetzungen dürfen digitale Klassen- und Notizbücher geführt werden und ist dies auch mit einem Webservice zulässig?

Nach § 13 SchulDSVO dürfen digitale Klassenbücher anstelle von papierenen Klassen- oder Kursbüchern geführt werden. Diese Vorschrift erlaubt es den Schulen, ihre bisher in Papierform geführten Klassenbücher ausschließlich elektronisch zu führen. Eine parallele Führung schließt die Regelung aus.

Entschließt sich eine Schule für die digitale Führung des Klassenbuches und damit zum Einsatz eines elektronischen Verfahrens, darf sie darin auch personenbezogene Daten der Schülerinnen, Schüler und Eltern speichern (§ 13 Abs. 3 SchulDSVO), wenn dies erforderlich ist. In diesem Fall muss das Verfahren umfänglich dokumentiert werden und die Schulleiterin oder der Schulleiter ist verpflichtet, eindeutige Regelungen zur Nutzung des Verfahrens für die Lehrkräfte und ggf. andere Nutzerinnen und Nutzer (Dienstanweisung) zu treffen und diese in Kraft zu setzen (Rechenschafts- und Dokumentationspflicht nach Art. 5 Abs. 2 DSGVO i. V. m. Art. 32 DSGVO).

Ferner ist das digitale Klassenbuch, sofern es sich nicht um die Dokumentation von Fehlzeiten und des erteilten Unterrichts handelt, zwingend durch einen zweiten Sicherungsmechanismus (sog. Zwei-Faktor-Authentisierung - 2FA) vor dem Zugang Unbefugter zu sichern (§ 13 Abs. 2 Nr. 3 SchulDSVO).

Zugang zum **digitalen Klassenbuch** dürfen nur die in § 6 SchulDSVO genannten sowie die zur Schulsozialarbeit eingesetzten Personen erhalten. Darüber hinaus sind alle Daten **zentral (Server der Schule oder des**

Dienstleisters) abzulegen und dürfen nicht lokal auf Endgeräten gespeichert werden.

Wird das digitale Klassenbuch nicht auf informationstechnischen Geräten der Schule, sondern unter Zuhilfenahme eines Dienstleisters geführt, handelt es sich um Auftragsverarbeitung nach Art. 28 DSGVO. In diesem Fall kann die Schulleitung eine solche Datenverarbeitung (unabhängig vom eingesetzten Verfahren) generell nur mit Genehmigung des Bildungsministeriums in Auftrag geben (§ 12 SchulDSVO).

Ergänzend zu den genutzten Funktionen zum Ersatz des papiernen Klassenbuchs bieten die Produkte häufig auch die Möglichkeit, das Lehrkräfte darin persönliche Notizen ablegen und somit die analogen Lehrerkalender in eine digitale Form zu überführen.

Die zum Schuljahr 2022/2023 durch das MBWFK erlassene Änderung der SchulDSVO (siehe Nachrichtenblatt Ausgabe Nr. 6/7/2022 – Schule –) ermöglicht es auch, losgelöst von digitalen Klassenbüchern, sogenannte **digitale Lehrkräftekalender** zu führen. Unter welchen Bedingungen dies möglich ist, wird in einem eigenen FAQ-Eintrag erläutert.

Unter welchen Voraussetzungen dürfen Schülerakten (insbesondere bei einem Schulwechsel) an eine andere Schule übersandt werden?

§ 9 Abs. 1 SchulDSVO legt fest, dass die Übersendung der gesamten Schülerakte nur auf Anforderung der aufnehmenden Schule, nur zur kurzfristigen Einsichtnahme, nur im Einzelfall und wenn es die besonderen Umstände des Schulwechsels erforderlich machen, zulässig ist. Dies bedeutet, dass im Regelfall - insbesondere beim Wechsel von der Grundschule an die weiterführende Schule - keine Schülerakte übersandt werden darf. Hintergrund dieser Regelung ist, dass die aufnehmende Schule die (Grund)Daten direkt bei den Eltern erheben soll, damit das Kind unbelastet die neue Schullaufbahn beginnen kann. Können die Eltern bestimmte notwendige Informationen nicht beibringen, kann die aufnehmende Schule diese Daten (z. B. Kopien der letzten Zeugnisse) bei der bisherigen Schule anfordern (§ 9 Abs. 1 Nr. 1 bis 6 SchulDSVO).

Das Verbot der automatischen (proaktiven) Aktenübersendung bei einem Schulwechsel kann nicht mit einer Einwilligungserklärung der Eltern umgangen werden.

Die teilweise vorherrschende Praxis, die Akten nach Verlassen der Grundschule unaufgefordert den weiterführenden Schulen zu übersenden, ist damit unzulässig. Genauso verhält es sich, wenn die weiterführenden Schulen diese Akten bei den Grundschulen pauschal anfordern.

Unter welchen Voraussetzungen kann eine Schule einen Messengerdienst als Kommunikationsmittel einführen?

Im privaten Umfeld nehmen Messengerdienste und soziale Medien als Kommunikationskanäle einen immer größeren Stellenwert ein. Lehrkräfte und Schulleitungen stehen häufig vor der Frage, ob der Einsatz von Facebook oder die Nutzung von WhatsApp oder anderen Messengerdiensten, wie z. B. Threema, für den Austausch von Informationen mit Schülerinnen, Schülern und Eltern (Betroffene) im Schulbereich zulässig ist. Auch Anfragen und Beschwerden von Eltern, deren Kinder mit Lehrkräften auf deren Anregung über solche Dienste mit ihnen kommunizieren sollen, machen eine Auseinandersetzung mit der Thematik erforderlich.

Aus folgenden Gründen ist die Nutzung von Messengerdiensten für die dienstliche Kommunikation zwischen Lehrkräften (kollegiumsintern) und mit Betroffenen (Schülerinnen und Schüler, Eltern etc.) kritisch zu sehen.

Bei der Bewertung sind sowohl die technischen (Produkt, Endgeräte) als auch die organisatorischen

(Nutzungsszenario, Nutzungsregeln, Mitbestimmung, Datenschutzdokumentation) Bedingungen zu betrachten.

1. Generell gilt:

Lehrkräfte müssen stets unterscheiden, ob sie mit Betroffenen dienstlich oder privat kommunizieren. Rechtlich betrachtet ist die dienstliche Kommunikation eine Kommunikation der Schule. Ein Beispiel für dienstliche Kommunikation wäre z.B. die Bekanntgabe von Noten oder Stundenausfall. Bei privater Kommunikation handelt die Lehrkraft dagegen für sich selbst, d.h. als Privatperson. Ein Beispiel für private Kommunikation wären z.B. Geburtstagsgrüße. In Zweifelsfällen ist von dienstlicher Kommunikation auszugehen.

In diesem Zusammenhang ist zunächst Folgendes zu beachten: Daten, welche eine Lehrkraft zum Zweck der dienstlichen Kommunikation erhalten hat, darf diese nicht einfach für private Zwecke nutzen. Ist der Lehrkraft die Telefonnummer eines Schülers also z.B. aus der Klassenliste bekannt, darf sie diese Information nicht einfach nutzen, um dem Schüler privat Geburtstagsgrüße zu senden.

Kommuniziert eine Lehrkraft dienstlich, hat sie die besonderen datenschutzrechtlichen Vorgaben des Schulgesetzes und der SchulDSVO zu beachten.

