Handreichung

Datenschutzanforderungen in der Schul-IT

Zweck

Ziel der Handreichung ist es, für Schulträger Transparenz über die Zuständigkeiten und Aufgaben im Bereich des Datenschutzes zu schaffen. Die Handreichung dient als Information, welche datenschutzrechtlichen Aufgaben es grundsätzlich gibt und welche Aufgaben von Schule oder Schulträger übernommen werden müssen. So sollen Schulträger in die Lage versetzt werden, Schulen ein besseres Verständnis für ihre Datenschutz-Aufgaben zu vermitteln und gemeinsam mit den Schulleitungen Datenschutz an Schulen umzusetzen.

Anwendungsempfehlungen

Diese Handreichung unterstützt Sie als Schulträger bei der Abgrenzung der datenschutzrechtlichen Pflichten im Zusammenspiel von Schule und Schulträger.

Die Muster-IT-Materialien auf dieser Webseite wurden im Rahmen einer Ressortforschung des Bundesministeriums der Finanzen (BMF) erstellt, die aus Mitteln des Deutschen Aufbau- und Resilienzplans (DARP) finanziert wurde.

Bundesministerium der Finanzen

Finanziert von der Europäischen Union
NextGenerationEU

Inhaltsverzeichnis

Einleitung

Der Schutz personenbezogener Daten hat in der heutigen digitalen Gesellschaft eine immer größere Bedeutung erlangt. Insbesondere Schulträger und Schulen müssen sich bewusst sein, dass sie mit einer Vielzahl sensibler Informationen arbeiten. Die Gewährleistung des Datenschutzes der Schülerinnen und Schüler, ihrer Eltern, der Lehrkräfte und weiterer Mitarbeitenden der Schule ist von höchster Wichtigkeit. Erfolgreicher Datenschutz kann im Kontext Schule jedoch nur erreicht werden, wenn Schulleitungen als Verantwortliche für die Prozesse innerhalb der Schule und die kommunalen Schulträger als Verantwortliche für die digitale Ausstattung der Schulen gut zusammenarbeiten. Diese Handreichung richtet sich an kommunale Schulträger und hat das Ziel, das Bewusstsein für Datenschutzfragen im Schul-IT-Betrieb zu schärfen und praktische Hinweise für die Einhaltung gesetzlicher Vorschriften durch Schulträger und Schulen zu bieten.

Zielgruppe

Die Handreichung richtet sich an Schulträger sowie zur Information ihrer Schulen; konkret an für die Einhaltung datenschutzrechtlicher Vorgaben verantwortliche Personen wie Behördenleitung (an den Schulen Schulleitung), Datenschutzbeauftragte und IT-Verantwortliche.

Aufbau der Handreichung

Diese Handreichung umfasst drei Hauptbereiche:

1. Grundverständnis Datenschutzrecht
2. Pflichten aus dem Datenschutzrecht
3. Checklisten für die Einhaltung von Datenschutzpflichten

Hinweise

An allen relevanten Stellen wird darauf hingewiesen, ob es sich um eine Pflicht des Schulträgers oder der Schule oder gegebenenfalls eine gemeinsame Pflicht handelt.

Der Bereich Grundverständnis Datenschutzrecht bildet die Grundlage für die nachfolgenden Pflichten. Hier geht es um Themen wie die einschlägigen Normen, die grundsätzliche Rechtmäßigkeit von Datenverarbeitungen und die Aufteilung der datenschutzrechtlichen Verantwortung zwischen Schulträger und Schule. Der Bereich Pflichten aus dem Datenschutzrecht stellt einzelne Pflichten wie das Bereitstellen einer Datenschutzinformation oder das Durchführen einer Datenschutzfolgenabschätzung vor. Der abschließende Bereich Checklisten dient einem schnellen Überblick über die typischerweise anfallenden Datenschutzaufgaben und Fragestellungen.

Hinweise

CHECKLISTE FÜR SCHULTRÄGER UND SCHULEN: Es werden zwei Checklisten angeboten, einmal für Schulträger und einmal für Schulen.

Grundverständnis Datenschutzrecht
Verantwortlichkeit nach DSGVO

Die Pflichten aus der DSGVO binden den Verantwortlichen im Sinne der DSGVO.

Hinweise

DEFINITION DES VERANTWORTLICHEN NACH ART. 4 NR. 7 DSGVO: „Verantwortlicher" (ist) 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.

Entscheidend ist also, wer die Zwecke und Mittel der Datenverarbeitung festlegt. Diese Definition, die für den öffentlichen und nicht-öffentlichen Bereich gleichermaßen gilt, trifft im Verwaltungsbereich regelmäßig auf Abgrenzungsschwierigkeiten.

Zwecke der Datenverarbeitung

Die Zwecke der Datenverarbeitung sind regelmäßig gesetzlich (z.B. durch das Schulgesetz) vorgegeben. Verwaltungshandeln – und damit auch das Handeln von Lehrkräften, Schulleitung und weiteren Beschäftigten der Schulen – ist an die Vorgaben aus dem eigenem Fachrecht gebunden. Zugleich eröffnen die rechtlichen Vorgaben Entscheidungsspielräume, innerhalb derer die Schulleitungen für ihre Schulen eigenständige Entscheidungen treffen können. Dementsprechend weisen viele Landesschulgesetze die datenschutzrechtliche Verantwortung den Schulen zu.

Mittel der Datenverarbeitung

Zu den Mitteln der Datenverarbeitung zählen IT-Infrastruktur und Anwendungen, die wiederum in vielen Kommunen vom Schulträger zentral und einheitlich vorgegeben werden. Daraus ergeben sich Konstellationen, die nicht einfach mit der Logik der DSGVO zur Deckung zu bringen sind.

Schrittweise etabliert sich hier eine Sichtweise, die auch in einem Beschluss des OVG Münster (Az. 19 B 417/22) vom 22.02.2023 zum Ausdruck gekommen ist: Die Schulträger tragen keine unmittelbare Verantwortung den Betroffenen gegenüber, wie sie von der DSGVO als Verantwortlichkeit normiert ist. Da die Schulträger aber (meistens) die Verantwortung für die IT-Ausstattung tragen und de facto den Schulen die Mittel der Datenverarbeitung alternativlos vorgeben, entsteht eine indirekte, vorgelagerte DSGVO-Verantwortlichkeit.

Indirekte Verantwortung der Schulträger

Die Schulträger müssen sicherstellen, dass die von Ihnen den Schulen zur Verfügung gestellte oder zur Nutzung genehmigte IT-Ausstattung den Anforderungen an einen datenschutzkonformen Einsatz an den Schulen genügt.

Den Schulen fehlen regelmäßig die Ressourcen, Hardware und vor allem Software, insbesondere Cloud-Dienste (Anwendungen, die auf Servern außerhalb der Schule laufen), auf ihre Datenschutzkonformität zu prüfen. Sie müssen sich hierfür auf Prüfungen durch die Schulträger verlassen können.

Indirekte Verantwortung höherer Verwaltungsebenen

Soweit Anwendungen zentral vom Kultusministerium oder einer anderen Verwaltungsebene oberhalb des Schulträgers vorgegeben werden, muss der Schulträger sich wiederum dieser Ebene gegenüber auf Datenschutzkonformität verlassen können.

Rahmendatenschutzkonzept

Der Nachweis der Datenschutzkonformität wird regelmäßig in sogenannten Rahmendatenschutzkonzepten („RDSK") dokumentiert. Ein RDSK ist kein Dokument, das die DSGVO oder ein anderes Gesetze vorsieht. Ein RDSK ist aber ein adäquater Ansatz, um der datenschutzrechtlichen Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO nachzukommen.

ABGRENZUNG VERANTWORTLICHKEIT SCHULTRÄGER ZU SCHULE: Die Definition aus dem Datenschutzrecht, wer gegenüber den von einer Verarbeitung personenbezogener Daten betroffenen Menschen als der Verantwortliche im Sinne der DSGVO einzuordnen ist, ist auf den Verwaltungsbereich schwer anwendbar.

Nach der DSGVO kommt es darauf an, wer die Zwecke und Mittel der Datenverarbeitung festlegt. Für Verwaltungshandeln, wie es der Betrieb einer (staatlichen) Schule ist, sind die Zwecke weitestgehend gesetzlich vorgegeben und werden die Mittel regelmäßig von höheren Verwaltungsebenen bereitgestellt.

Mit Blick auf den Grundsatz der Schulautonomie, die den Schulen bzw. ihrer Leitung Entscheidungsfreiheiten überlässt, ist regelmäßig die Schule für die Verarbeitung personenbezogener Daten in ihrem Tätigkeitsbereich die Verantwortliche im Sinne der DSGVO.

Für höhere Verwaltungsebenen wie die Schulträger wird von einer allgemeinen Pflicht ausgegangen, den Schulen IT (Hardware wie Software) in einer Weise zur Verfügung zu stellen, die Schulen einen datenschutzkonformen Einsatz ermöglicht. In Verbindung mit der Rechenschaftspflicht aus der DSGVO ergibt sich für die Schulträger gegenüber den Schulen die Pflicht Rahmendatenschutzkonzepte zur Verfügung zu stellen, die die Datenschutzkonformität der Mittel nachweisen.

Die Schulen können im Rahmen ihrer Datenschutzpflichten, insbesondere ihrer Rechenschaftspflicht, auf die Rahmendatenschutzkonzepte und gegebenefalls ergänzende Musterdokumente des Schulträgers verweisen.

Datenschutzkonzept

In Ergänzung zum Rahmendatenschutzkonzept wird DSGVO-Verantwortlichen, also in diesem Zusammenhang den einzelnen Schulen, zur Erfüllung ihrer unmittelbaren Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO ein Datenschutzkonzept („DSK“) empfohlen. Wo nach Art. 35 DSGVO für einen Verarbeitungsprozess eine Datenschutzfolgenabschätzung („DSFA“) erforderlich ist, tritt diese neben das DSK.

Musterdokumente

Da vielen Schulen auch die Ressourcen zur vollumfänglichen Erstellung von DSK und DSFA fehlen, ist es naheliegend, dass die Schulträger neben dem RDSK (aus eigener Verantwortung heraus) auch Muster-Dokumente für das DSK und die DSFA der einzelnen Schulen zur Verfügung stellen. Zusätzlich können die Schulträger den Schulen Muster für die Datenschutzinformation (Art. 12 bis 14 DSGVO) und den Eintrag in das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO) bereitstellen. Auch Muster für die Prozesse auf Auskunft (Art. 15 DSGVO) oder Löschung (Art. 17 DSGVO) und weitere Betroffenenrechte aus der DSGVO sind eine wertvolle Unterstützung für die Schulen, damit diese ihre Kräfte auf ihre schulischen Kernaufgaben fokussieren können.

Einschlägige Normen

Das Datenschutzrecht ist im Kern europäisches Recht, das von der Datenschutz-Grundverordnung („DSGVO“) vorgegeben wird. Die DSGVO umfasst alle wesentlichen Regelungen zum Datenschutz.

Von zentraler Bedeutung für die Einhaltung des Datenschutzes an Schulen ist das Schulrecht, aus dem sich die Zwecke und darüber die Rechtsgrundlagen der Datenverarbeitung ergeben.

Hinweise

Diese Handreichung richtet sich an Schulträger in der gesamten Bundesrepublik Deutschland. Sie geht nicht auf die Details aus dem jeweiligen Landesrecht ein.

Das Schulrecht enthält – im Detail unterschiedlich von Bundesland zu Bundesland – Regelungen, die abstrakte Vorgaben aus der DSGVO für datenverarbeitende Prozesse und Strukturen im Schulbereich konkretisieren. Für jeden Schulträger und jede Schule ist es zwingend erforderlich, sich über die konkreten Regelungen mit Datenschutzbezug im eigenen Schulrecht zu informieren. Das jeweilige Kultusministerium gibt hierzu Auskunft.

Für staatliche Schulen greifen auch Vorgaben aus den Landesdatenschutzgesetzen („LDSG“). Hieraus ergeben sich aber nur selten konkrete Vorgaben, die als zusätzlicher Faktor im Schuldatenschutz zu berücksichtigen wären. Hierzu sollten die einzelnen Kultusministerien der Länder Auskunft geben können, ob im jeweiligen Land Regelungen des LDSG von Schulträgern oder Schulen zu beachten sind.

Ebenfalls von Relevanz ist das Dienstrecht des jeweiligen Bundeslandes. Hieraus ergibt sich regelmäßig eine gesetzliche Verpflichtung der Beschäftigten auf die Vertraulichkeit (also den datenschutzkonformen Umgang mit personenbezogenen Daten), so dass Beschäftigte nicht ausdrücklich oder zusätzlich auf die Vertraulichkeit verpflichtet werden müssen. Zusätzlich enthält das Dienstrecht der Länder regelmäßig die DSGVO ergänzende Vorgaben zum Umgang mit den Daten der Beschäftigten. Auch zu den einschlägigen Vorgaben aus dem jeweiligen Landesdienstrecht sollten die einzelnen Kultusministerien Auskunft geben können.

Rechtmäßigkeit der Datenverarbeitung

Wichtig für das Verständnis von Datenschutzrecht ist, dass es sich hierbei um unmittelbaren Grundrechtsschutz handelt. Wird der Datenschutz nicht eingehalten, wird mindestens ein Grundrecht der Betroffenen verletzt. Das Grundrecht ist in Art. 8 der EU-Grundrechtscharta verankert und wurde außerdem für Deutschland vom Bundesverfassungsgericht 1983 im Volkszählungsurteil entwickelt.

Nach der Grundlogik der Artikel 6 und 9 DSGVO ist die Verarbeitung personenbezogener Daten verboten, außer eine Rechtsgrundlage gestattet diese Verarbeitung.