2. Im Bereich der dienstlichen Kommunikation ist im Einzelnen Folgendes zu beachten:

Die Schule kann personenbezogene Daten der Betroffenen entweder zu Verwaltungszwecken oder zu didaktisch-pädagogischen Zwecken verarbeiten (vgl. § 4 SchulDSVO).

Die Erhebung personenbezogener Daten der Betroffenen zu Verwaltungszwecken erfolgt ausschließlich durch die Schulleitung und das ihr gegenüber weisungsgebundene Personal des Schulsekretariats (§ 8 Abs. 1 SchulDSVO). Die Lehrkräfte sind nicht berechtigt, diese Daten zu eigenen Zwecken zu erheben, sondern erhalten sie nach Maßgabe des § 6 SchulDSVO aus dem Datenbestand der Schule. Natürlich dürfen Lehrkräfte auf Weisung der Schulleitung Daten für die Schulverwaltung erheben.

§ 30 Abs. 1 SchulG i. V. m. § 5 SchulDSVO führt abschließend auf, welche personenbezogenen Daten die Schule für ihre Zwecke erheben und weiter verarbeiten darf.

Die Daten, die die Lehrkräfte zu Verwaltungszwecken erhalten, können von den Lehrkräften selbstverständlich auch für die Kommunikation im pädagogisch-didaktischen Zusammenhang verwendet werden.

Die Entscheidung, in welcher Weise die Schule im Rahmen der Schulverwaltung und im Zusammenhang mit der pädagogisch-didaktischen Kommunikation mit den Betroffenen kommuniziert, liegt jedoch primär bei der Schulleiterin oder dem Schulleiter. Nach § 33 Abs. 2 SchulG tragen die Schulleiterinnen und Schulleiter die Verantwortung für die Erfüllung des pädagogischen Auftrages der Schule sowie die Organisation und Verwaltung der Schule entsprechend den Rechts- und Verwaltungsvorschriften. Daraus folgt, dass die Entscheidung, in welcher Weise die elektronische Kommunikation mit den Betroffenen erfolgt, nicht von jeder Lehrkraft selbst getroffen werden kann.

3. Warum ist die Nutzung von Messengerdiensten, insbesondere WhatsApp, nicht ohne weiteres zulässig?

Obwohl es sich bei Messengerdiensten um Telekommunikationsdienste handelt, werden die europäischen (E-Privacy-Richtlinie der EU) und die deutschen Rechtsregelungen (Art. 10 Grundgesetz, Telekommunikationsgesetz) von einigen der Diensteanbieter, zu denen auch WhatsApp gehört, nicht beachtet.

Viele Anbieter ermöglichen nicht einfach nur Telekommunikation, sondern werten diese Telekommunikationsvorgänge auch zur Nutzeranalyse (u. a. Auswertung von Standortdaten, Daten darüber, wer mit wem kommuniziert und empirische Auswertungen für Werbezwecke) aus. Da mit der Nutzung dieser Dienste die Nutzungsbedingungen anerkannt werden müssen, die einen Ausschluss solcher Vorgänge nicht möglich machen, würde man die personenbezogenen Daten der Schülerinnen und Schüler und der Eltern im Rahmen der dienstlichen Kommunikation diesen Analysen preisgeben.

Bestimmte Messengerdienste gleichen bei der ersten Anmeldung und danach laufend in der Regel die im verwendeten Gerät (z. B. Smartphone) gespeicherten Kontaktdaten ab. Damit werden den Diensteanbietern personenbezogene Daten von unbeteiligten dritten Personen bekannt. Dieser Vorgang würde somit durch eine dienstliche Maßnahme der Lehrkraft ausgelöst werden.

Im Grundsatz findet die Nutzung eines Telekommunikationsanbieters (TK-Anbieter) im Rahmen eines Auftragsverhältnisses statt. Der Auftraggeber beauftragt den Auftragnehmer (TK-Anbieter), Telekommunikation in Form von z. B. Telefonie, E-Mail oder eben Messaging bereitzustellen und zu ermöglichen. Es handelt sich in diesem Fall somit um Auftragsverarbeitung, für die die Vorschriften des Art. 28 DSGVO Anwendung finden. Nach diesen Vorschriften bleibt der Auftraggeber für die Einhaltung der datenschutzrechtlichen Regelungen verantwortlich und hat dies durch das vertraglich vereinbarte Weisungsrecht gegenüber dem Auftragnehmer sicherzustellen. Sofern Telekommunikationsdienste auf der Grundlage des deutschen Rechts in Anspruch genommen werden, ist ein solcher Auftragsverarbeitungsvertrag im Grundsatz entbehrlich, da die Vorschriften zum Schutz des Fernmeldegeheimnisses ausreichend auch die datenschutzrechtlichen Belange soweit sicherstellen. Die Einhaltung wird durch die dafür zuständigen Kontrollinstitutionen, insbesondere die Bundesnetzagentur, überwacht. Hierzu gehört auch die Prüfung der von den Telekommunikationsanbietern zugrunde gelegten Vertragsklauseln und Nutzungsbedingungen.

Viele der bekannten Messengerdienste ausländischer, insbesondere außereuropäischer Anbieter, erfüllen diese Vorgaben nicht.

Ferner ist zu berücksichtigen, dass die Lehrkraft sicherstellen muss, private und dienstliche Kommunikation möglichst eindeutig (technisch) zu trennen. Während bei der Nutzung von E-Mail eine solche Trennung durch die Verwendung verschiedener E-Mail-Adressen möglich ist, ist eine solche Abgrenzung bei Messengerdiensten nicht ohne weiteres möglich.

Kommuniziert eine Lehrkraft mit einem privat genutzten Messengerdienst, wie z. B. WhatsApp, auch in dienstlicher Funktion, erfolgt dies mit demselben Gerät und demselben Messengerdienst. Eine Abgrenzung zwischen dienstlicher und privater Kommunikation ist damit nicht möglich.

Was ist konkret zu beachten, wenn eine Schule einen Messengerdienst als Kommunikationsmittel einführen möchte?

Ein Messenger-Einsatz zur Kommunikation zwischen Lehrkräften (Eltern, Schülerinnen und Schülern) mit einem extern gehosteten Dienst stellt eine Auftragsverarbeitung nach Artikel 28 DSGVO i. V. m. §§ 11, 12 Schul-Datenschutzverordnung dar. Vor dem Einsatz und dem Abschluss eines Nutzungsvertrages/Auftragsverarbeitungvertrages mit einem Anbieter sind noch Vorarbeiten erforderlich.

Grundsätzlich hat jede Schule vor der Einführung/Nutzung eines Onlinedienstes zu prüfen, ob dieser rechtmäßig (insb. Beachtung DSGVO, § 127 SchulG, §§ 2, 11-15 SchulDSVO + Urheberrecht, Jugendmedienschutz) eingesetzt werden kann.

Im ersten Schritt muss ein datenschutzkonform einsetzbares Produkt gefunden werden. Die Datenschutzkonformität eines Dienstes allein garantiert jedoch noch nicht die datenschutzkonforme Nutzung („Nur weil ein Auto TÜV-geprüft ist, kann ich damit trotzdem noch über rote Ampeln fahren“).