Artikel 6 DSGVO

Art. 6 ist die Grundsatznorm, die für die Rechtmäßigkeit der Datenverarbeitungen innerhalb des Verwaltungshandelns – und Schulbetrieb ist insoweit Verwaltungshandeln – als zentrale Brücke die Regelung in Art. 6 Abs. 1 e) DSGVO enthält.

ART. 6 ABS. 1 E) DSGVO: Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: (...)

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; (...)

Somit ergibt sich die Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Schulbetrieb über Art. 6 Abs. 1 e) DSGVO aus dem jeweils einschlägigen Verwaltungsrecht. Das ist im Schulbetrieb weitestgehend das Schulrecht des jeweiligen Bundeslandes und ergänzend mit Blick auf den Beschäftigtendatenschutz das Dienstrecht des Landes.

Die Rechtmäßigkeitsprüfung setzt sich regelmäßig aus drei Schritten zusammen:

1. Dient die konkrete Verarbeitung personenbezogener Daten einem legitimen Zweck – also einem Zweck, der aus dem Schul- oder Dienstrecht vorgegeben ist?

2. Ist die konkrete Verarbeitung personenbezogener Daten zur Erreichung dieses Zweckes erforderlich? Oder ist der Zweck gleichermaßen auch über Prozesse erreichbar, die die Datenschutzrechte der Betroffenen weniger einschränken?

3. Greifen zusätzliche Normen, die die konkrete Art der Datenverarbeitung untersagen oder von der Einhaltung zusätzlicher Vorgaben abhängig machen (z.B. gesetzlich vorgegebene Löschfristen)?

Artikel 9 DSGVO

Art. 9 ergänzt Art. 6 DSGVO mit Blick auf besonders schützenswerte Daten.

BESONDERS SCHÜTZENSWERTE DATEN NACH ART. 9 DSGVO:

- Rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten zur eindeutigen Identifizierung einer Person
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Überzeugung

Die Verarbeitung von Daten nach Art. 9 Abs. 1 DSGVO ist nur in bestimmten Fällen (Themenbereichen) nach Abs. 2 des Artikels gestattet. Auf die Darstellung der Fälle nach Art. 9 Abs. 2 DSGVO wird hier verzichtet, da zugleich auch die Rechtsgrundlage nach Art. 6 Abs. 1 e) DSGVO erfüllt sein muss und alle einschlägigen Regelungen, soweit nach ihnen die Verarbeitung einer Artikel-9-Kategorie zulässig ist, mindestens eine der Fallgruppen nach Art. 9 Abs. 2 DSGVO mit abdecken sollten.

Sollte aber die Verarbeitung einer der oben genannten Datengruppen – gerade auch unter dem Blickpunkt der Erforderlichkeit – im Rahmen der grundsätzlichen Prüfung nach Art. 6 DSGVO zweifelhaft sein, sind die Fälle nach Art. 9 Abs. 2 DSGVO zwingend als Orientierung hinzuzuziehen und sollte eine eigenständige Prüfung nach Art. 9 DSGVO erfolgen.

Einwilligungen

Sowohl Art. 6 Abs. 1 a) wie Art. 9 Abs. 2 a) DSGVO verweisen auf Einwilligungen als Rechtsgrundlage. Einwilligungen sind aber nur als Auffanglösung gedacht für Arten von Datenverarbeitungen, die nicht unter die Zwecke des Schul- oder Dienstrechts fallen und dennoch legitimer Natur sind. Die Anforderungen an die Rechtmäßigkeit einer Einwilligung nach Art. 7 und 8 DSGVO sind vergleichsweise hoch und gerade mit Blick auf das Kriterium der Freiwilligkeit schwer darstellbar. Zudem sind Einwilligungen jederzeit widerrufbar und damit keine Grundlage für eine auf Dauer angelegte Verarbeitung personenbezogener Daten.

In allen Konstellationen, in denen keine Rechtsgrundlage nach Art. 6 Abs. 1 e) DSGVO gegeben ist, sollte die oder der zuständige Datenschutzbeauftragte oder das zuständige Rechtsamt konsultiert werden, ob Einwilligungen eine sinnvolle Alternative sind und wie sie rechtskonform auszugestalten sind.

Eine gängige und wenig komplexe Einwilligungssituation ist die Zustimmung, Kontaktdaten der Klasse und der Eltern den anderen Familien zur Verfügung zu stellen. Die Konstellation ist leicht verständlich. Familien, die ihre Daten nicht bereitstellen wollen, müssen dies selbstverständlich auch nicht.

Soweit es um den Einsatz einer IT-Anwendung geht, die ein Dienst der Informationsgesellschaft im Sinne des Art. 8 DSGVO ist, und eine Betroffene oder ein Betroffener das 16. Lebensjahr noch nicht vollendet hat, ist zusätzlich zur Einwilligung der Kinder und Jugendlichen (unter 16 Jahren) eine Zustimmung der Sorgeberechtigten erforderlich.

Sonstige Rechtmäßigkeitsvoraussetzungen

Die Frage der Rechtsgrundlage mit ihrem Fokus auf den legitimen Zweck und die Erforderlichkeit steht zentral im Mittelpunkt der datenschutzrechtlichen Rechtmäßigkeit. Art. 5 DSGVO legt neben der Rechtmäßigkeit der Verarbeitung durch Vorliegen einer Rechtsgrundlage weitere grundsätzliche Anforderungen an die Verarbeitung personenbezogener Daten fest. Die in Art. 5 DSGVO knapp genannten Anforderungen finden ihre Ausprägung in weiteren Artikeln der DSGVO. Diese werden nachfolgend im Bereich Pflichten aus dem Datenschutzrecht näher vorgestellt.

Datenschutz, Datensicherheit und Informationssicherheit

Für die Auseinandersetzung mit dem Datenschutz ist es hilfreich, zentrale Begriffe in den richtigen Zusammenhang zu stellen.

Datenschutz

Der Ausdruck Datenschutz ist der Oberbegriff für das Rechtsgebiet, wie es durch Art. 8 EU-Grundrechtscharta und die DSGVO im Zusammenspiel mit weiteren datenschutzrechtlichen Normen vorgegeben ist.

Datensicherheit

Die Sicherheit der Daten ist ein wesentlicher Baustein rechtkonformer Verarbeitung personenbezogener Daten (siehe Art. 32 DSGVO). Mit Sicherheit ist der Schutz der Daten anhand der Ziele Vertraulichkeit, Integrität und Verfügbarkeit gemeint. Da Datenschutz Grundrechtsschutz und damit Schutz natürlicher von der Datenverarbeitung betroffener Personen ist, dient die Datensicherheit dem Schutz dieser Menschen. Entscheidend ist dieser Punkt bei der Strukturierung einer Datenschutzfolgenabschätzung. Diese muss sich nur mit Risiken aus-

einandersetzen, deren Verwirklichung für die betroffenen Menschen schädlich wäre. Risiken, die allein die datenverarbeitende Organisation schädigen können, sind aus Datenschutzperspektive irrelevant.

Informationssicherheit

Die Informationssicherheit entspricht in vielerlei Hinsicht der Datensicherheit. Die Informationssicherheit ist aber über das BSI-Gesetz geregelt und fällt unter die Aufsicht des Bundesamts für die Sicherheit in der Informationstechnik („BSI“) sowie in Bundesländern, die ein Landesamt für die Sicherheit in der Informationstechnik haben, unter deren Aufsicht. Der zentrale Unterschied ist die Zwecksetzung: Die Informationssicherheit dient dem Schutz der Organisation, nicht der betroffenen Menschen. Da staatliche Stellen aus ihrer Grundrechtsbindung heraus grundsätzlich den Schutz der Grundrechte als eigenes Ziel verfolgen (müssen), sind die Unterschiede zur Datensicherheit tatsächlich gering.

Datenschutzrisiko und Schutzbedarfskategorie

Prozesse aus der Informationssicherheit sind im IT-Umfeld regelmäßig besser etabliert als Datenschutzprozesse. Daher wird auch in Datenschutzzusammenhängen oft über Schutzbedarfskategorien diskutiert – einem Begriff aus der Informationssicherheit. Die Kategorien „normal“, „hoch“ und „sehr hoch“ sind der DSGVO und anderen Datenschutznormen aber fremd. Das Datenschutzrecht spricht nur von Risiken:

- Kein oder nur geringes Risiko
- (Normales) Risiko
- Hohes Risiko

Eine vertiefte Auseinandersetzung mit den unterschiedlichen Perspektiven bedarf es meist nicht, aber ein Verständnis für die unterschiedliche Ausgangslage ist hilfreich – gerade im Austausch zwischen Datenschutzbeauftragten und Informationssicherheitsbeauftragten.

Das Standard-Datenschutzmodell („SDM“) der Datenschutzkonferenz („DSK“) der deutschen Datenschutzaufsichtsbehörden, das ein Modell zur Risikobewertung und Zuordnung von Schutzmaßnahmen aus Datenschutzperspektive auf Basis des IT-Grundschutzkompendiums ist, wurden die Risiken aus der DSGVO ins Verhältnis gesetzt zu den **Schutzbedarfskategorien der Informationssicherheit:**

- Kein oder nur geringes Risiko wie das (normale) Risiko entsprechen der Schutzbedarfskategorie normal.
- Ein hohes Risiko entspricht der Schutzbedarfskategorie hoch.

- Für die Schutzbedarfskategorie sehr hoch, die durch essenzielle Gefahren für die Organisation und die ihr zugeordneten Personen definiert ist (Ausfall elementarer staatlicher Leistungen über eine nicht tolerable Zeitspanne hinaus, Gefahr für Leib und Leben), gibt es laut SDM im Datenschutz keine Entsprechung.

Diese Grundaussage ist schon allein deswegen begrüßenswert, weil die Schutzbedarfskategorie sehr hoch Sicherheitsmaßnahmen erfordert, die von einer Schule kaum zu erbringen sind.

Abweichend von den Aussagen des SDM könnte man die Verarbeitung von personenbezogenen Daten mit der Kategorie sehr hoch gleichsetzen, wenn ein Verlust der Vertraulichkeit mit Gefahren für Leib und Leben einhergehen würde, wie es zum Beispiel für Kronzeugen im Bereich schwerster Kriminalität oder Kinder denkbar wäre, deren Aufenthaltsort dringend vor einer außerordentlich gewalttätigen Person geschützt werden muss.

All dies sind aber Sonderkonstellationen, die kaum im Rahmen allgemeiner IT-Prozesse planbar und abbildbar sind. Daher spielt die höchste Schutzbedarfskategorie im Schulalltag keine Rolle.

Pflichten aus dem Datenschutzrecht

Art. 5 DSGVO fasst die Pflichten aus dem Datenschutz zusammen, die nachfolgenden Artikel konkretisieren die zentralen Pflichten. Die letztlich elementare Frage, ob eine Verarbeitung personenbezogener Daten in der konkreten Form datenschutzkonform ist, liegt in der oben beschriebenen Prüfung, ob eine Rechtsgrundlage vorliegt, die diese Datenverarbeitung abdeckt. Im Mittelpunkt dieser Prüfung stehen die Fragen nach dem legitimen Zweck der Datenverarbeitung und nach der Erforderlichkeit der Datenverarbeitung in der angestrebten Art und Weise.

Zusätzlich zu dieser Kernfrage ergeben sich aus dem Datenschutzrecht ergänzende Pflichten, die hier vorgestellt werden sollen. Die Darstellung beschränkt sich hierbei auf Fragen, die sich im Zusammenhang mit der IT-Ausstattung der Schulen ergeben. Die Pflichten gelten mehr oder weniger identisch für analoge Datenverarbeitungen, ohne das hier auf analoge Themen weiter eingegangen wird.

Berechtigungskonzept und Mandatenkonzept

Ein zentrales Element jeder Art digitaler Ausstattung ist das Berechtigungskonzept. In vielen Konstellationen ist es weniger die Frage, ob eine Schule als Gesamtorganisation die Daten einer bestimmten Person für bestimmte Zwecke verarbeiten darf. Vielmehr ist die Frage, wer alles auf diese Daten zugreifen darf.

Das einfachste Beispiel ist die Personalakte, die der Dienstgeber zu seinen Mitarbeitenden nicht nur führen darf, sondern führen muss. Zugleich ist klar, dass nicht alle Mitarbeitenden – und im Sinne einer Übertreibung – alle Schülerinnen und Schüler sowie deren Eltern Zugang zu den Personalakten der Lehrkräfte erhalten.

Analoge Berechtigungen

In der analogen Datenverarbeitung ergibt sich ein Berechtigungskonzept darüber, welche Unterlagen in welchen Schränken oder Räumen verschlossen aufbewahrt werden und wer Zugang zu den jeweiligen Schlüsseln hat.

Administratoren

Eine spezielle Anwendergruppe sind die IT-Administratoren. So wie Hausmeister oft über Generalschlüssel und Zweitschlüssel zu fast allen Unterlagen technischen Zugang haben, ohne inhaltlich befugt zu sein, die Unterlagen zu lesen oder in anderer Form zu nutzen, so haben Administratoren regelmäßig einen sehr umfassenden Zugang zu allen Daten.

Sowohl bei Hausmeistern wie bei Administratoren ist die Kombination aus Zugangsberechtigung in Verbindung mit einem Zugriffsverbot rechtmäßig, da sie für den Betrieb der jeweiligen Infrastruktur unverzichtbar sind. Entscheidend sind hier die Verpflichtung dieser Personen auf ihre ganz besondere Form der Vertraulichkeit, die regelmäßig mit einer Schulung oder Unterweisung in den Pflichten zum Datenschutz und Geschäftsgeheimnisschutz einhergehen sollte.

Stark vereinfacht greift hier das prominente Zitat aus den „Spiderman"-Filmen: „Mit großer Macht kommt große Verantwortung."

Mandantentrennung

Bei IT-Diensten, die mehreren Organisationen in technisch gleicher Weise angeboten werden, bedarf es regelmäßig einer Mandantentrennung. Das ist die grundsätzliche Aufteilung der Datenbestände nach den einzelnen Organisationen, die den Dienst nutzen. Hierbei gibt es unterschiedlich strikte Trennungen.

- Separate Systeme: Komplett getrennte Infrastruktur, auf der jeweils identische Software läuft.

- Physische Trennung: Die Anwendung läuft für mehrere Organisationen auf der selben Plattform, ist aber über sogenannte virtuelle Server so nebeneinander eingerichtet, dass sie organisationsweise einzeln gestartet, gestoppt oder verändert (aktualisiert) werden kann.

- Logische Trennung: Die Bereiche der einzelnen Organisationen laufen gemeinsam in einer zentralen Anwendung, sind aber durch Rechtezuordnungen voneinander getrennt.

Das erforderliche Ausmaß der Trennung orientiert sich an der Schutzbedürftigkeit der Daten. In der Abgrenzung einzelner Schulen voneinander dürfte regelmäßig eine logische Trennung

ausreichend sein. Wenn Dienste bei Anbietern am Markt in Anspruch genommen werden, deren Service von einer Vielzahl unterschiedlicher Kunden genutzt wird, bedarf es einer Abwägung zwischen dem Schutzbedarf der darüber verarbeiteten Daten und der Schutzmaßnahmen des Anbieters gegen Verletzungen der von ihm etablierten Mandantentrennung.

Rechte und Rollen

Der Begriff Rechte- und Rollenkonzept wird oft synonym genutzt zum Ausdruck Berechtigungskonzept. Das Rechte- und Rollenkonzept umfasst aber regelmäßig nur ein technisches und ein organisatorisches Berechtigungskonzept; gelegentlich auch nur eins von beiden. Zu einem vollständigen Berechtigungskonzept zählt auch die Zuweisung der einzelnen Rollen an konkrete Personen.

Technisches Rechtekonzept

Ein technisches Rechtekonzept beschreibt Bündel von technischen Rechten innerhalb einer Anwendung. So geht der Befehl Löschen technisch mit einer Gruppe von Einzelschritten in der Datenbank hinter der Anwendung einher. In der konkreten Umsetzung gibt es abhängig von der Komplexität der jeweiligen Anwendung unterschiedlich komplexe Rechtekonzepte.

Für den Einsatz an den Schulen ist nur erforderlich, dass bei einer Prüfung des Berechtigungskonzepts deutlich wird, welche Pakete es gibt und welche Rechte diese umfassen. Der Fokus liegt darauf, im Rollenkonzept einzelnen Anwendendengruppen nicht unabsichtlich zu umfassende Rechte zuzuweisen.

Das technische Rechtekonzept wird im Normalfall vom Hersteller der Anwendung zur Verfügung gestellt.

Organisatorisches Rollenkonzept

Das organisatorische Rollenkonzept fasst die Rechtebündel aus dem Rechtekonzept zu größeren vorkonfektionierten Paketen zusammen, die für bestimmte Anwendendengruppen bereitgestellt werden. So erhält die Rolle Super-Admin deutlich weitreichendere Rechte als z.B. ein fachlicher Admin. Lehrkräfte erhalten umfangreichere Rechte als Schülerinnen und Schüler.

Diese Rollen sind abhängig vom Bedarf der Schule und den Funktionen der Anwendung zu standardisieren, um über die Standardisierung Zuverlässigkeit und Datensicherheit herzustellen.

Neben der Nutzungslogik gibt es bei den organisatorischen Rollen noch die Strukturlogik. Also welche Lehrkraft auf die Daten welcher Klasse zugreifen kann. Je nach Bedarf der Schule (und der Anwendung) kann hier differenziert werden zwischen in einer Klasse unterrichtenden und vertretenden Lehrkräften.

Das gesamte Rollenkonzept ist auf Grundlage der gleichen Logik wie die Prüfung der Rechtsgrundlage zu erstellen. Es geht immer um die Frage nach dem Zweck des Datenzugangs und dessen Erforderlichkeit. Wenn zum Beispiel eine vertretende Lehrkraft in gleicher Weise wie eine unterrichtende Lehrkraft auf die Daten einer Klasse zugreifen können soll, damit sie uneingeschränkt den Unterricht fortführen kann, ist es legitim und erforderlich keine Aufteilung in diese zwei Rollen vorzunehmen. Nach diesem Beispiel wäre der Verzicht auf eine zu kleinteilige Rollendifferenzierung vertretbar.

Das organisatorische Rollenkonzept sollte im Normalfall der Schulträger den Schulen zur Verfügung stellen.

Konkretes Berechtigungskonzept

Am Ende ist entscheidend, dass nur zuständige Personen auf personenbezogene Daten zugreifen. Dementsprechend ist ein Berechtigungskonzept erst vollständig, wenn die einzelnen Anwendenden – egal ob Administrator, Schulleitung, Sekretariat, Lehrkraft, Schülerin oder Schüler – einer oder mehreren Rollen zugewiesen wurden. Dies geschieht regelmäßig beim Anlegen der Nutzungskonten für die jeweilige Anwendung.

Es bedarf nicht zwingend einer eigenständigen Dokumentation, soweit die Administration der Nutzungskonten dokumentiert, welche Person wann von wem welche Rollen zugewiesen bekommen hat.

Die Zuweisung konkreter Rollen ist eine Aufgabe, die regelmäßig im Verantwortungsbereich der Schule liegt.

Entzug von Rechten

Das vermutlich größte Problem bei Zugriffsberechtigungen sind deren Aktualität. Genauso wie Rechte oder Rollen zugewiesen werden, sind diese bei Wegfall der Zuständigkeit auch wieder zu entziehen. Für einen Wegfall gibt es unterschiedliche Gründe wie das Verlassen der Schule oder der Wechsel in eine andere Klasse (sowohl für Lehrkräfte wie für Schülerinnen und Schüler). Es geht darum, sogenannte „Karteileichen“ zu vermeiden bzw. auf kurze Zeiträume wie zum Beispiel bis zum Schuljahreswechsel zu reduzieren.

Jede Schule ist verpfllichtet, zumindest zum Schuljahreswechsel alle Rollen- und Rechtezuweisungen für sämtliche Anwendenden in den von ihr genutzten Anwendungen zu überpürfen und für das kommende Schuljahr zu aktualisieren.

Protokollierungskonzept

Als Protokollierung wird bei IT-Anwendungen das automatisierte Erfassen von Aktivitäten bezeichnet. Die Protokollierung wird vom Datenschutz sowohl im Sinne der Datensicherheit (Merkmal Nachvollziehbarkeit) gefordert, wie vom Datenschutz kritisch betrachtet (Merkmal

Überwachung). Entscheidend ist auch hier der Blick auf Zweck und Erforderlichkeit und über das Merkmal der Erforderlichkeit eine vernünftige Beschränkung. Dementsprechend spielt im Protokollierungskonzept die Löschfrist eine zentrale Rolle. Siehe daher auch den nachfolgenden Abschnitt zum Thema Löschkonzept.

Metadaten

Bei den Protokollierungsdaten wird unterschieden zwischen den für alle Anwendenden sichtbaren Daten, oft als Metadaten bezeichnet, und den nur für entsprechend berechtigte Administatoren zugängliche Nutzungsprotokolle (auch Logfiles genannt). Zu den sichtbaren Metadaten zählt zum Beispiel in einer Dateiübersicht, wann welche oder welcher Anwendende die Datei gespeichert hat. Vergleichbar sind diese Einträge mit der Angabe in einem (herkömmlichen) Sitzungsprotokoll, wer das Protokoll geführt hat.

Soweit Klassenlisten automatisiert generiert werden – zum Beispiel über eine Schnittstelle zu einer zentralen Verzeichnisanwendung – kann auch die Aufzählung der Schülerinnen und Schüler als eine Art Metadatum bezeichnet werden.

Bei Metadaten, die letztlich einem Urhebervermerk entsprechen, ist der Löschbedarf deutlich geringer als bei einer Nutzungsprotokollierung, da Metadaten für einen wesentlichen Nachweis über Tätigkeiten und Zugehörigkeiten stehen und in deutlich geringerem Maß einer Überprüfung oder Überwachung dienen.

Nutzungsprotokollierung

Eine Nutzungsprotokollierung, wie sie in vielen Anwendungen in Form eines sogenannten Logfiles (Weblog oder Severlog) erfasst wird, ist essenziell, wenn es zu einem Missbrauch der IT-Anwendung gekommen ist oder z.B. ein (krimineller) Angriff auf die Anwendung erfolgt ist. Auch unabsichtliches Fehlverhalten kann darüber rekonstruiert werden. Die Protokolle sind nur besonders dazu berechtigten Administratoren zugänglich, die sie bei Bedarf weiteren Beteiligten, Forensikern oder Ermittlungsbehörden zur Verfügung stellen können.

Je nach Schutzbedarf der Anwendung werden die Daten durch entsprechende Sicherheitsanwendungen automatisiert ausgewertet, die Auffälligkeiten frühzeitig erkennen können und die IT-Verantwortlichen auf Risiken oder Missbrauch aktiv hinweisen können.

Ein Schutz sensibler Anwendungen ist ohne automatisierte Überwachung nicht möglich. Zugleich ist darauf zu achten, dass die Überwachung die Rechte und Freiheiten der Nutzenden nicht übermäßig einschränkt. Weder Lehrkräfte oder andere Mitarbeitende der Schule noch Schülerinnen und Schüler sollen einer anlasslosen personenbezogenen Überwachung und Verhaltensanalyse unterworfen werden.

Die Einführung einer Nutzungsprotokollierung und insbesondere von automatisierten Auswertungen sind aus dem Personalrecht heraus regelmäßig mitbestimmungspflichtig. Hierbei geht es aber regelmäßig weniger um das Ob der Einführung als um das Wie mit Blick auf Zugänge zu den Daten und deren Speicherzeit.

Für die Logfiles zu Internetseiten (Weblogs genannt) hat sich eine Speicherzeit von sieben Tagen als angemessen etabliert. Vor der starken Zunahme von sogenannten Cyberangriffen in den letzten Jahren ist hier aber eine fortschreitende Veränderung hin zu längeren Speicherzeiten zu erkennen. Für Anwendungen, die keine einfache Internetseite sind, gilt eine Speicherung von 30 Tagen inzwischen als Mindestwert, 90 Tage als gängig und auch eine Jahresfrist wird bei sensiblen und angriffsgefährdeten Anwendungen selten von Datenschutzaufsichtsbehörden kritisiert.

Zuständigkeit

Es ist Aufgabe der Schulträger, den Schulen zu den Anwendungen Protokollierungskonzepte zur Verfügung zu stellen. Zentrales Element der Konzepte ist die Abwägung zwischen Erforderlichkeit der Protokollierung und Auswertung einerseits und den Gefahren übermäßiger Überwachung andererseits. Mit Blick auf sich verändernde Gefährdungslagen sind solche Konzepte regelmäßig zu überprüfen und bei Bedarf zu aktualisieren.

Löschkonzept

Grundlogik

Spiegelbildlich zur Rechtmäßigkeit der Datenverarbeitung steht die Pflicht zur Datenlöschung, wenn die Rechtmäßigkeit z.B. durch Fristablauf entfallen ist. Viele Datenverarbeitungen sind erst einmal rechtmäßig, weil aktuelle Zwecke damit verfolgt werden. Sobald aber der letzte angestrebte Zweck erreicht wurde, entfällt das Recht zum weiteren Speichern und dreht sich in eine Verpflichtung zum Löschen um.

Dementsprechend baut auch das Thema Löschen auf den beiden Grundparametern Zweck der Datenverarbeitung und Erforderlichkeit zur Zweckerreichung auf.

Für Löschkonzepte ist dementsprechend eine Zusammenstellung aller für ein personenbezogenes Datum einschlägigen Speicherzwecke entscheidend.

Löschfristen (Aufbewahrungsfristen)

Ein häufiger Zweck, dem das Speichern von Daten dient, ist das Einhalten von Aufbewahrungsfristen. Dezidierte Löschfristen gibt es nur in seltenen Fällen. Auch gesetzlich oder durch Rechtsverordnung festgelegte Aufbewahrungsfristen gibt es nur wenige. Mehr und mehr Bundesländer erlassen aber für ihr Schulwesen Rechtsverordnungen, die Aufbewahrungs- oder Löschfristen festlegen. Die Kultusministerien informieren zur Rechtslage im jeweiligen Land.

Die Schulträger sollten den Schulen Übersichten mit den einschlägigen Aufbewahrungs- und Löschfristen zur Verfügung stellen. Soweit die Schulträger den Schulen Anwendungen zur Verfügung stellen, in die Löschautomatismen integriert sind, sollten diese die einschlägigen Fristen bereits als Voreinstellung abbilden.

Das Ende der Aufbewahrungsfrist stellt fast immer den Wegfall des letzten verbliebenen Speicherzwecks dar – und begründet damit den Beginn der Löschpflicht. Das muss nicht zwingend so sein, kann aber als Grundregel betrachtet werden. Ausnahmen sind zum Beispiel sich über einen langen Zeitraum erstreckende Rechtsstreitigkeiten. Auch wenn die normale Aufbewahrungsfrist zwischenzeitlich abläuft, sind die Daten mindestens bis zum Abschluss des Rechtsstreits aufzubewahren.