Von der Möglichkeit einer datenschutzkonformen Nutzung kann am ehesten ausgegangen werden, wenn der Anbieter seinen Sitz in der EU, im EWR oder in einem Land, für welches ein sogenannter Angemessenheitsbeschluss entsprechend Artikel 45 DSGVO vorliegt (dies ist für die Schweiz erfüllt), hat. Gleiches gilt für die Standorte der Server. Bei Anbietern aus den USA muss man trotz des seit Juni 2023 vorhandenen Angemessenheitsbeschlusses davon ausgehen, dass diese die Voraussetzungen für eine datenschutzkonforme Nutzung nicht uneingeschränkt erfüllen können, da der Angemessenheitsbeschluss nur bei Firmen greift, die sich auch nach dem „Data Privacy Framework“ zertifiziert haben. In allen anderen Fällen sind durch die Schule weiterhin die erweiterten Prüfpflichten zu erfüllen und es kann davon ausgegangen werden, dass dies in den meisten Fällen nicht zu einer positiven Einschätzung führen wird. Weiter ist immer zu beachten, dass viele Dienste

die Nutzendendaten (zumindest Metadaten) zu eigenen Zwecken (Profilbildung, Tracking, Werbung) nutzen, was ebenso einen Einsatz im schulischen Kontext ausschließt.

Im zweiten Schritt der Einsatz an der Schule dann durch die entsprechenden Maßnahmen vorbereitet und durchgeführt werden:

- Schulkonferenzbeschluss
- Beteiligung des örtlichen Personalrates
- Festlegung eines Nutzungsszenarios,
- Ergreifung und Dokumentation technischer und organisatorischer Maßnahmen zur IT-Sicherheit,
- Information gegenüber den Betroffenen,
- Erlass von Nutzungsordnungen
- ggf. Beschaffung/Bereitstellung von Endgeräten
- ...

Ergänzend ist zu beachten, dass die Einführung einer Messenger-App nicht zu einer Benachteiligung von Schülerinnen und Schülern führen darf, die keine entsprechenden Geräte besitzen oder eine Messenger-App nicht einsetzen wollen. Ein Messengereinsatz würde, bei Fehlen dienstlich bereitgestellter Endgeräte, eine freiwillig erteilte Einwilligung der betroffenen Personen (Eltern für Ihre Kinder bei Minderjährigen) erfordern. Ob echte Freiwilligkeit im Abhängigkeitsverhältnis Schülerin/Schüler zu Schule im Spannungsfeld der Schulpflicht besteht, ist zumindest kritisch zu sehen.

Unter welchen Voraussetzungen sind Foto- oder Videoaufnahmen von Schülerinnen und Schülern möglich?

An Schulen wird häufig der Wunsch geäußert, Foto- oder Videoaufnahmen von Schülerinnen und Schülern anzufertigen und diese zu verschiedensten Zwecken zu nutzen. Anlässe können hier beispielsweise Einschulungs- oder Entlassungsfeiern, Projektwochen, Wettbewerbe, Klassenfahrten sowie auch schulöffentliche Aufführungen von Orchestern oder Theatergruppen sein. Ebenso sind die verfolgten Zwecke vielseitig. Hier sind beispielsweise der Aushang von Fotos in Klassenräumen oder im Schulgebäude, die Veröffentlichung auf der Schulwebseite, die Weitergabe an Eltern, die Erstellung von Jahrbüchern, die Speicherung im Schulverwaltungsprogramm oder einem digitalen Klassenbuch sowie die Erstellung von „Erinnerungsfotos“ durch Eltern zu nennen.

Für eine Bewertung der Zulässigkeit solcher Aufnahmen ist in erster Linie folgende Frage zu beantworten:

Wer fotografiert wen, zu welchem Anlass und zu welchem Zweck?

Hinsichtlich des Fotografierens im Schulbereich sind neben dem Schulgesetz (SchulG) und der Schul-Datenschutzverordnung (SchulDSVO) auch die Regelungen in der EU-Datenschutzgrundverordnung (DSGVO) und ggf. des Kunsturhebergesetzes („Recht am eigenen Bild“) zu beachten.

Der zulässige Datenumfang für Verarbeitungen von personenbezogenen Daten von Schülerinnen, Schülern und Eltern im Rahmen des Schulverhältnisses, wozu auch Foto- und Videoaufnahmen zählen, ergibt sich aus § 30 Abs. 1 SchulG i. V. m. § 5 SchulDSVO und der Anlage 2 zur SchulDSVO. Alle dort aufgeführten Daten dürfen i. d. R. erhoben und verarbeitet werden, ohne dass es einer Einwilligung der Betroffenen Bedarf.

In dieser abschließenden Aufzählung findet sich seit der Neufassung der SchulDSVO im Juli 2022 auch das Datum „Lichtbild/Foto zu Schulverwaltungszwecken (rechtmäßig erhoben)“. Hier ist abweichend für eine rechtmäßige Erhebung und Nutzung eine zweckbezogene, informierte und freiwillig erteilte Einwilligung

erforderlich.

Hierbei ist immer auch **die Erforderlichkeit sowie der Zweck** der Erstellung dieser Aufnahmen zu prüfen und zu erläutern.

Im sogenannten Schüleraufnahmebogen (hier herunterladbar) werden bereits die Einwilligungen für häufig in Schule auftretende Verarbeitungen abgefragt. Der Bogen kann auf die individuelle Situation vor Ort angepasst und ggf. um weitere Szenarien ergänzt werden

Die diesem Artikel zum Download beigefügten Handreichungen geben detailliertere Informationen unterschiedlichen Szenarien und den Rahmenbedingungen bei der Erstellung und Weiterverarbeitung von Foto- und Videoaufnahmen. Ebenso werden Hinweise zur Gestaltung der erforderlichen Einwilligung gegeben. Ergänzende Informationen und Muster zum Thema Einwilligung sind in diesem FAQ-Beitrag zu finden.
[Datei] Hinweise zu Foto- und Videoaufnahmen an Schulen
[Datei] Mustereinwilligung für Foto-, Audio-, Videoaufnahmen
[Datei] Muster für einen Aushang bei Veranstaltungen
[Datei] Mustereinwilligung Jahrbuch

Wann liegt eine Datenpanne vor und was ist in einem solchen Fall zu unternehmen?

Die EU-Datenschutzgrundverordnung (DSGVO) fordert in den Grundsätzen der Verarbeitung (Artikel 5), dass die personenbezogenen Daten durch technische und organisatorische Maßnahmen (Erläuterungen im Artikel 32) vor Verlust, Missbrauch, Manipulation und Offenlegung geschützt werden müssen.

Trotz guter Schutzmaßnahmen ist es nicht ausgeschlossen, dass beispielsweise durch menschliches Fehlverhalten, Diebstahl oder Hackerangriffe oder Schadsoftware dieser Schutz verletzt wird. Gehen dann personenbezogene Daten verloren, werden manipuliert oder werden öffentlich, liegt eine Datenpanne nach Artikel 33 DSGVO vor.