Löschmechanismen

Die konkrete Löschmethode ist abhängig von den technischen Möglichkeiten der jeweiligen Anwendung und den organisatorischen Möglichkeiten der Schulen, Löschaufgaben zuverlässig umzusetzen. Erstrebenswert sind automatisierte Datenlöschungen zu bestimmten Stichtagen oder nach vorab definierten Zeitabläufen.

Automatisierte Löschung reduziert den Personalaufwand deutlich, geht aber auch mit dem Risiko ungewollten vorzeitigen Löschens einher. Als Schutz gegen ungewolltes vorzeitiges Löschen bieten sich Erinnerungszeitfenster in den Automatismen an, die z.B. einen Monat vor dem Löschzeitpunkt den zuständigen Administratoren die Möglichkeit geben, Daten aus dem Löschdurchgang auszuschließen.

Nicht-automatisierte Löschungen, die von Anwendenden manuell gestartet werden müssen, sind als feste Routine im Schulalltag zu etablieren. Regelmäßig bieten sich hierzu Termine zum Schuljahreswechsel an, da viele Speicherzwecke mit dem Schuljahreswechsel entfallen.

Kaum realistisch umsetzbar sind Löschprozesse für große und unstrukturierte Datenmengen, konkret für E-Mail-Postfächer. Die inhaltliche Ausrichtung der einzelnen E-Mails im Posteingang wie Postausgang ist so divers, dass die Anwendung differenzierter Löschzeiten kaum mit vertretbarem Aufwand möglich ist. Denkbar ist aber, dass in Zukunft KI-Funktionen des E-Mail-Servers die einzelnen Mails vorsortieren und passenden Löschzeiten zuordnen.

Soweit für eine Schule eine maximale Speicherzeit der E-Mail-Korrespondenz definiert wurde, sind gesendete und empfangene E-Mails bei Erreichen dieser Maximalzeit zu löschen.

Mittelfristig sollte auf alternative Kommunikationswege zu E-Mail und den verbreiteten Messengern umgestellt werden wie zum Beispiel Schul-Apps, über die Informationen nicht nur zwischen den Lehrkräften oder den Lehrkräften und den Schülerinnen und Schülern sondern auch zwischen Lehrkräften und Sorgeberechtigten ausgetauscht werden.

Eigenständige, strukturierte Anwendungen erleichtern den Einsatz automatisierter Löschprozesse deutlich (Zugleich verringern sie die Gefahr versehentlicher Fehlversendungen).

Wichtig ist es, klare Zuständigkeiten für das Löschen zu definieren, insbesondere wo manuelles Löschen in Datenbeständen erforderlich ist, zu denen nur die jeweilige Lehrkraft Zugang hat. Nach Erledigung des Löschens sollte im Sinne der datenschutzrechtlichen Rechenschaftspflicht ein Löschprotokoll erstellt werden und bei der zentralen Datenschutzdokumentation gespeichert werden.

Schulträger sollten soweit möglich die technischen Bedingungen für automatisiertes Löschen zur Verfügung stellen. Für manuelles Löschen sollten sie den Schulen Standardprozesse als Vorlage zur Verfügung stellen. Die Schulen sind aber letztlich dafür verantwortlich, dass die Daten ihrer Organisation tatsächlich gelöscht werden und Vollzug der Löschung dokumentiert wird.

Anonymisieren

Das Thema Anonymisieren personenbezogener Daten spielt in unterschiedlichen Zusammenhängen eine Rolle. Der Begriff wird an dieser Stelle vorgestellt, weil Anonymisieren ein Ersatz (ein Substitut) für das Löschen ist. Sind zuvor personenbezogene Daten anonymisiert, entspricht das aus einer rein datenschutzrechtlichen Perspektive dem Löschen der Daten.

Zur Frage, wann genau Daten anonymisiert sind, gibt es keine ganz klare Linie. Grundsätzlich sind Daten anonymisiert, sobald eine zuvor bestehende Beziehbarkeit der Daten auf eine konkrete Person nicht wiederherstellbar ist.

Von Datenschutzaufsichtsbehörden wurde zeitweilig vertreten, dass Anonymisierung erst vorliegt, wenn niemand – egal ob innerhalb oder außerhalb der Organisation des Verantwortlichen – den Bezug wiederherstellen kann. Da diese Perspektive Ermittlungsfähigkeiten von Polizeibehörden und den Einsatz von Hochleistungsrechnern umfassen würde, wäre das Ergebnis vollständiger Anonymisierung nach vielfach vertretener Ansicht kaum erreichbar.

Die Rechtsprechung zumindest des Europäischen Gerichts Erster Instanz („EuG“) hat eine niedrigere Schwelle angesetzt und stellt nur auf die Wiederherstellbarkeit aus den Mitteln und (rechtlichen) Möglichkeiten der jeweiligen Organisation abgestellt. Im konkreten Fall hatte eine EU-Behörde Daten an ein Forschungsinstitut übergeben, in denen der Bezug zu den Personen auf eine Personalnummer beschränkt worden war. Da das Forschungsinstitut aus eigenen Möglichkeiten heraus keinen Zugang zur Zuordnung der Nummern zu konkreten Personen hat, wurden die Daten aus Sicht des Forschungsinstituts als anonym eingestuft. Auch wenn die Daten für die EU-Behörde weiterhin personenbezogen sind.

Ein anderes Beispiel für anonyme Daten sind Statistiken: Die reine Statistik als Ergebnis der statistischen Erhebung ist regelmäßig anonym; die der Statistik zugrundeliegenden Erhe-

bungsdaten sind hingegen regelmäßig personenbezogen. Daher ist das Weitergeben von Statistiken (z.B. des Notenspiegels einer Klasse) regelmäßig kein Datenschutzthema, die Bereitstellung aller Einzelbenotungen wäre es hingegen schon.

Sowohl Schulträger wie Schulen können für einzelne Datenhaltungen prüfen, in welcher Weise Anonymisieren möglich ist und ob das Anonymisieren statt des Löschens die passendere Vorgehensweise ist.

Zweckbindung

Die Rechtmäßigkeit jeder Datenverarbeitung geht einher mit einer strengen Zweckbindung. Hinter diesem Grundsatz steht, dass Daten, die für einen Zweck (z.B. Förderbeitrag zur Teilnahme an der Klassenreise) erhoben wurden, nicht für einen anderen Zweck genutzt werden (z.B. Erstellung einer Sozialstatistik der Klasse im Politikunterricht).

Im Rahmen von IT-Projekten ist dieser Grundsatz vor allem beim Einsatz von Schnittstellen zu beachten. Auch wenn bestimmte personenbezogene Daten bereits in einer Datenbank der Schule vorhanden sind, dürfen sie nicht zwingend über eine Schnittstelle in weitere Datenbanken, deren Betrieb gänzlich anderen Zwecken dient, überführt werden.

Diese Einschränkung der Datennutzung ist im Schulalltag selten von Relevanz, da die Mehrheit der Datenverarbeitungen durch vergleichsweise allgemeine Zwecke des Schulbetriebs gerechtfertigt sind. Diese allgemeinen Zwecke sind regelmäßig so breit angelegt, dass unterschiedliche Konkretisierungen in der Datennutzung noch vom übergeordneten Zweck abgedeckt sind.

Dennoch sollte sich jeder Datenschutzverantwortliche bei der Änderung von Prozessen und insbesondere der Überführung von Daten in neue Nutzungszusammenhänge kritisch fragen, ob diese Veränderung gegen den Grundsatz der Zweckbindung verstoßen könnte.

Datensicherheit

Grundlogik

Die zentrale Norm für Datensicherheit ist Art. 32 DSGVO.

GRUNDBEGRIFF DER DATENSICHERHEIT NACH ART. 32 ABS. 1 1. HALBSATZ DSGVO: Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; (...)

Entscheidend ist nach dieser Grundlogik einerseits die Beurteilung des Risikos und andererseits die Auswahl der Schutzmaßnahmen sowie die Beurteilung ihrer Angemessenheit. Diese Definition zeigt, dass Datensicherheit eine Anforderung fern präziser Kategorien ist, sondern auf zwei eng miteinander verbundenen Risikobeurteilungen aufbaut: Wie groß ist das Risiko und genügen die Schutzmaßnahmen zur Reduktion der Risiken auf ein vertretbares Minimum?

Wie im einleitenden Teil bereits dargestellt, kommt es bei der Risikobeurteilung nicht auf die Perspektive der Schule bzw. des datenschutzrechtlich Verantwortlichen an. Entscheidend ist die Perspektive der von der Verarbeitung personenbezogener Daten betroffenen Personen, also der Lehrkräfte und sonstigen Mitarbeitenden der Schule wie der Schülerinnen und Schüler und ihrer Eltern.

Im Rahmen der Datensicherheit wird unterschieden zwischen technischen und organisatorischen Schutzmaßnahmen. Schematisiert betrachtet liegt die Verantwortung für technische Maßnahmen bei den IT-Verantwortlichen und die die Verantwortung für die organisatorischen Maßnahmen bei den Personalveranwortlichen. Eine dritte gesonderte Säule ist die Verantwortung für bauliche Gegebenheiten, wo es auf die Zutrittssicherung von Räumen beziehungsweise den Zugang zu verschließbaren Schränken ankommt.

Davon ausgehend, dass für die Bereitstellung der IT-Dienste der Schulträger verantwortlich ist, liegt bei diesem auch die Verantwortung für die technischen Schutzmaßnahmen. Bei der Schule selbst liegt die Verantwortung für die Umsetzung organisatorischer Maßnahmen, für die der Schulträger der Schule zur Unterstützung Empfehlungen bereitstellen kann.

ASPEKTE DER DATENSICHERHEIT NACH ART. 32 ABS. 1 2. HALBSATZ DSGVO: (...) diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

- Die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- Die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die in Art. 32 Abs. 1 2. Halbsatz DSGVO aufgezählten Maßnahmen nennt das Gesetz beispielhaft. Keine einzelne Maßnahme ist verpflichtent. Entscheidend ist allein die Risikobeurteilung nach dem 1. Halbsatz der Norm.

Vertraulichkeit

Zur Vertraulichkeit zählen alle Maßnahmen, die Daten gegen unberechtigte Offenbarung schützen sollen.

Zu den organisatorischen Maßnahmen zählen die Verpflichtung der Mitarbeitenden auf die Vertraulichkeit, wie sie bei staatlichen Beschäftigten regelmäßig bereits durch Aufnahme in das Dienstverhältnis erfolgt. Eine wirksame Verpflichtung setzt aber auch Schulungen in Datensicherheit voraus, damit Mitarbeitende nicht auf Ausforschungsangriffe wie z.B. das sogenannte Phising (Fischen nach Passworten) oder Social Engineering (Ausfragen am Telefon oder per Chat/ E-Mail) hereinfallen.

Zu den technischen Maßnahmen zählt in erster Linie das Berechtigungskonzept. Ein wirksames Berechtgungskonzept ist die zentrale Grundlage dafür, dass nur aktuell berechtigte Personen Zugang zu personenbezogenen Daten haben.

Fast ebenso wichtig sind Maßnahmen zum Schutz der digitalen Zugänge. Klassisch ist das der Passwortschutz, bei dem hochwertige Passwortstandards erzwungen werden sollten (Im Mittelpunkt steht hier die Mindestlänge des Passworts und das Verbot des identischen Passworts für mehrere Zugänge). Deutlich gesteigert wird der Zugangsschutz aber durch Ergänzungen wie Zwei-Faktor-Authentifizierung oder die neuere Passkey-Technologie.

Bei mobilen Endgeräten insbesondere, aber eigentlich bei allen Endgeräten ist Festplattenverschlüsselung wesentlich. Die Festplattenverschlüsselung verhindert bei einem Verlust des Geräts (z.B. im Bus liegen gelassen), dass Finder Zugang zu den darauf gespeicherten Daten erhalten.

Integrität

Die Anforderung der Integrität schützt Daten vor unberechtigter Veränderung.

Integrität wird zum einen ebenfalls durch den Zugangsschutz (in Verbindung mit dem Berechtigungskonzept, speziell dem Recht Daten zu bearbeiten) geschützt, da eine beschränkte Zahl an Zugriffsberechtigten auch die Zahl der Datenbearbeitenden beschränkt.

Zum anderen gilt die Nutzungsprotokollierung als wichtig für den Integritätsschutz. Die Protokollierung kann Datenveränderungen zwar nicht verhindern, ermöglicht aber Nachforschungen, wie es zu den unberechtigen Veränderungen gekommen ist. Auf Grundlage der Nachforschungsergebnisse können Sanktionen ergriffen werden.

Verfügbarkeit

Die Verfügbarkeit betrifft die technische Erreichbarkeit von Datenbanken und Anwendungen. Soweit Daten außerhalb der Schule gespeichert sind, ist eine redundante Netzanbindung von Bedeutung, wenn z.B. durch Bauarbeiten eine Leitung ausfällt.

Belastbarkeit

Die Belastbarkeit ist ein Unterpunkt der Verfügbarkeit und betrifft die Leistungsfähigkeit der Server und der Netzinfrastruktur. Die technischen Gegebenheiten müssen so bestellt sein, dass eine gleichzeitige Nutzung durch die Zahl der zu erwartenden Nutzenden in einer vertretbaren Geschwindigkeit möglich ist.

Wiederherstellbarkeit

Die Wiederherstellbarkeit ist ein weiterer Unterpunkt der Verfügbarkeit und betrifft Datensicherungen (Backups).

Aus unterschiedlichen Gründen ist fast sicher davon auszugehen, dass die primär eingesetzten Speichermedien (Server) einmal technisch ausfallen werden. Es kann insoweit dahingestellt bleiben, ob der Ausfall durch inneren technischen Zusammenbruch der Speicher (Überalterung der Festplatten), Verlust der Speicher (z.B durch Feuer oder Wassereinbruch im Rechenzentrum), einen Cyberangriff (z.B. in Form von sogenannter Ransomware) oder menschliches Versagen (Administratorenfehler) zustande kommt.

Für jeden Datenbestand bedarf es daher eines Backup-Konzepts und – deutlich wichtiger – einer Umsetzung des Konzepts in gelebten Backup-Prozessen. Die Erfahrung lehrt, dass viele Einrichtungen denken, sie hätten eine Datensicherung. Wenn es aber auf die Sicherung ankommt, werden Defizite offensichtlich, die letztlich in einer Unbrauchbarkeit des Backups münden. Essenzieller Teil aller Backup-Prozesse sind regelmäßige Wiederherstellungstests, bei denen die Nutzbarkeit der Backups aktiv überprüft wird.

Mit Blick auf physische Risiken für Rechenzentren (Serverräume) sollten Backups an mindestens einem anderen Ort als dem Standort des Primärspeichers aufbewahrt werden. Da Schadsoftware regelmäßig schon länger in einem Datenbestand sitzt, bevor ihre Existenz oder schädliche Wirkung erkannt wird, sollte es Backups über verschiedene Zeitintervalle geben. Welche Intervalle für die jeweilige Datenbank sinnvoll sind, ist abhängig vom Umfang und Inhalt der Datenbank.

Wichtig bei der Planung der Backups ist, in welchem Umfang Daten auf einzelnen Endgeräten gespeichert werden. Optimalerweise erfolgt keinerlei Speicherung allein auf einem Endgerät, sondern nur in Ordnern, die mit einem Onlinespeicher (Cloudspeicher) fortlaufend synchronisiert werden. Ist Onlinespeicherung aktiviert, gehen beim Verlust eines Endgeräts maximal die Daten verloren, die seit der letzten aktiven Internetverbindung neu auf dem Gerät gespeichert wurden.

Verschlüsselung

Verschlüsselung gibt es in zwei Bereichen: bei der Datenspeicherung und bei der Datenübertragung.

Die Verschlüsselung von Datenspeichern wurde beim Schutz der Vertraulichkeit bereits angesprochen. Ist ein Speichermedium verschlüsselt, können nur Anwendende darauf zugreifen, die das Passwort der Verschlüsselung kennen beziehungsweise in deren entsprechenden Einstellungen eine passende Authentifizierung hinterlegt ist.

Für größere Server ist eine Verschlüsselung eher unüblich, da man mit zu großen Leistungseinschränkungen rechnet. Daher steht bei Servern regelmäßig der Gebäudeschutz im Vordergrund, um auf diese Weise die Gefahr eines Zugangs zum Speichermedium zu reduzieren. Alle Endgeräte und auch kleinere Server, wie man sie als NAS (Network Attached Storage) kennt, sind aber heutzutage so leistungsfähig, dass eine Festplattenverschlüsselung für sie kein Problem darstellt und entsprechend auf aufwendige Gebäudesicherungen verzichtet werden kann.

Bei der Verschlüsselung von Datenübertragungen sind zwei Bereiche zu unterscheiden: E-Mail-Übertragungen und alle anderen. Für den Datenaustausch zwischen Nicht-E-Mail-Servern gibt es etablierte Verschlüsselungsmechanismen, die man z.B. beim Aufruf einer Internetseite an dem S am Ende von HTTPS erkennt. Die gleiche Verschlüsselungstechnik kommt auch in Apps für Mobilgeräten und in Desktop-Anwendungen zum Einsatz, die Daten von einem Server abrufen. Die Verschlüsselung beruht auf kryptografischen Prozessen und dahinter liegenden Zertifikaten. Hier ist regelmäßig allein auf die Aktualität der Zertifikate zu achten, die meist jedoch von den Anwendungen automatisiert selbstverwaltet wird.

Man spricht insoweit von einer Ende-zu-Ende-Verschlüsselung, weil die Daten an den verschiedenen Knotenpunkten des Internets nicht ausgelesen werden können bzw. sich nur als eine Form von unverständlichem „Datensalat“ darstellen. Nur der Server am einen Ende und das Endgerät des Nutzenden können die übertragenen Daten entschlüsseln.

Beim Versand von E-Mails kommt eine Technologie zum Einsatz, für die Verschlüsselung über zwei verschiedene Technologieformen auch möglich ist. Diese werden S/MIME und PGP genannt. Beide sind aber mit Defiziten behaftet und setzen vor allem voraus, dass sendende wie empfangende Person beide ein Zertifikat der selben Technologie besitzen und aktiviert haben. Da die Verbreitung dieser Zertifikate derzeit außerordentlich gering ist, ist Ende-zu-Ende-Verschlüsslung in der E-Mail-Kommunikation eher ein Nischenthema.

E-Mails werden in den meisten Fällen transportverschlüsselt verschickt. Diese Form der Verschlüsselung schützt aber nur vor unberechtigten Zugriffen zwischen den Knotenpunkten des Internets. An den offiziellen Übergabepunktenund insbesondere auf den Servern der E-Mail-Hostinganbieter sind die Nachrichten lesbar. Das wirft insbesondere in der Kommu-

nikation mit Eltern Probleme auf, die ihre E-Mail-Postfächer sehr häufig bei kostenlosen Anbietern haben und diesen im Gegenzug für die kostenlose Bereitstellung die Analyse des eigenen Postfachs und Auswertung für Werbeprofile gestattet haben.

Pseudonymisierung

Pseudonymisierung bedeutet, dass ein unmittelbar personenbezogenes Datum wie z.B. der Name durch einen Platzhalter wie z.B. eine Personalnummer ersetzt wurde. Beim Verantwortlichen existiert dann eine Zuordnung zwischen Platzhalter und Person, so dass der Personenbezug weiterhin besteht, nur die Bezugskette um ein Element verlängert wurde.

Der Vorteil der Pseudonymisierung ist, dass im Fall einer unberechtigten Offenlegung der Daten, die allein auf das Pseudonym bezogen sind, nur anonyme – und damit nicht personenbezogene Daten – vorliegen, wenn die unberechtigte Person keinen Zugang zu den Referenzdaten hat, die die Zuordnung zwischen Pseudonym und Person ermöglichen.

Daher ist Pseudonymisierung eine starke Schutzmaßnahme in allen Zusammenhängen, wo die Referenzdaten deutlich getrennt von der primären Nutzung bzw. Datenbank gespeichert sind.

Ein typisches Pseudonym sind die Identifikationsnummern, die in sogenannten Cookies im Speicher der Internetbrowser gespeichert werden. Über diese sogenannten Cookie-IDs kann ein Browser wiederkehrenden Besuchen auf einer Internetseite zugeordnet werden. Davon ausgehend, dass ein Endgerät und damit der darauf installierte Internetbrowser regelmäßig nur von einer Person genutzt wird, ergibt sich eine Kette, die im Ergebnis einen Personenbezug herstellt.

Regelmäßige Überprüfbarkeit

Wenn Schutzmaßnahmen nicht regelmäßig überprüft und auf ihre Wirksamkeit hin getestet werden, steht die Gefahr im Raum, dass sie nur eine theoretische Schutzwirkung entfalten und es tatsächlich an einem risikoadäquaten Schutz fehlt. Daher handelt es sich bei der regelmäßigen Überprüfung der Schutzmaßnahmen sowohl hinsichtlich der Erforderlichkeit wie der Effektivität um eine wesentliche Datenschutzpflicht. Die Überprüfungen sind z.B. in Form von Auditberichten zu dokumentieren.

Vertraulichkeitsverpflichtung

Die Verpflichtung der Mitarbeitenden der Schulen auf die Vertraulichkeit ist von zentraler Bedeutung. Wie bereits im Abschnitt Vertraulichkeit innerhalb des Bereichs Datensicherheit beschrieben, ergibt sich die Verpflichtung auf die Vertraulichkeit bei Beschäftigten der Verwaltung regelmäßig bereits aus dem Dienstrecht. Wirksam wird die Verpflichtung aber nur durch entsprechende Schulungsangebote, über die Beschäftigte auf ihre Pflichten aus dem Bereich der Datensicherheit und die vom Dienstgeber zur Verfügung gestellten technischen Möglichkeiten hingewiesen werden. Die Verpflichtung der Beschäftigten auf die Vertraulichkeit ist eine Pflicht der Schulen.

Dienstleisterbindung (Auftragsverarbeitung)

Die meisten digitalen Dienste werden nicht vom Verantwortlichen selbst betrieben. Üblich ist die Nutzung von Anwendungen, die als sogenannte Cloud-Anwendungen oder Software-as-a-Service („SaaS“) von Externen zur Verfügung gestellt werden. Insoweit ist es unerheblich, ob der Externe eine andere Behörde ist wie z.B. der Schulträger, die Kommune, der Landkreis oder das Kultusministerium, oder ob der Dienst eines privatwirtschaftlichen Anbieters genutzt wird.

Das Datenschutzrecht nennt alle Formen externer Datenverarbeitung, bei der es dem Externen auf die konkreten Inhalte der Datenverarbeitung nicht ankommt und er mit Blick auf die konkreten Daten keine eigenen Zwecke verfolgt, eine Auftragsverarbeitung. Diese ist in Art. 28 DSGVO normiert.

Die zentrale Rechtslogik hinter dem Art. 28 DSGVO ist, dass ein Auftragsverarbeiter für die Verarbeitung personenbezogener Daten über die von ihm betriebene Infrastruktur keine eigene Rechtsgrundlage nachweisen muss und auch ansonsten fast vollständig von den Pflichten der Verantwortlichen aus der DSGVO befreit ist. Der Auftragsverarbeiter ist nur den Pflichten aus Art. 28 DSGVO zur Weisungsgebundenheit und Vertraulichkeit und den Pflichten aus Art. 32 DSGVO zur Datensicherheit unterworfen.

Ob Auftragsverarbeitung vorliegt oder nicht, ergibt sich aus der Art der Leistungsbeziehung. Wenn der Auftragsverarbeiter an den Daten keine eigenen Rechte hat und durch die Verarbeitung der Daten keine eigenen Zwecke verfolgt, liegt eine Weisungsgebundenheit im Sinne des Art. 28 DSGVO vor und damit Auftragsverarbeitung. Dennoch verlangt Art. 28 Abs. 3 DSGVO eine Vereinbarung in Textform zwischen Verantwortlichem und Auftragsverarbeiter.

Diese Auftragsverarbeitungsvereinbarungen (oft AV-Vertrag oder AVV genannt) bestehen regelmäßig aus einem allgemeinen Vertragsteil, der die in Art. 28. DSGVO vorgegebenen Pflichten wiedergibt, und meist drei Anlagen. Die erste Anlage beschreibt die konkrete Art der Datenverarbeitung, die zweite nennt die Unterauftragnehmer, die zum Einsatz kommen, und die dritte Anlage legt die technischen und organisatorischen Maßnahmen („TOMs“) fest, auf die der Auftragsverarbeiter sich und seine Unterauftragnehmer mit Blick auf die konkrete Datenverarbeitung verpflichtet.

In einem Beschluss vom 22.02.2023 hat das OVG Münster (Aktenzeichen 19 B 417/22) zu erkennen gegeben, dass es die Pflicht zum Prüfen der AV-Verträge beim Schulträger sieht. Dies ergebe sich daraus, dass der Schulträger die Verantwortung für die Bereitstellung der digitalen Infrastruktur trägt und damit auch für die Prüfung der externen Anbieter.

Neben den Anbietern von Onlinediensten sind externe IT-Administratoren regelmäßig als Auftragsverarbeiter einzustufen; zumindest wenn zu ihren Aufgaben auch das Anlegen oder Verwalten von Nutzendenkonten oder das Auswerten von Nutzungsprotokollen zählt.

Nicht als Auftragsverarbeitung gilt es, wenn Dienstleister zwar im Rahmen ihrer Tätigkeit Zugang zu personenbezogenen Daten erhalten, ihre Arbeit aber nicht auf die Verarbeitung dieser Daten ausgerichtet ist. Typisches Beispiel hierfür sind Reinigungskräfte, die Papierkörbe leeren sollen. Soweit sich in den Papierkörben Dokumente mit personenbezogenen Daten befinden, haben die Reinigungskräfte zum einen Zugang zu diesen Daten und zum anderen sind sie mit der Entsorgung (Vernichtung) dieser Daten beauftragt. In solchen Konstellationen ist der Auftrag aber die Entsorgung des Papiers, egal ob es sich um Blätter mit personenbezogenen Daten handelt oder nicht. Denkbar ist eine allgemeine Vertraulichkeitsverpflichtung solcher Dienstleister.

Auch keine Auftragsverarbeiter sind Dienstleister, die unter eine eigene Regulierung fallen. Neben Branchen wie Banken und Versicherungen sind das vor allem Telekomunikationsanbieter. Die sind durch das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz („TDDDG“, früher Fernmeldegeheimnis) strafbewehrt auf strenge Vertraulichkeitsstandards verpflichtet. Ergänzender Vertraulichkeitsverpflichtungen bedarf es nicht.

Ebenso fallen Berufsgruppen, die eigenverantwortlich handeln mit eigenem Entscheidungsspielraum und regelmäßig eigenen Dokumentationspflichten, nicht unter die Auftragsverarbeiter. Das bezieht sich konkret auf Berufsgeheimnistragende wie Rechtsanwältinnen und Rechtsanwälte, Ärztinnen und Ärzte, Psychologinnen und Psychologen, Sozialarbeiterinnen und Sozialarbeiter und weitere in § 203 Strafgesetzbuch genannte Berufsgruppen.