Ereignisse, die eine Datenpanne im Sinne der DSGVO darstellen:

- Versand einer E-Mail an eine große Zahl Empfänger, die nicht in Bcc in die Mail eingefügt wurden
  -> Offenlegung einer großen Zahl von Kontaktinformationen
- Verlust eines unverschlüsselten USB-Sticks mit Zeugnissen, Klassenlisten oder Gutachtenentwürfen
  -> Mögliche missbräuchliche Nutzung durch den "Finder" und ggf. nachteilige Auswirkungen auf die Personen, deren Daten auf dem USB-Stick gespeichert waren
- Durch einen technischen Defekt oder falsche Konfiguration der Benutzerrechte besteht für einen unbeschränkten Personenkreis die Möglichkeit, auf Dateien im Schulverwaltungsnetz zuzugreifen
  -> Offenlegung sensibler Informationen oder Beschäftigtendaten
- Durch eine Sicherheitslücke bekommen Unbefugte Zugriff auf die Benutzerdaten eines Online-Lernsystems
  -> Identitätsdiebstahl, Manipulation von Daten
- Der Schulverwaltungsserver wird bei einem Einbruch gestohlen
  -> Schüler*innen und Elterndaten inklusive sensibler Gesundheitsdaten können missbräuchlich genutzt werden
  -> Existiert keine Sicherungskopie sind Daten nicht wiederherstellbar -> keine Zeugniserstellung möglich etc.
- Altakten werden nach Ablauf der Aufbewahrungsfrist in den Altpapiercontainer entsorgt
  -> Datenschutzkonforme Löschung nicht gegeben, Daten könnten öffentlich werden

Im Falle einer Datenpanne sollten folgende Schritte unternommen werden:

1. Information des zentralen Datenschutzbeauftragten für die öffentlichen Schulen um das weitere Vorgehen abzustimmen (datenschutzbeauftragterschule@bimi.landsh.de)
2. Bei Datenpannen mit Schulverwaltungsrechnern/Im Landenetz-Bildung (LanBSH) zusätzlich Meldung an das IQSH
3. Meldung der Datenpanne innerhalb von 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde

(Unabhängiges Landeszentrum für Datenschutz - ULD) mit beigefügtem Muster per Mail an mail@datenschutzzentrum.de und in Kopie an datenschutzbeauftragterschule@bimi.landsh.de; Ergänzend Versand per Post an ULD
4. ggf. Information der Betroffenen über Art und Umfang der Datenpanne
5. Beseitigung von Ursachen, die zur Panne geführt haben, bspw. durch technische Sicherheitsmaßnahmen, Belehrung des Personals

[Datei] Muster-Datenpannenmeldung

Wann müssen personenbezogene Daten in der Schulverwaltung und bei Lehrkräften gelöscht werden?

In der Schule werden regelmäßig personenbezogene Daten über Schülerinnen und Schüler sowie Eltern verarbeitet. Dies passiert sowohl in der Schulverwaltung (Schülerakte, Schulverwaltungssoftware, schulorganisatorische Belange etc.) als auch durch Lehrkräfte (persönliche Notizen über das Leistungs- und Sozialverhalten, Noten, Zeugnisentwürfe, Kontaktlisten etc.). Aus Datenschutzsicht ist es dabei unerheblich, ob die Daten digital oder in Papierform vorliegen.

Die Datenschutzgrundverordnung (DSGVO - EU-Verordnung 2016/679) versteht unter Verarbeitung „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten...". Hierzu gehört auch das Löschen oder die Vernichtung (Artikel 4 Nr. 2).

Verarbeitung passiert kontinuierlich über die gesamte Verweildauer von SuS, bspw. bei der Aufnahme an der Schule, Versetzungen, Abschlussprüfungen und im regulären Schulbetrieb. Hinzu kommen weitere Dokumente, beispielsweise im Rahmen von schulärztlichen Untersuchungen, bei inklusiv beschulten SuS oder im Rahmen des Nachteilsausgleichs. **Alle Dokumente mit Relevanz für das Schulverhältnis müssen ordnungsgemäß abgelegt werden** - bei aktiven SuS üblicherweise in der Schulverwaltung (Sekretariat), nach Entlassung in einem zur Schule gehörenden Aktenaufbewahrungsraum. Damit Informationen schnell und vollständig gefunden werden können und die aus der DSGVO hervorgehenden Rechenschafts- und Dokumentationspflichten erfüllt sowie die Betroffenenrechte nach Artikel 15 - 22 DSGVO gewahrt werden können, muss die Schule ein datenschutzkonformes Speicher- und Löschkonzept vorweisen und umsetzen.

Der **Grundsatz für die Löschung**/Aufbewahrung von personenbezogenen Daten lautet: "Daten sind zu löschen, sofern Sie für die konkrete Aufgabenerfüllung nicht mehr erforderlich sind, es sei denn, eine gesetzliche Vorschrift schreibt eine längere Aufbewahrungszeit/längere Löschfrist vor." (Artikel 5 Abs. 1 Buchst. e DSGVO sowie § 10 Abs. 1 Satz 6 SchulDSVO).

Für die **Schulverwaltung** regelt der § 10 der Schuldatenschutzverordnung die besonderen Löschfristen abschließend. Da für die verschiedenen in Schule anfallenden Unterlagen auch unterschiedliche Löschfristen festgelegt sind, bedarf es einer daran angepassten Schriftgutverwaltung, um bspw. am Schuljahresende einfach und schnell Unterlagen sortiert nach ihren Löschfristen in den Aktenaufbewahrungsraum zu überführen bzw. dort gelagerte Unterlagen dem zuständigen **Archiv zur Übernahme anzubieten** bzw. diese, bei Verzicht auf das Anbieten (Klärung mit dem zuständigen Kommunalarchiv im Vorwege), **datenschutzkonform zu löschen** (siehe dieser FAQ-Eintrag). Ein mögliches Verfahren und weitere Informationen zur Schriftgutverwaltung sind der beigefügten Datei zu entnehmen.

Für **Lehrkräfte** erfolgt die Regelung durch den § 15 SchulDSVO. Hiernach sind - dem Grundsatz der DSGVO folgend - Unterlagen ebenfalls unverzüglich, datenschutzkonform zu **löschen, sobald sie für die konkrete Aufgabenerfüllung nicht mehr erforderlich** sind. Einzige **Ausnahme** sind Unterlagen, die zur Dokumentation von Leistungsbewertungen in gerichtlichen Verfahren notwendig sein können. Diese sind noch **2 Jahre über das Schuljahresende hinaus** aufzubewahren.

[Datei] Hinweise zur Schriftgutverwaltung - Muster für ein Ablage- und Löschkonzept

Was ist bei der E-Mail-Kommunikation zwischen Kolleginnen und Kollegen sowie mit Eltern und Schülerinnen/Schülern zu beachten?

Für die E-Mailkommunikation steht allen Lehrkräften eine E-Mailadresse (@schule-sh.de) für die dienstliche Nutzung zur Verfügung. Die Rahmenbedingungen hierfür wurden in einer Dienstvereinbarung festgelegt und ergeben sich im Übrigen aus der Richtlinie zur Nutzung von Internet und E-Mail vom Januar 2021 sowie dem § 9 Abs. 5 SchulDSVO. Andere, beispielsweise über den Hosting-Anbieter der Schulhomepage (Adressen der Form name@schulname.de) bereitgestellte Mailadressen dürfen zukünftig nicht mehr für die dienstliche Kommunikation verwendet werden. Ausnahme bildet die zwingend erforderliche pädagogische Kommunikation im unterrichtlichen Kontext mit den Schülerinnen und Schülern (bspw. bei der Nutzung von IServ).

Folgende **ergänzende Hinweise** sind zu beachten:

- Die **landesnetzinterne Kommunikation** mit personenbezogenen Informationen im Mailtext ist ohne Einschränkungen zulässig. Hierzu gehören neben der Domäne "landsh.de" auch andere, im Landesnetz befindliche E-Mail-Domänen. Eine Übersicht findet sich unter diesem Link (nur aus dem Landesnetz erreichbar!)
- Die Kommunikation mit anderen Personen (extern, Eltern usw.) ist uneingeschränkt zulässig, wenn es sich beim Mailinhalt um **organisatorische Belange und allgemeine Informationen** handelt.
- Beim **Versand von personenbezogenen Informationen muss, abhängig von der Sensibilität und dem Schutzbedarf, ggf. verschlüsselt kommuniziert werden** (bspw. verschlüsselte Dokumente im Anhang). Idealerweise wird in solchen Fällen auf andere Kommunikationsformen (Anruf, Gespräch, Brief) zurückgegriffen.