Jede Art von Beratung wie zum Beispiel IT-Beratung oder Design-Beratung stellt auch keine Auftragsverarbeitung dar, da Beraterinnen und Berater genauso wie Kreative nicht weisungsgebunden handeln. In den meisten Fällen ist es aber auch nicht notwendig, diesen Dienstleistern über die Kontaktdaten ihrer Ansprechpersonen hinaus personenbezogene Daten zur Verfügung zu stellen. Sollte das doch notwendig sein, sollten sie vor Bereitstellung der Daten auf die Vertraulichkeit und die Löschung der Daten bei Beratungsende verpflichtet werden.

Kooperationen (Gemeinsame Verantwortung)

Neben der weit verbreiteten weisungsgebundenen Auftragsverarbeitung nach Art. 28 DSGVO kennt das Datenschutzrecht auch die gemeinsame Verarbeitung von personenbezogenen Daten nach Art. 26 DSGVO. Diese Art der Kooperation wird gemeinsame Verantwortung genannt. Dabei ist es im Außenverhältnis den Betroffenen gegenüber unerheblich, wie groß die jeweiligen Anteile der Verantwortung sind. Den Betroffenen gegenüber haften die gemeinsam Verantwortlichen erst einmal gesamtschuldnerisch.

Ähnlich der Auftragsverarbeitung verlangt auch Art. 26 DSGVO zur Regelung der gemeinsamen Verantwortung eine Vereinbarung der Parteien in Textform. Diese Vereinbarung muss insbesondere deutlich machen, wie die jeweiligen Verantwortungsbereiche der beteiligten Parteien aussehen und wie die Haftungsübernahme für datenschutzrechtlich begründete Ansprüche zwischen den Parteien verteilt ist.

Ergänzend besteht die Pflicht aller Parteien in ihren jeweiligen Datenschutzinformationen auf das Vorliegen einer gemeinsamen Verantwortung hinzuweisen und über die Grundstrukturen der Verantwortungsaufteilung zu informieren.

Die genaue Abgrenzung, wann eigenständige, parallele Verantwortlichkeiten, wann Auftragsverarbeitung oder wann eine gemeinsame Verantwortung vorliegt, ist nicht immer ganz eindeutig.

Stellt der Schulträger der Schule eine Onlineanwendung zur Verfügung oder wird diese Anwendung vom Kultusministerium des Landes oder einer anderen Behörde zur Verfügung gestellt, stellt sich die Frage, ob hier Auftragsverarbeitung oder eine gemeinsame Verantwortung vorliegt. Soweit der Schulträges oder die andere Behörden sich auf die technische Bereitstellung des Dienstes beschränkt, sind diese als Auftragsverarbeiter einzuordnen. Soweit der Anbieter des Dienstes die darüber verarbeiteten Daten auch für eigene Zwecke nutzt, entsteht eine gemeinsame Verantwortung.

Die Schwierigkeiten der Abgrenzung besteht insbesondere bei Anbietern digitaler Dienste, die die Nutzung ihrer Anwendungen zum Training eigener KI-Funktionen nutzen wollen. In dem Bereich fehlt es aktuell an abschließenden rechtlichen Klärungen, so dass vorerst keine Anwendungen genutzt werden sollten, deren Nutzung zugleich dem Training eines KI-Modells dient. Die Nutzung fertiger KI-Modelle auf Basis eines abgeschlossenen Trainings ist grundsätzlich denkbar.

Drittstaatentransfers

Die DSGVO enthält in den Art. 44 bis 49 spezielle Regelungen für Datenübertragungen nach außerhalb des Europäischen Wirtschaftsraums (Drittstaatentransfers genannt). Hintergrund dieser Normen ist, dass der Schutzstandard der DSGVO durch eine Verlagerung der Datenverarbeitung in Länder, in denen die DSGVO keine Anwendung findet, nicht unterlaufen werden soll.

Drittstaatentransfers sollten im Schulalltag eher selten erforderlich sein, da die Schulträger in der Lage sein sollten, für alle im Schulbetrieb erforderlichen Formen der Datenverarbeitung Prozesse und Anwendungen zur Verfügung zu stellen, die ohne einen Drittstaatentransfer auskommen.

Wo ein Drittstaatentransfer erforderlich ist, zum Beispiel weil ein vergleichbarer Dienst über einen europäischen Anbieter nicht in gleichwertiger bzw. ausreichender Zuverlässigkeit oder von entsprechenden Funktionsumfang verfügbar ist, ist zu differenzieren zwischen Ländern, für die ein Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO vorliegt oder nicht.

LÄNDER MIT ANGEMESSENHEITSBESCHLUSS NACH ART. 45 DSGVO (STAND DEZEMBER 2024):

- Andorra
- Argentinien
- Farör Inseln
- Guernsey
- Isle of Man
- Israel
- Japan
- Jersey
- Kanada (beschränkt auf privat-wirtschaftliche Unternehmen)
- Neuseeland
- Schweiz
- Südkorea
- Vereinigte Staaten von Amerika (beschränkt auf privat-wirtschafltiche Unternehmen, die sich nach dem Data-Privacy-Framework zertifiziert haben)
- Vereinigtes Königreich Großbritannien und Nordirland
- Uruguay

Bei den USA, die wegen der Vielzahl dort sitzender Dienstleister eine deutlich größere Rolle spielen als alle anderen Länder mit Angemessenheitsbeschluss, ist auf die Einschränkung zu achten, dass die Dienstleister sich nach dem Data-Privacy-Framework zertifiziert haben müssen.

Bei dieser Prüfung ist wiederum darauf zu achten, dass bei den Zertifizierung zwischen Beschäftigtendaten und Nicht-Beschäftigtendaten unterschieden wird. Da der Einsatz von Anwendungen im Schulbetrieb nicht ohne Nutzendenkonten für Lehrkräfte oder andere Mitarbeitende der Schule erfolgen wird, kommen nur Anbieter in Frage, die sich auch für die Verarbeitung von Beschäftigtendaten zertifiziert haben.

Standardvertragsklauseln

Liegt für das Empfängerland kein Angemessenheitsbeschluss nach Art. 45 DSGVO vor, bedarf es des Abschluss eines Vertrags nach dem vorgefertigten Wortlaut der Standardvertragsklauseln nach Art. 46 Abs. 2 c) DSGVO. Aus Klausel 14 der Standardvertragsklauseln ergibt sich die Pflicht, zu prüfen ob der Datenempfänger im Empfängerland die zugesicherten Regelungen nach der dortigen Rechtslage einhalten kann. Diese Prüfung wird Transfer Impact Assessment genannt. Sie ist regelmäßig kaum zu leisten, da die Beurteilung des jeweiligen Rechtssystems außerordentlich komplex ist. Schulen sollten nur Vereinbarungen nach den Standardvertragsklauseln abschließen, zu denen der Schulträger oder das Kultusministerium ein positives Transfer Impact Assessment vorlegen können.

Datenschutzinformation

Grundlagen

Datenschutz als Grundrecht wurde 1983 vom Bundesverfassungsgericht festgelegt in der Aussage, dass jeder Mensch das Recht haben muss, über die Verarbeitung seiner Daten selbst zu bestimmen. Daher wird das Grundrecht auch das Recht auf informationelle Selbstbestimmung genannt und nicht das Grundrecht auf Datenschutz.

Die Möglichkeit selbstbestimmte Entscheidungen zu treffen, setzt Wissen voraus, worüber man entscheidet. Dementsprechend ist Transparenz über Datenverarbeitungen im Datenschutz von zentralem Wert. Ausfluss dieses Transparenzgebots in Art. 5 Abs. 1 a) DSGVO ist die Pflicht nach Art. 12 bis 14 DSGVO den Betroffenen vor Beginn der Datenverarbeitung Informationen zur Verfügung zu stellen.

Wichtig: Es handelt sich hierbei um eine Bereitstellungspflicht für den Verantwortlichen. Es handelt sich nicht um eine Pflicht zu informieren für die Betroffenen. Daraus ergibt sich, dass jede Abfrage, ob eine Person eine Datenschutzinformation gelesen habe oder zur Kenntnis genommen habe, eine unrechtmäßige Frage ist, da sie keinen legitimen Zweck erfüllt.

Art. 12 Abs. 1 DSGVO normiert allgemeine Kriterien für Datenschutzinformationen.

ALLGEMEINE TRANSPARENZANFORDERUNG NACH ART. 12 ABS. 1 DSGVO: Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch.

Angesichts der Vielzahl von Prozessen, in denen im Schulalltag personenbezogene Daten verarbeitet werden, ist schwer zu beurteilen, in welcher Genauigkeit Betroffene informiert werden können – ohne zugleich der Maßgabe der Verständlichkeit entgegenzuwirken.

Grundsätzlich ist zu empfehlen, dass Schulen unterschiedliche Datenschutzinformationen für die verschiedenen Zielgruppen Schülerinnen und Schüler, Eltern sowie Beschäftigte zur Verfügung stellen.

Für Schülerinnen und Schüler sowie für Eltern bietet es sich an, die Informationen über die Internetseite der Schule zur Verfügung zu stellen und bei Einschulung einmalig auf diese zu verweisen. Empfehlenswert ist ein modularer Aufbau, der Grundsatzthemen des Schullebens in einzelnen Blöcken adressiert. Treten zum Beispiel durch die Einführung neuer digitaler Dienste neue Formen der Datenverarbeitung hinzu, können die Dokumente um weitere Blöcke ergänzt werden.

Kommen Auftragsverarbeiter zum Einsatz, müssen diese nicht zwingend namentlich benannt werden. Ausreichend ist erst einmal die Information, dass Externe, die über entsprechende Verträge auf den Datenschutz verpflichtet sind, zum Einsatz kommen.

Die Pflicht zur Bereitstellung der Datenschutzinformationen liegt bei den Schulen. Die Schulträger können sie durch die Bereitstellung von Mustervorlagen unterstützen.

Information hinsichtlich Daten, die direkt vom Betroffenen stammen

Art. 13 DSGVO betrifft alle Daten, die direkt bei den Betroffenen erhoben werden. Das dürfte im Schulbetrieb die Mehrheit der Daten ausmachen. Die Norm listet auf, welche Angaben eine Datenschutzinformation mindestens umfassen muss. Dabei wird differenziert zwischen allgemeinen Informationen zum Verantwortlichen, Verweisen auf die bestehenden Rechte der Betroffenen aus der DSGVO und den Angaben zu den konkreten Verarbeitungen personenbezogener Daten.

Information hinsichtlich Daten, die von Dritten bezogen wurden

Art. 14 DSGVO gleicht Art. 13 fast vollständig, betrifft aber Daten, die der Verantwortliche nicht bei den Betroffenen selbst erhoben hat. Daraus ergibt sich die zusätzliche Pflicht nach Art. 14 Abs. 2 f) DSGVO die Quelle der Daten zu nennen. Zudem ist der Verantwortliche nach Art. 14 Abs. 3 DSGVO zur aktiven Information innerhalb bestimmter Fristen verpflichtet.

Die Relevanz des Art. 14 DSGVO dürfte im Schulalltag überschaubar sein, da Art. 14 Abs. 5 DSGVO Ausnahmen festlegt, wann auf die Information verzichtet werden kann. Hier spielt insbesondere Art. 14 Abs. 5 c) DSGVO eine Rolle, da die Schulen die Daten – zum Beispiel künftiger Schülerinnen und Schüler und ihrer Eltern – im Rahmen gesetzlich vorgegebener Prozesse erhalten.

Rechte der Betroffenen

Die DSGVO bietet den betroffenen Personen mehrere Rechte, die den Menschen eine wirksame Ausübung ihres Datenschutz-Grundrechts ermöglichen sollen.

Widerspruchsrecht

Die zentrale Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen von Verwaltungshandeln ist Art. 6 Abs. 1 e) DSGVO in Verbindung mit dem einschlägigen Verwaltungsrecht. Gegen diese Rechtsgrundlage räumt Art. 21 Abs. 1 DSGVO ein Widerspruchsrecht ein.

WIDERSPRUCHSRECHT NACH ART. 21 ABS. 1 DSGVO: Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e und f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling. Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Entscheidend für das Widerspruchsrecht ist der Verweis auf Gründe aus einer besonderen persönlichen Situation. Ob der Widerspruch erfolgreich ist, ist im Rahmen eines Widerspruchsverfahrens anhand des Merkmals aus Art. 21 Abs. 1 Satz 2 DSGVO zu beurteilen, ob die Schule wiederum zwingende schutzwürdige Gründe für die Verarbeitung nachweisen kann, die in Abwägung zu den Interessen der betroffenen Person überwiegen.

Auf das Bestehen des Widerspruchsrechts nach Art. 21 DSGVO ist in den Datenschutzinformationen deutlich hinzuweisen (laut Art. 21 Abs. 4 DSGVO in „von anderen Informationen getrennter Form“).

Widerrufsrecht

Sollte eine Verarbeitung nicht auf Basis der allgemeinen Rechtsgrundlage für Verwaltungshandeln (Art. 6 Abs. 1 e DSGVO) erfolgen, sondern auf Grundlage einer Einwilligung, steht den Einwilligenden nach Art. 7 Abs. 3 Satz 1 DSGVO das Recht zu, ihre Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Die Verarbeitung ist ab Widerruf einzustellen.

Recht auf Auskunft

Art. 15 DSGVO etabliert für die Betroffenen ein umfassendes und tiefgreifendes Auskunftsrecht. Die Existenz des Auskunftsrechts ist ein gewichtiges Argument für Datensparsamkeit – also das geringe Erfassen und Speichern von Daten in Kombination mit zügigem Löschen. Alle Daten, die aktuell nicht mehr vorhanden sind, müssen nicht beauskunftet werden.