- Bei E-Mails, die an mehrere Empfänger gerichtet sind (Rundschreiben etc.), müssen alle **Empfänger in Bcc** gesetzt werden.
- Keine Weiterleitung auf private Mailadressen
- Keine private Kommunikation über dienstliche Mailadressen
- Keine Speicherung auf nicht genehmigten privaten Endgeräten
- Regelmäßige Bereinigung des Mailaccounts (Nachrichten und Adressbuch, vgl. § 15 SchulDSVO)

- Aktenrelevante Nachrichten sind zur entsprechenden (Schüler-)Akte zu nehmen (vgl. § 7 SchulDSVO)

[Datei] DS-Basics_Mailkommunikation

Was ist beim Einsatz von Lernprogrammen, Apps, und Onlinediensten zu beachten, wenn bei der Nutzung personenbezogene Daten verarbeitet werden?

Die zunehmende Digitalisierung an den Schulen und die Anforderungen an zeitgemäßen, ansprechenden und wirklichkeitsnahen Unterricht führen zu einem stark steigenden Bedarf nach dem Einsatz unterschiedlichster digitaler Werkzeuge. Die Bandbreite erstreckt sich vom **lokalen Einsatz von Office-Anwendungen, einfacher Simulationsprogramme und interaktiven Apps bis hin zur Nutzung kommerzieller, zentral betriebenen Lernplattformen, Videokonferenz- und Lernmanagementsystemen**. Für die Nutzung kommen Endgeräte verschiedener Hersteller, Betriebssysteme und Leistungsklassen zum Einsatz, die sowohl im Eigentum und **in Verantwortung der Schule** betrieben werden, als auch **schülereigene Endgeräte** in beliebigen Konfigurationsvarianten. Die Nutzung kann ausschließlich in der Schule, aber auch ergänzend im privaten Umfeld stattfinden (Distanzlernen, Hausaufgaben etc.).

Für die Beantwortung der Fragen, ob ein bestimmtes, von Schule nachgefragtes, Produkt oder ein Onlineangebot überhaupt in Schule rechtmäßig eingesetzt werden kann, ist zunächst ein Nutzungskonzept zu entwerfen, in dem Zwecke und Ziele, beteiligte Personengruppen, die Verwendungsorte und die Herkunft der Endgeräte (schulisch/privat) festgelegt wird.

Für die Klärung der Frage, ob die Anwendung vor der Nutzung einer datenschutzrechtlichen Prüfung unterzogen werden muss und welche Dokumentationserfordernisse daraus für die Schule erwachsen, ist **entscheidend, ob das geplante Verfahren mit einer Verarbeitung personenbezogener Daten einhergeht**. Findet die Verarbeitung darüber hinaus nicht lokal, sondern bei einem Dienstleister (Programmanbieter, Hostingdienstleister) statt, ist zusätzlich ein Auftragsverarbeitungsvertrag zwischen Schule und Dienstleister zu schließen und ggf. eine Genehmigung beim Bildungsministerium einzuholen.

Einen Mustergenehmigungsantrag finden Sie hier. Auf derselben Seite stehen zudem Muster-Dokumentenpakete für einige häufig in Schule genutzte Dienste sowie die sogenannten Landeslösungen zum Download bereit.

Lehrkräfte sollten nicht eigenmächtig Apps oder Onlinedienste, die mit der Verarbeitung personenbezogener Daten einher gehen, einführen oder gar Schülerinnen und Schüler zur Installation verpflichten. Hier ist immer eine Absprache/Genehmigung mit/durch die Schulleitung erforderlich, da diese die Gesamtverantwortung für die Einhaltung und Organisation des Datenschutzes trägt (§ 2 SchulDSVO).

Die diesem Beitrag beigefügten Unterlagen sollen Ihnen erste Informationen zu diesem Themenkomplex und Hilfestellungen bei der Auswahl geben sowie die erforderliche Verarbeitungsdokumentation mit Mustern unterstützen.
[Datei] Verarbeitungsdokumentation_Muster
[Datei] Checkliste_Auftragsverarbeitung_I
[Datei] Checkliste_Auftragsverarbeitung_II
[Datei] Checkliste_Dokumentationspflichten
[Datei] Schnellüberblick zum Auswahl-, Prüf- und Einführungsverfahren für digitale Medien

Was ist datenschutzrechtlich von klasseninternen Notenspiegeln zu halten?

Mit Hilfe eines anonymisierten Notenspiegels wird üblicherweise ein Leistungsüberblick (bezogen auf eine Klassenarbeit oder auf die Gesamtleistung in einem Fach) für eine Schulklasse erstellt. Anhand dieser Leistungsübersicht ist nur feststellbar, wie viele Schülerinnen und Schüler einer Klasse welche Noten erreicht haben. Wird der Notenspiegel in der Klasse den Schülerinnen und Schülern oder betroffenen Eltern zur Kenntnis gegeben, werden damit zunächst keine personenbezogenen Daten übermittelt, weil sich kein Bezug zu einzelnen Schülern herleiten lässt. Allerdings kann es besondere Konstallationen geben, bei denen der Notenspiegel in Verbindung mit anderen Informationen doch potenziell eine Zuordnung zur Schülerin/zum Schüler ermöglicht. Daher sollte die Bekanntgabe eines Notenspiegels pädagogisch abgewogen werden und ggf. unterbleiben. Die Bekanntgabe der Durchschnittsnote einer Klassenarbeit ist hier dann eine Alternative. Die Übermittlung/Bekanntgabe von individuellen Noten wird in diesem FAQ-Eintrag behandelt.

Was ist vor der Einführung eines schulischen WLAN zu beachten?

Um die Nutzung eines WLAN an Schule zu ermöglichen, müssen im Vorfeld bestimmte Fragen der Datensicherheit und des Datenschutzes geklärt sein, damit das WLAN ordnungsgemäß betrieben werden kann. Darunter ist bei der Einführung, neben der Art des Zugangs, auch die weitere Gewährleistung der Sicherheit des in der Schule eingesetzten WLAN zu beachten.

Eine damit verbundene Frage ist die sogenannte „Störerhaftung“ und die damit einhergehende verpflichtende, detaillierte Protokollierung des Internetzugriffs. Hier hat sich die Gesetzliche Grundlage in den vergangenen Jahren geändert: 2017 wurde von der Bundesregierung eine Novelle des Telemediengesetzes (TMG) beschlossen. Hierzu gehörte auch die Abschaffung der Störerhaftung auf Unterlassung. In Kombination mit dem am 01.12.2021 in Kraft getretenem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) **entfällt dadurch die Notwendigkeit der umfangreichen Protokollierung** der schulischen WLAN-Nutzung. Darüber hinaus wird empfohlen das schulische WLAN mit einem Jugendschutzfilter auszustatten. Dadurch entfällt auch eine mögliche umfangreiche Protokollierung aus pädagogischen Gründen. Eine minimalistische Protokollierung mit kurzer Speicherdauer z.B.

der An- und Abmeldung von Geräten im WLAN kann durchaus sinnvoll sein und ist üblich, um z.B. technische Probleme analysieren zu können oder die Auslastung statistisch auszuwerten.

Bietet eine Schule zusätzlich zum schulischen WLAN ein frei zugängliches, ungefiltertes WLAN an (z.B. EchterNorden, Stadtnetze), muss in der Nutzungsordnung (s.u.) festgehalten werden, dass dieses Netz im schulischen Kontext nicht genutzt werden darf. **Alle folgenden Erläuterungen beziehen sich ausschließlich auf das pädagogische WLAN.**

Je nach Konfiguration des WLANs ist eine vollkommen anonyme Nutzung unwahrscheinlich. Daher muss vor der Inbetriebnahme der Infrastruktur auch die Datenschutz-Dokumentation erfolgt sein. Um diesen Prozess zu Unterstützen stellt das IQSH über die Medienberatungsseite Musterdokumente zur Verfügung. Diese beinhalten neben einem Mustereintrag für das VVT und den Datenschutzhinweisen auch die Dienstanweisung und Nutzungsordnung. Da der Zugang zum Schul-WLAN sehr unterschiedlich realisiert werden kann, enthalten diese Musterdokumente insgesamt drei Beispiele (s.u. Exkurs). Dabei obliegt der Schulleitung die Verantwortung diese Dokumente entsprechend der konkreten Situation vor Ort anzupassen und sie nach der Vervollständigung in Kraft zu setzen.

Hinweise zur Vervollständigung der Dokumentation

Darüber hinaus sind die weiteren Vorgaben aus dem FAQ-Eintrag Was ist beim Einsatz von Lernprogrammen, Apps, und Onlinediensten zu beachten, wenn bei der Nutzung personenbezogene Daten verarbeitet werden? auch auf das WLAN anzuwenden. Insbesondere ist ein Auftragsverarbeitungsvertrag (AVV) mit dem Dienstleister zu schließen, der das WLAN verwaltet. Bei den weiteren Dokumenten z.B. bei der Vervollständigung der Datenschutzhinweise und bei der technischen Beschreibung des Verfahrens ist die Schulleitung zudem ggf. auf die Unterstützung des Dienstleisters angewiesen.

Exkurs zur technischen Umsetzung mit Hilfe von Vouchern

Es gibt verschiedene Möglichkeiten ein schulisches WLAN umzusetzen. Die drei Beispiele aus den Musterdokumenten sind:

1. die Vergabe personenbezogener Zugänge (Benutzername + Passwort),
2. die Nutzung eines geteilten Zugangs (geteiltes Passwort) und
3. die Nutzung zeitlich begrenzter 1x Voucher für Gäste (z.B. Eltern bei Veranstaltungen in der Schule).

Voucher-Systeme lassen sich, neben dem in Beispiel 3 beschriebenen Szenario, deutlich differenzierter nutzen, als nur für die Realisierung von Gast-Zugängen. Unter anderem gibt es Voucher-Systeme mit Nutzer(Gruppen)verwaltung. Hierüber ließe sich dann auch Beispiel 1 (personalisierte Zugänge) abbilden. In diesem Fall der Voucher-Nutzung müssten die Musterdokumente nur geringfügig angepasst werden.

Darüber hinaus existieren vielfältige, weitere Konfigurationsmöglichkeiten. Diese unterscheiden sich meist in Zeit (Dauer), Mehrfachnutzung eines Zugangs und der Möglichkeit der Zuordnung. Daraus ergeben sich die nachfolgenden Leitfragen für die Definition des eigenen Einsatzszenarios:

- Wie lange soll ein Voucher halten? (x Tage/Monate/Jahre)
- Auf wie vielen Geräten soll ein Voucher genutzt werden können?
- Soll ein Voucher einem Gerät bzw. einer Person zugeordnet werden?

Hier können verschiedene Szenarios definiert werden:

- Soll z.B. den Eltern an einem Elternabend der Zugang zum WLAN ermöglicht werden, kann hierfür einfach 1 Voucher erzeugt werden, der nur 12 Stunden gültig ist, aber 100x genutzt werden kann. Hierbei muss dann nicht dokumentiert werden vom wem der Voucher genutzt wird.
- Soll ein Voucher-System für den Unterricht verwendet werden, kann es praktikabler sein Voucher z.B. für ein Halbjahr oder Schuljahr auszustellen. In diesem Fall sollte eine Zuordnung von Vouchern und Personen bzw. Geräten erfolgen, so dass einzelne Voucher auch vor Ablauf ihrer Gültigkeit manuell gesperrt werden können.

Hinweis: Bei der Definition eines konkreten Szenarios sollte auch beachtet werden, ob in einem Missbrauchsfall geeignete Maßnahmen getroffen werden können, um diesen zu beenden und ggf. auch nachzuverfolgen. Hier müssen Datenschutz und Datensicherheit bzw. Jugendschutz mit einander in Einklang gebracht werden.

Welche Auswirkung hat die EU-Datenschutz-Grundverordnung (DSGVO) auf die personenbezogene Datenverarbeitung der Elternvertretungen?

Die Elternvertreterinnen und Elternvertreter sind nach § 76 Absatz 1 Schulgesetz (SchulG) ehrenamtlich tätig und nach den §§ 95 und 96 Landesverwaltungsgesetz (LvWG) zur Verschwiegenheit verpflichtet. Weitergehende Ausführungen zum rechtlichen Status der einzelnen Elternvertreterinnen und der Elternvertreter macht das Schulgesetz nicht. Dasselbe gilt für die Gremien (Schulelternbeirat, Kreiselternbeirat, Landeselternbeirat).

Elternvertreterinnen und Elternvertreter nehmen ihre Aufgaben als natürliche Personen wahr.

Sofern es um die Verarbeitung personenbezogener Daten z. B. der Eltern geht, gelten für die Elternvertretungen und die Gremien somit zunächst die Grundsätze der DSGVO.

Artikel 4 Nr. 7 DSGVO definiert die Verantwortlichen für die Verarbeitung personenbezogener Daten. Danach sind „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Damit kann auch eine natürliche Person "Verantwortlicher" im Sinne der DSGVO sein.

Die Schul-Datenschutzverordnung (SchulDSVO) trifft für die personenbezogene Datenverarbeitung in § 16 folgende Regelung

Datenverarbeitung der Elternvertretungen

(1) Die Elternvertretungen verarbeiten personenbezogene Daten **eigenständig und eigenverantwortlich entsprechend den datenschutzrechtlichen Bestimmungen**. Die Mitwirkung an der Elternvertretung ist freiwillig; **Eltern sind nicht verpflichtet, gegenüber Elternvertretungen personenbezogene Angaben zu machen**.

(2) Zur Unterstützung für ihre Arbeit erhalten die Klassenelternbeiräte und der Schulelternbeirat personenbezogene Daten der Eltern und Lehrkräfte gemäß § 9 Absatz 4 von der Schule.

(3) An die Kreiselternbeiräte und an den Landeselternbeirat werden die für ihre Arbeit erforderlichen Namen und Anschriften nicht durch die Schule, sondern gemäß § 15 Absatz 2 der Wahlverordnung für Elternbeiräte vom 7. Mai 2012 (NBl. MBK. Schl.-H. S. 113), geändert durch Verordnung vom 31. Mai 2017 (NBl. MBWK. Schl.-H. S. 176), durch die Schulelternbeiratsvorsitzende oder den Schulelternbeiratsvorsitzenden übermittelt.

Die personenbezogene Datenverarbeitung hat sich somit im Grundsatz nach den Bestimmungen der DSGVO zu richten, da die Elternvertreterinnen und Elternvertreter als natürliche Personen für die personenbezogene Datenverarbeitung "Verantwortlicher" sind.