Moderne IT-Systeme sollten im Sinne von Datenschutz durch Technikgestaltung nach Art. 25 Abs. 1 DSGVO (auch „Privacy by Design“ genannt) so eingerichtet werden, dass Auskunft leicht und umfassend bereitgestellt werden kann. Schulträger sollten diese Anforderung bei der Auswahl von digitalen Diensten berücksichtigen.

Auskunft ist nach Art. 12 Abs. 3 Satz 1 DSGVO innerhalb eines Monats zu erteilen. Diese Frist kann um zwei Monate verlängert werden, wenn die Komplexität oder die Zahl der Anfragen dies erforderlich macht.

Recht auf Berichtigung

Nach Art. 16 DSGVO dürfen Betroffene die Berichtigung fehlerhaft erfasster Daten verlangen.

Recht auf Löschung

Aus Art. 17 DSGVo dürfen Betroffene Löschung ihrer Daten verlangen. Diesem Verlangen kann der Verantwortliche aber eigene Speicherpflichten entgegenhalten, wie sie sich aus gesetzlichen Aufbewahrungspflichten ergeben können.

Soweit Aufbewahrungspflichten fehlen, ist eine Beurteilung oft komplex, ob sich aus allgemeinen Gesichtspunkten Aufbewahrungspflichten ergeben oder der Löschaufforderung nachzukommen ist.

Effiziente Löschfunktionen, die auch möglichst alle Arten von „Schattendaten“ umfassen, sind im Sinne von Datenschutz durch Technikgestaltung nach Art. 25 Abs. 1 DSGVO bei der Einführung neuer Anwendungen bereits zu berücksichtigen.

Recht auf Einschränkung der Verarbeitung

Die Einschränkung der Datenverarbeitung ist der „kleine Bruder“ des Löschens. Einschränken wird oft auch „Sperren“ der Daten genannt. Durch Einschränken der Daten wird der Kreis der Personen verkleinert, die ursprünglich Zugang zu den Daten hatten, ohne dass die Daten vollständig aus dem System gelöscht werden.

Für den Zeitraum, in dem Daten nicht mehr aktiv genutzt werden, aber für die Einhaltung von Aufbewahrungsfristen weiterhin gespeichert werden, ist eine Einschränkung der Zugangsrechte im Sinne von Datenschutz durch Technikgestaltung nach Art. 25 Abs. 1 DSGVO sehr zu empfehlen. Letztlich entspricht dieser Punkt der fortlaufenden Aktualisierung des Berechtigungskonzepts.

Mitteilungspflichten

In den Fällen einer Berichtigung, Löschung oder Einschränkung von Daten, die zuvor Dritten zur Verfügung gestellt wurden (z.B. anderen Behörden), ergibt sich aus Art. 19 DSGVO eine Mitteilungspflicht an diese Dritten.

Recht auf Datenübertragbarkeit

Art. 20 DSGVO normiert ein Recht auf Datenübertragbarkeit, das aber auf Daten beschränkt ist, die die berechtigte Person dem Verantwortlichen bereitgestellt hat. Das umfasst nicht Daten, die der Verantwortliche selbst erfasst hat. Damit betrifft die Norm keine Daten, die zum Beispiel Lehrkräfte zu Schülerinnen und Schülern erhoben haben oder Nutzungsprotokolle, die von den Anwendungen automatisiert erstellt wurden.

Der Anspruch kann sich aber auf Leistungen der Schülerinnen und Schüler beziehen, die sie erbracht und in den digitalen Diensten der Schule gespeichert haben. Insoweit sollten alle Dienste, die solche Speicherungen von Eigenleistungen vorsehen, im Sinne von Datenschutz durch Technikgestaltung nach Art. 25 Abs. 1 DSGVO eine Exportfunktion umfassen, über die den Betroffenen ihre Daten zur Verfügung gestellt werden können.

Verbot automatisierter Entscheidungen oder einer automatisierten Profilbildung

Jeder Mensch hat nach Art. 22 DSGVO das Recht, nicht einer Entscheidung unterworfen zu sein, die ausschließlich auf einer automatisierten Entscheidung beruht und der betroffenen Person gegenüber rechtliche Wirkung entfalten kann oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies gilt auch für die rein automatisierte Erstellung eines Profils der betroffenen Person.

Diese Norm schließt zum Beispiel aus, dass Schulnoten rein automatisiert vergeben werden oder Schülerinnen oder Schüler automatisiert bestimmten Leistungsgruppen zugeordnet werden. Möglich ist aber, dass eine Anwendung Vorschläge mit Bezug auf einzelne Personen entwickelt, so lange anschließend ein Mensch die abschließende Entscheidung auf Grundlage eigener Erwägungen trifft.

Datenschutzmanagement

Neben den Rechten und Pflichten, die die Betroffenen im Sinne des Grundrechtsschutzes unmittelbar betreffen, legt die DSGVO den Verantwortlichen weitere Pflichten auf. Diese lassen sich unter der Überschrift Datenschutzmanagement zusammenfassen.

Datenschutzbeauftragte

Die Art. 37 bis 39 DSGVO legen fest, wann eine Organisation eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benötigt, sowie was deren Rechte und Aufgaben sind. Behörden, und damit auch Schulen, benötigen nach Art. 37 Abs. 1 a) DSGVO immer eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten. Art. 37 Abs. 3 DSGVO stellt klar, dass für mehrer Behörden (Schulen) gemeisnam eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter bestellt werden kann.

Die Aufgaben der Datenschutzbeauftragten sind in Art. 39 DSGVO festgelegt und fokussieren sich auf die zwei Komponenten Beratung und Kontrolle. Die Verarbeitung personenbezogener Daten ist niemals durch Datenschutzbeauftragte zu genehmigen, sie sollten aber gerade bei der Einführung neuer Dienste einbezogen und zur Stellungnahme aufgefordert werden.

Verzeichnis der Verarbeitungstätigkeiten

Nach Art. 30 DSGVO haben Verantwortliche und Auftragsverarbeiter Verzeichnisse ihrer Verarbeitungstätigkeiten zu führen (oft als „VVT" abgekürzt). In weiten Teilen sind die Informationen im VVT deckungsgleich mit den Angaben in den Datenschutzinformationen. Der Wortlaut der DSGVO sagt es nicht, aber nach dem Zweck der Norm sollte der Eintrag in das VVT zu jeder Verarbeitung auch eine Beschreibung des Prozesses umfassen.

Wichtig ist, dass es nicht um ein Verzeichnis der genutzen Dienste oder Anwendungen geht. Der Blick der DSGVO ist auf den Tätigkeiten, also den verschiedenen Prozessen, die mit einer Anwendung durchgeführt werden. Sollten mehrere Anwendungen für einen Prozess benötigt werden, sollten alle diese Anwendungen in dem Prozess genannt werden. Es ergibt sich daraus ein Eintrag im Verzeichnis. Kann eine Anwendung aber für unterschiedliche Prozesse genutzt werden (wie Outlook z.B. als E-Mail-Client, Kontaktverzeichnis und Termin- und Aufgabenverwaltung), ist diese Anwendung in unterschiedlichen Einträgen zu den einzelnen Prozessen zu dokumentieren.

Um die Verzeichnisse mit vertretbarem Aufwand auf aktuellem Stand zu halten, ist der Einsatz einer Datenschutzmanagementsoftware empfehlenswert. Soweit allein mit Office-Dokumenten wie Textdatei oder einer Tabelle gearbeitet wird, ist der Aktualisierungsaufwand extrem, wenn einzelne Anwendungen eine Vielzahl von Prozessen betreffen.

Optimalerweise stellt der Schulträger den Schulen Musterverzeichnisse zu den typischen Verarbeitungsprozessen in einer Schule zur Verfügung. Das dient auch der Einheitlichkeit der Datenschutzdokumentation im Verantwortungsbereich des Schulträgers.

Fortlaufende Überprüfung und Anpassung

Wie oben im Abschnitt Datensicherheit bereits angesprochen, ist fortlaufende Überprüfung und Aktualisierung im Datenschutz wichtig. Neben der Aktualisierung der Schutzmaßnahmen (siehe Sicherheit) betrifft dies auch die Datenschutzdokumentation.

Hierfür sollten mit den Datenschutzverantwortlichen an den Schulen, speziell den Datenschutzbeauftragten wiederkehrende Prozesse etabliert werden. Etablierte Audit-Mechanismen aus dem Bereich des Qualitätsmanagements sind sehr zu empfehlen.

Rechenschaftspflicht

Im Rahmen des Datenschutzmanagement sei erneut auf die zentrale Pflicht aus Art. 5 Abs. 2 DSGVO verwiesen, dass der Verantwortliche in der Lage sein muss durch entsprechende Dokumentation zur allen Aspekten des Datenschutz Rechenschaft abzulegen (also Nachweise bereitstellen zu können).

Schwellwertanalyse und Datenschutzfolgenabschätzung

Im Mittelpunkt der Risikoanalyse steht die Datenschutfolgenabschätzung („DSFA“) nach Art. 35 DSGVO. Eine DSFA ist erforderlich, wenn eine Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Datenschutzrechte der Betroffenen zur Folge hat. Art. 35 Abs. 1 DSGVO nennt beispielhaft Kriterien, wann ein hohes Risiko vorliegen könnte.

Die Beurteilung, ob ein solches hohes Risiko vorliegt, erfolgt im Rahmen einer sogenannten Schwellwertanalyse („SWA“).

Schwellwertanalyse

Art. 35 Abs. 3 DSGVO nennt drei konkrete Konstellationen, in denen eine DSFA erforderlich ist. Von diesen dürfte keine auf Anwendungen im Schulbetrieb zutreffend sein.

Der Europäische Datenschutzausschuss („EDSA“) hat bereits 2017 das Working Paper 248 veröffentlicht, das neun typische Kriterien nennt, die im Rahmen einer Schwellwertanalyse betrachtet werden sollten.[1] Sollten zwei der neun Kriterien erfüllt sein, sei regelmäßig von der Erforderlichkeit einer DSFA auszugehen.

Aus dieser Liste ist im Schulalltag, wenn die Verarbeitung die Schülerinnen und Schüler betrifft, das 7. Kriterium einschlägig: Verarbeitung von Daten schutzbedürftiger Gruppen, konkret Kinder.

Einzelne Anwendungen wie ein digitales Klassenbuch, in dem auch krankheitsbedingte Fehlzeiten vermerkt werden, erfüllen das 4. Kriterium – Verarbeitung von besonders schützenswerten Datenkategorien, speziell Gesundheitsdaten.

Schwer zu greifen ist das 5. Kriterium der umfangreichen Verarbeitung. Ob eine Gruppe von z.B. tausend Schülerinnen und Schülern schon eine umfangreiche Verarbeitung im Sinne des EDSA darstellt, kann bezweifelt werden. Der Fokus bei Erstellung der Schwellwerte war auf gesamtgesellschaftlich gesehen umfangreichen Verarbeitungen. Auf die Größe einer Kommune oder gar eines Bundeslandes bezogen, stellt die Verarbeitung der Daten an einer Schule keine umfangreiche dar.

1WP 248 Rev. 01 - Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt (datenschutz-bayern.de)

Wenn man aber die Zahl im Zusammenspiel mit der Schutzbedürftigkeit der Schülerinnen und Schüler, einzelnen Verarbeitungen besonders schützenswerter Datenkategorien und der Bedeutung schulischer Daten sowohl für die persönliche Entwicklung wie für das gesellschaftliche Ansehen sieht, dürfte für zentrale Anwendungen des Schulbetriebs die Grenze zum hohen Risiko erreicht sein.

Für den Schulbetrieb begleitende oder ergänzende Anwendungen, insbesondere solche die nur Daten der Lehrkräfte verarbeiten, dürfte die Schwelle zum hohen Risiko regelmäßig nicht erreicht sein.

Letztlich ist für jede einzelne Verarbeitungstätigkeit eine SWA durchzuführen und möglichst im VVT zu dokumentieren.

Datenschutzfolgenabschätzung

Ist eine DSFA erforderlich, initiiert dies einen eigenständigen DSFA-Prozess. Es ist ein DSFA-Team zu bilden ist aus Personen, die den betreffenden Prozess fachlich beurteilen können, Personen, die die eingesetzten digitalen Anwendungen in ihrer Tiefe beurteilen können, und betroffenen Personen, deren Perspektive ebenfalls einbezogen werden soll. Die oder der Datenschutzbeauftragte ist beratend ebenfalls einzubeziehen.

Der Schulträger sollte den Schulen Muster für die DSFA zu den typischerweise nach Art. 35 DSGVO prüfpflichtigen Datenverarbeitungen zur Verfügung stellen.

Der DSFA-Prozess läuft regelmäßig in fünf Schritten ab.

1. Zuerst sind die Risiken zu formulieren, die sich aus dem personenbezogene Daten verarbeitenden Prozess und aus dem Einsatz der angestrebten Anwendungen und IT-Infrastruktur ergeben können.

2. Diesen Risiken sind ohne Blick auf Schutzmaßnehmen Risikowerte zuzuordnen auf Basis der Eintrittswahrscheinlichkeit der Risikoverwirklichung und des Schadensausmaß einer Risikoverwirklichung.

3. Anschließend sind Schutzmaßnahmen zu formulieren und den Risiken zuzuordnen.

4. Darauf erfolgt eine erneute Risikobewertung unter Einbeziehung der ergriffenen Schutzmaßnahmen.

5. Abschließend sind die verbliebenen Restrisiken dahingehend zu beurteilen, ob sie vom Verantwortlichen als vertretbare Restrisiken akzeptiert werden können.