Bei der Verarbeitung personenbezogener Daten haben die Elternvertreterinnen und Elternvertreter nicht nur die **Verschwiegenheitsverpflichtung** zu beachten, sondern auch **Maßnahmen** zu ergreifen, um die von ihnen (elektronisch oder konventionell (Papier)) verarbeiteten **personenbezogenen Daten der betroffenen Personen** (Daten von Eltern, Schülerinnen und Schülern) **vor dem Zugriff und Zugang Unbefugter zu schützen** (Artikel 25 Abs. 2 DSGVO).

Ferner haben sie sicherzustellen, dass die personenbezogenen Daten der betroffenen Personen **unverzüglich gelöscht/vernichtet werden, wenn diese nicht mehr zur Aufgabenerfüllung benötigt werden** (Artikel 25 Abs. 2 Satz 2 DSGVO).

Die Bestellung eines Datenschutzbeauftragten ist für die o. g. Gremien nicht erforderlich. Diese Gremien sind lediglich ein Zusammenschluss natürlicher Personen, deren Aufgabenstellung im Schulgesetz zur unabhängigen Wahrnehmung in eigener Verantwortung definiert ist. Solche Gremien sind in Artikel 37 DSGVO nicht benannt.
[Link] Infoseite des Bildungsministeriums zur Elternarbeit

Welche grundlegenden Bedingungen aus Datenschutzsicht muss eine Schulhomepage erfüllen?

Seit 25.05.2018 gelten die Vorschriften der EU-Datenschutz-Grundverordnung (DSGVO), die umfassende Informationspflichten der verantwortlichen Stellen gegenüber den betroffenen Personen vorschreiben.

Sofern Schulen eigene Webseiten betreiben, sind sie verpflichtet, entsprechende Datenschutzerklärungen zu veröffentlichen.

Die Datenschutzerklärungen müssen auf die jeweiligen Verhältnisse der Webseite abgestellt werden. Daher kann in dieser FAQ kein allgemein anzuwendendes Muster mit vorgefertigten Formulierungen bereitgestellt werden.

Beigefügt sind als Unterstützung

- Hinweise zu den Informationspflichten im Allgemeinen und im Zusammenhang mit einem Webauftritt (Link zum ULD).
- Ein Muster für eine Datenschutzerklärung (s.u.) und ein Impressum (s.u.) einer statischen Schulhomepage, die maximal ein Kontaktformular zur Interaktion enthält.
- eine Checkliste (s.u.), mit deren Hilfe wichtige Punkte geprüft werden können. Die Liste erhebt keinen Anspruch auf Vollständigkeit.

Die möglicherweise erforderlichen weiteren Informationen zur Datenverarbeitung müssen an die tatsächlichen Verhältnisse der Webseite angepasst werden.

Bei der Gestaltung einer Schulhomepage sollten folgende Punkte beachtet werden:

Technische Realisierung:

- Hosting bei einem Provider innerhalb Deutschlands/der EU (Auftragsverarbeitung).
- DSGVO-konforme Datenschutzhinweise, korrektes Impressum.
- Datenschutzhinweise und Impressum müssen von der Startseite und allen Unterseiten direkt erreichbar sein.

- Keine Cookies außer der sog. Sessioncookies (technisch notwendig).
- Cookie-Hinweis muss beim Aufruf der Seite erscheinen (Pop-Up).
- Keine Nutzung von Google-Fonts, sondern von auf dem Webserver lokal gespeicherten Schriftarten
- Kein Einsatz von Analysetools wie Google-Analytics o.ä.
- Nutzungsauswertung/Analyse darf maximal lokal erfolgen (bspw. durch Matomo)

Unzulässige Inhalte auf einer Schulhomepage (kein Anspruch auf Vollständigkeit) sind:

- Fotos/Bilder/Grafiken/Namensnennungen, für die keine Einwilligung zur Veröffentlichung vorliegt bzw. nicht mehr nachgewiesen werden kann. (bspw. Bilder von SuS, die bereits die Schule verlassen haben und deren Schülerakte gelöscht wurde)
- Gleiches gilt für Kontaktlisten
- Fotos aus anderen Quellen, für die keine Nutzungsrechte bestehen (Urheberrecht)
- Eingebettete Videos, die einen Player eines nicht datenschutzkonformen Anbieters nutzen
- Plugins/Like-Buttons von Sozialen Netzwerken oder Streamingdiensten/Videoportalen

Anfahrtsbeschreibungen sollten, wenn erforderlich, mit Openstreetmap als OpenSource-Alternative realisiert werden.

Veröffentlichung von Namen, Kontaktdaten

- Namensnennungen und Angaben privater Telefonnummern oder Mailadressen von Kolleginnen und Kollegen dürfen nur erfolgen, wenn hierfür die Einwilligungen vorliegen.
- Dies gilt nicht für
  - die Schulleitung (Funktionsträger)
  - Ansprechpartner anderer Behörden, deren Daten im Internet bereits veröffentlicht sind
  - dienstliche Telefonnummern

[Datei] Muster Datenschutzerklärung
[Datei] Muster Impressum
[Datei] Checkliste Schulhomepage

Welche Sicherheitsmaßnahmen zur Gewährleistung von Datenschutz und Datensicherheit kann Schule ergreifen?

Die EU-Datenschutzgrundverordnung (DSGVO) fordert zum Schutz der Daten und damit zur Gewährleistung des Datenschutzes (Schutz der Personen und Ihrer Rechte und Freiheiten) und der Datensicherheit (Schutz der Daten vor Verlust, Veränderung, Offenlegung) die Ergreifung sogenannter technischer und organisatorischer Maßnahmen (TOM). Hierbei handelt es sich um einen der Grundsätze der Verarbeitung nach Artikel 5 DSGVO. Wie TOMs ausgewählt werden und welche Kriterien dabei zu beachten sind, ergibt sich aus Artikel 32 DSGVO.

Auswahl und Implementierung von TOMs sollen zu einer Risikominimierung beitragen und berücksichtigen sowohl die Eintrittswahrscheinlichkeit für eine bestimmte Situation als auch die Schwere des zu erwartenden Schadens für die betroffenen Personen. Die TOMs sollen dem Stand der Technik entsprechen und regelmäßig überprüft werden.

Die Schulleitung ist verantwortlich für die Dokumentation der TOMs und die Überwachung der Einhaltung sowie die regelmäßige Evaluation.

Für die Schulen wurde zentral ein Basis-IT-Sicherheitskonzept entwickelt, welches gleichzeitig eine Bestandsaufnahme (IST-Situation) ermöglicht und im ausgefüllten Zustand auch als Nachweis im Sinne der DSGVO fungiert. Weitere Erläuterungen können dem Konzept entnommen werden. Das Muster ist dieser FAQ beigefügt.

Risikominimierung kann darüber hinaus neben technischen Maßnahmen auch durch organisatorische Maßnahmen erreicht werden, wobei technische Maßnahmen immer vorzuziehen sind. Einfach anzuwendende und praktikable Erstmaßnahmen können dem beigefügten Infoblatt "Sicheres Arbeiten" entnommen werden.

Darüber hinaus sind technische und organisatorische Maßnahmen spezifisch an die Gegebenheiten vor Ort anzupassen.

Wichtig ist, dass organisatorische Maßnahmen verbindlich (bspw. durch eine Belehrung oder Dienstanweisung), allen Beteiligten bekannt und praktikabel umzusetzen sind, damit die nötige Sensibilität und auch Akzeptanz erreicht werden kann.

[Datei] Sicheres_Arbeiten_Basics
[Datei] Muster-Basis-IT-Sicherheitskonzept

Wenn Eltern am Unterricht ihres Kindes teilnehmen (sog. Hospitieren), dürfen sie dabei Notizen fertigen und diese anderen Eltern zugänglich machen?

Wenn Eltern auf der Grundlage von § 11 Abs. 4 Schulgesetz am Unterricht teilnehmen, tun sie dies als Privatpersonen. Im Gegensatz zu Elternbeiräten unterliegen sie keinen Verschwiegenheitspflichten. Erlangte Informationen, beispielsweise über den Unterrichtsstil der Lehrkraft, dürften von ihnen festgehalten und anderen Personen bekannt gemacht werden. Natürlich hat die Schule bzw. die betroffene Lehrkraft das Recht, sich gegen unwahre Behauptungen zur Wehr zu setzen.

Wer ist der Datenschutzbeauftragte meiner Schule und welche Aufgaben hat dieser?

Mit Inkrafttreten der EU-Datenschutzgrundverordnung am 25.05.2018 wurden alle öffentlichen Stellen verpflichtet, einen Datenschutzbeauftragten zu bennen. Das Bildungsministerium hat in Abstimmung mit der Aufsichtsbehörde entschieden, hierfür eine zentrale Position im Ministerium zu schaffen. Somit existiert für allle öffentlichen Schulen ein zentraler Ansprechpartner, der auch alleinig an die Aufsichtsbehörde gemeldet wurde.

Schulen benennen daher keinen eigenen Datenschutzbeauftragten gegenüber der Aufsichtsbehörde (ULD).

Nichtsdestotrotz ist es empfehlenswert, eigene Datenschutzkompetenz an Schule aufzubauen und ggf. einen weiteren Ansprechpartner neben der nach § 2 Schuldatenschutzverordnung (SchulDSVO) für die Organisation und Einhaltung des Datenschutzes verantwortliche Schulleitung zu haben. Diese Datenschutzkoordinatoren können dann auch als Bindeglied zum zentralen Datenschutzbeauftragten für die öffentlichen Schulen fungieren.

In allen Belangen, bei denen die Nennung des Datenschutzbeauftragten erforderlich ist (bspw. Datenschutzhinweise auf der Schulhomepage, Anmeldeformulare, Einwilligungen gegenüber der Schule etc.) sind folgende Angaben aufzunehmen:

Die/Der Datenschutzbeauftragte der Schule ist

Zentraler Datenschutzbeauftragter des Bildungsministeriums für die öffentlichen Schulen
DatenschutzbeauftragterSchule@bimi.landsh.de
Telefon: +49 431 988 2452

Die Aufgaben des Datenschutzbeauftragten sind insbesondere:

- Ansprechpartner in Datenschutzfragen für alle an Schule Beteiligten
- Beratung auf Anfrage

- Durchführung von Schulungen und Sensibilisierungsveranstaltungen (bspw. Schulentwicklungstage, IQSH-Fortbildungen)
- Bereitsstellung von allgemeinen Informationen zum Datenschutz (dieses Infoportal, Muster, Handreichungen etc.)
- Unterstützung bei der Kommunikation mit der Aufsichtsbehörde im Falle von Datenpannen
- Zusammenarbeit mit der Aufsichtsbehörde
- Überprüfung der Einhaltung der datenschutzrechtlichen Vorschriften und Vorgaben

[Datei] Informationen des Bildungsministeriums zum Inkrafttreten der DSGVO

Wer ist für die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten (VVT) verantwortlich und wie ist dieses aufgebaut?

Die EU-Datenschutzgrundverordnung (DSGVO) hat als ein übergeordnetes Ziel die Schaffung maximaler Transparenz hinsichtlich der Ausgestaltung, des Umfangs und der Sicherheit bei der Verarbeitung personenbezogener Daten durch die Verantwortlichen. Im Schulumfeld sind dies Schulen, das Ministerium, Schulämter, Schulträger, Elternvertretungen und andere Institutionen/Unternehmen/Behörden, die Daten von Schülerinnen, Schülern, Eltern und auch Beschäftigten verarbeiten.

Diese Grundsätze der Verarbeitung sind in Artikel 5 Absatz 1 DSGVO beschrieben.

Darüber hinaus stehen den, Personen deren Daten verarbeitet werden, umfangreiche Rechte wie beispielsweise Information vor einer Datenerhebung oder Auskunft zu gespeicherten Daten zu.

Die Betroffenenrechte sind in den Artikeln 12 - 23 der DSGVO beschrieben.

Um die Einhaltung der Grundsätze nachweisen zu können und darüber transparent zu informieren bzw. die Betroffenenrechte zu wahren ist es erforderlich, dass Verarbeitungsprozesse in Schule dokumentiert sind. Diese Rechenschafts- und Dokumentationspflicht wurde ebenfalls als ein Grundpfeiler in Artikel 5 Absatz 2 DSGVO aufgenommen.

Ein zentrales Dokument ist hierbei das Verzeichnis von Verarbeitungstätigkeiten, in dem alle übergeordneten Verarbeitungstätigkeiten einer datenverarbeitenden Stelle beschrieben werden. Der Inhalt des VVT ist durch Artikel 30 DSGVO festgelegt, für die übersichtliche Erfassung existieren Musterdokumente (siehe unten).

Verantwortlich für die Erstellung und die Erfüllung der Dokumenations- und Rechenschaftspflichten im Ganzen ist die Schulleitung (§ 2 SchulDSVO).

Für die Schulen wurde ein Muster-VVT erarbeitet (siehe unten), welches die primär in Schule anfallenden Verarbeitungstätigkeiten abbildet und somit den Schulen einen wesentlichen Teil der Erstellungsarbeit abnimmt. Die Schule muss hier nur das Vorblatt mit den Schuldaten komplettieren und innerhalb der Verarbeitungstätigkeiten ggf. Fachverantwortliche benennen und die Angaben auf mögliche schulspezifische Angaben hin prüfen und ggf. anpassen.

Nur für nicht im Muster-VVT erfasste Verarbeitungstätigkeiten muss die Schule auf Basis der Mustervorlage eigene Einträge im VVT ergänzen.
[Datei] Muster-VVT
[Datei] Hinweise zum VVT
[Datei] Kurzinfo VVT
[Datei] Muster_VT

Wie können Schülerdaten auf einem Stand-Alone-PC der Schulverwaltung vor unbefugter Kenntnisnahme geschützt werden, wenn das Gerät nicht ausreichend vor Diebstahl geschützt werden kann?

Wenn aufgrund der räumlichen Situation in der Schule ein Diebstahl der Hardware nicht ausgeschlossen werden kann, sollten die auf dem PC gespeicherten Daten nur in verschlüsselter Form auf der Festplatte gespeichert werden. Hierfür gibt es kostengünstige oder sogar kostenfreie Software, die es komfortabel ermöglichen, die Daten sicher zu verschlüsseln. Die Programme erstellen ein virtuelles Laufwerk auf der Festplatte, in dem alle Daten verschlüsselt abgelegt werden. Dieses Laufwerk kann versteckt werden, so dass es auch nicht im Explorer-Fenster erscheint.

In jedem Falle sollte auf tägliche Datensicherungen (Backups) Wert gelegt werden. Das Sicherungsmedium sollte nicht in der Nähe des PC, sondern an einem sicheren Ort gelagert werden. Eine sichere Datenhaltung kann auch durch die Verwendung einer Wechselfestplatte oder eines verschlüsselten USB-Sticks erreicht werden, wenn diese nach Dienstschluss an einem geschützten Ort (beispielsweise in einem Tresor) aufbewahrt werden.