Optimalerweise gelangt das DSFA-Team bei der finalen Beurteilung dazu, dass alle verbliebenen Risiken akzeptabel sind, so dass der Verantwortliche eine positives Ergebnis der DSFA festhalten und dokumentieren kann. Sollte ein positives Ergebnis auch durch weitere Schutzmaßnahmen nicht erreicht werden können, ist entweder auf die geprüfte Art der Datenverarbeitung zu verzichten oder das Ergebnis nach Art. 36 DSGVO der zuständigen Datenschutzaufsichtsbehörde zur Konsultation vorzulegen.

Die DSFA beziehungsweise die in ihr dokumentierte Risikobewertung ist regelmäßig zu wiederholen, um veränderten Rahmenbedingungen Rechnung tragen zu können.

Checkliste für die Einhaltung von Datenschutzpflichten

Die Checkliste für Schulträger und die Checkliste für Schulen auf den Folgeseiten geben eine Übersicht, welchen Fragen die jeweilige Verwaltungsebene sich stellen sollte.

Die Kultusministerien der Länder sind eingeladen, diese Vorlagen auf Basis der im Schul- und Dienstrecht des Landes geltenden Vorgaben zu konkretisieren.

Ebenso sind die Schulträger eingeladen, die Checklisten auf Grundlage der Gegebenheiten in ihrem Zuständigkeitsbereich zu konkretisieren.

Je konkreter die Checklisten durch Vorarbeit der höheren Verwaltungsebenen ausgearbeitet werden können, desto hilfreicher sind sie für die Schulen. Im Optimalfall erhalten Schulen über ihr Ministerium und ihren Schulträger neben den Rahmendatenschutzkonzepten in einem Umfang Vorgaben, Handreichungen und Muster, dass die Schule sich auf einige wenige abschließende Datenschutzfragen beschränken kann, die allein in der Schule entschieden werden können.

Checkliste für Schulträger

Nr.	Thema/ Fragestellung	Referenz
1.0	Wie ist die Art und Weise der Datenverarbeitung zu beschreiben?	Übergreifend
1.0.1	Gibt es zu dieser Art der Datenverarbeitung konkrete Vorgaben aus dem Kultusministerium?	Übergreifend
1.1	Durch welche Vorschriften im Schul- oder Dienstrecht ist diese Verarbeitung personenbezogender Daten vorgegeben?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 6 Abs. 1 e) DSGVO
1.2	Welchem Zweck dient die Verarbeitung personenbezogender Daten?	Siehe „Rechtmäßigkeit der Datenverarbeitung“
1.3	Von welchen Personengruppen werden durch die Tätigkeit alles Daten verarbeitet?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 13, 14 sowie 30 DSGVO
1.3.1	Werden Daten von Schutzbefohlenen, insbesondere Kindern und Jugendlichen verarbeitet?	Siehe „Schwellwertanalyse“; Working Paper 248 des EDSA
1.4	Welche Kategorien von Daten werden innerhalb des Prozesses verarbeitet?	Siehe Art. 30 DSGVO
1.4.1	Werden durch den Prozess besonders schützenswerte Daten nach Art. 9 Abs. 1 DSGVO verarbeitet?	Siehe „Rechtmäßigkeit der Datenverarbeitung“, „Schwellwertanalyse“, Art. 9, 30, 32, 35 DSGVO
2.0	Wer ist der Verantwortliche für die Verarbeitung personenbezogener Daten? Wer bestimmt über die Zwecke und Mittel der Datenverarbeitung?	Siehe „Verantwortlichkeit nach DSGVO“, Art. 4 Nr. 7 DSGVO
2.1	Verarbeitet der Schulträger personenbezogene Daten in eigener Verantwortung?	Siehe „Verantwortlichkeit nach DSGVO“, Art. 4 Nr. 7, 6, 9 DSGVO
2.2	Verarbeitet der Schulträger personenebezogene Daten aus den Schulen als deren Auftragsverarbeiter?	Siehe „Verantwortlichkeit nach DSGVO“, „Dienstleisterbindung (Auftragsverarbeitung), Art. 4 Nr. 8, 28 DSGVO

2.2.1	Wenn ja, wurde mit den Schulen eine Vereinbarung über die Auftragsverarbeitung geschlossen?	Siehe „Dienstleisterbindung (Auftragsverarbeitung)“, Art. 28 DSGVO
2.3	Greift der Schulträger für die Verarbeitung der personenbezogenen Daten auf Externe als Auftragsverarbeiter zurück? Wenn ja, wer sind die Auftragsverarbeiter?	Siehe „Dienstleisterbindung (Auftragsverarbeitung)“, Art. 28 DSGVO
2.3.1	Wurde mit den nachgeordneten Auftragsverarbeitern jeweils eine Vereinbarung über die Auftragsverarbeitung geschlossen?	Siehe „Dienstleisterbindung (Auftragsverarbeitung)“, Art. 28 DSGVO
2.4	Verarbeitet der Schulträger personenbezogene Daten in gemeinsamer Verantwortung? Wenn ja, wer sind die weiteren Parteien der gemeinsamen Verantwortung?	Siehe „Verantwortlichkeit nach DSGVO“, „Kooperationen (Gemeinsame Verantwortung)“, Art. 26 DSGVO
2.4.1	Liegt eine Vereinbarung zur Verarbeitung in gemeinsamer Verantwortung vor?	Siehe „Kooperationen (Gemeinsame Verantwortung)“, Art. 26 DSGVO
2.5	Ist der Schulträger nicht unmittelbar in die Datenverarbeitung einbezogen, trägt aber als zuständige Behörde für die digitale Ausstattung der Schulen eine indirekte Verantwortung, aus der heraus er die Verarbeitung personenbezogener Daten im Sinne eines Rahmendatenschutzkonzepts für die Schulen die Einhaltung des Datenschutzes prüfen und dokumentieren sollte?	Siehe „Verantwortlichkeit nach DSGVO“, Art. 5 Abs. 2 DSGVO
2.5.1	Wenn ja, wurde ein Rahmendatenschutzkonzept erstellt und den Schulen zur Verfügung gestellt?	Siehe „Verantwortlichkeit nach DSGVO“, Art. 5 Abs. 2 DSGVO
3.0	Liegt eine Rechtsgrundlage für die Datenverarbeitung vor? (siehe oben zur Norm im Schul- oder Dienstrecht, die die Verarbeitung vorgibt)	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 6 Abs. 1 e), 9 Abs. 2 DSGVO
3.1	Ist die Datenverarbeitung in der geplanten Form zur Zweckerreichung erforderlich, insbesondere könnte der Zweck auch durch eine Art der Datenverareitung erreicht werden, der die Rechte und Freiheiten der Betroffenen weniger einschränkt?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 5 Abs. 1, 6 Abs. 1, 9 Abs. 2 DSGVO
3.2	Wenn Art-9-Daten verarbeitet werden, liegt eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vor?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 9 Abs. 2 DSGVO

3.3	Werden Daten auf Grundlage einer Einwilligung verarbeitet?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 6 Abs. 1 a), 7, 8, 9 Abs. 2 a) DSGVO
3.3.1	Wenn Daten auf Grundlage einer Einwilligung verarbeitet werden, waren die Einwilligenden ausreichend über die Umstände der Datenverarbeitung informiert und haben in einer klaren und dokumentierten Form eingewilligt?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 7 DSGVO
3.3.2	Wurde den Schulen eine Mustereinwilligungserklärung zur Verfügung gestellt?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 7 DSGVO
3.3.3	Bestehen Zweifel, dass die Einwilligung freiwillig abgegeben wurde?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 7 DSGVO
4.0	Wurde ein Sicherheitskonzept für diese Verarbeitung oder die für diese Verarbeitung genutzte Anwendung erstellt?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.1	Besteht ein Berechtigungskonzept basierend auf technischen Rechten und organisatorischen Rollen für diese digitale Anwendung?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO
4.1.1	Unterstützt das Berechtigungskonzept die Beschränkung der Zugänge auf das für die Zweckerreichung erforderliche Minimum?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO
4.1.2	Umfasst das Berechtigungskonzept Prozesse zur Einschränkung der Verarbeitung von Daten, die in der aktiven Nutzung nicht mehr benötigt werden und allein aus Aufbewahrungspflichten weiter gespeichert bleiben?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO
4.1.3	Steht die Anwendung mehreren Schulen zur Verfügung und wurde daher ein Mandantenkonzept erstellt und umgesetzt?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO
4.1.4	Prüft die Schule regelmäßig (zumindest jährlich) die Zuweisung der Rollen an die einzelnen Nutzenden der Anwendung und entzieht nicht mehr benötigte Rechte?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO

4.2	Sind alle Lehrkräfte und Mitarbeitenden der Schulen durch das Dienstrecht ausreichend auf die Vertraulichkeit verpflichtet oder bedarf es spezieller Vertraulichkeitsverpflichtungen?	Siehe „Vertraulichkeitsverpflichtung“; Art. 24, 32 DSGVO
4.2.1	Sind alle Lehrkräfte und Mitarbeitenden der Schulen ausreiched in Fragen der Vertraulichkeit und Datensicherheit geschult?	Siehe „Vertraulichkeitsverpflichtung“; Art. 24, 32 DSGVO
4.2.2	Sind alle Administratoren in ausreichender Weise auf ihre besonderen Pflichten im Hinblick auf Vertraulichkeit und Datensicherheit verpflichtet und geschult?	Siehe „Vertraulichkeitsverpflichtung“; Art. 24, 32 DSGVO
4.3	Besteht ein Protokollierungskonzept für diese Anwendung und wurde dessen Rechtmäßigkeit zur Vermeidung übermäßiger Überwachung geprüft?	Siehe „Protokollierungskonzept“; Art. 24, 25, 32 DSGVO
4.4	Sind die Aufbewahrungsfristen für die Speicherung personenbezogener Daten in diesem Prozess bzw. dieser Anwendung festgelegt?	Siehe „Löschkonzept“; Art. 24, 25, 32 DSGVO
4.4.1	Sind Löschprozesse für diese Verarbeitungstätigkeit definiert? Handelt es sich um automatisierte oder manuelle Löschungen?	Siehe „Löschkonzept“; Art. 24, 25, 32 DSGVO
4.4.2	Sind Verantwortliche für das Löschen festgelegt und wird das Löschen in Löschprotokollen dokumentiert?	Siehe „Löschkonzept“; Art. 24, 25, 32 DSGVO
4.4.3	Kommt als Alternative zum Löschen das Anonymisieren von Daten zum Einsatz? Wenn ja, wurde die Wirksamkeit des Anonymisierens überprüft?	Siehe „Löschkonzept“; Art. 24, 25, 32 DSGVO
4.5	Welche Form des Zugangsschutzes kommt bei dieser Anwendung zum Einsatz? Anbindung an einen zentralen Verzeichnisdienst (Single-Sign-on z.B. über ein Active Directory), Passwortschutz, Zwei-Faktor-Authentifizierung oder Passkey-Technologie?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.6	Wurde auf allen eingesetzten Endgeräten die Festplattenverschlüsselung aktiviert?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO

4.7	Stehen den Schulen redundante Netzanbindungen zur Verfügung?	Siehe „Datensicherheit"; Art. 24, 32 DSGVO
4.8	Wurden die Server der eingesetzten Anwendung einem Lasttest unterzogen mit zufriedenstellenden Ergebnissen?	Siehe „Datensicherheit"; Art. 24, 32 DSGVO
4.9	Wie sieht der Backup-Prozess aus?	Siehe „Datensicherheit"; Art. 24, 25, 32 DSGVO
4.9.1	Befinden sich Backups an verschiedenen Orten?	Siehe „Datensicherheit"; Art. 24, 25, 32 DSGVO
4.9.2	Gibt es Backups über verschiedenen Zeitintervalle?	Siehe „Datensicherheit"; Art. 24, 25, 32 DSGVO
4.9.3	Wird die Wiederherstellung der Daten aus den Backups regelmäßig überprüft? Mit welchem Ergebenis?	Siehe „Datensicherheit"; Art. 24, 25, 32 DSGVO
4.10	Sind alle Datenübertragungen Ende-zu-Ende-verschlüsselt?	Siehe „Datensicherheit"; Art. 24, 25, 32 DSGVO
	Kommen im Rahmen dieses Prozesses Datenübertragungen per E-Mail zum Einsatz und ist für die Daten in diesem Prozess das Schutzniveau der Transportverschlüsselung ausreichend?	Siehe „Datensicherheit"; Art. 24, 25, 32 DSGVO
4.11.	Kommt in diesem Prozess die Pseudonymisierung von Daten zum Einsatz? Wenn ja, wie ist sie organisiert? Wo ist das Zuordnungverzeichnis von Pseudonym zu Person gespeichert?	Siehe „Datensicherheit"; Art. 24, 25, 32 DSGVO
4.12	Werden die Schutzmaßnahmen aus der Datensicherheit regelmäßig überprüft (auditiert) und das Ergebnis dokumentiert? Wie ist die letzte Überprüfung ausgefallen?	Siehe „Datensicherheit"; Art. 24, 25, 32 DSGVO
5.0	Wird die Aktualität der Datenschutzdokumente regelmäßig evaluiert und werden die Dokumente nach Bedarf aktualisiert? Was sind die Ergebnisse der letzten Evaluation?	Siehe „Datenschutzmanagement"; Art. 32 DSGVO

5.1	Wurde den Schulen für diese Verarbeitungstätigkeit eine Musterblock für ihre Datenschutzinformation zur Verfügung gestellt?	Siehe „Datenschutzinformation“; Art. 12-14 DSGVO
5.2	Wurde den Schulen für diese Verarbeitungstätigkeit ein Mustereintrag für ihr Verzeichnis der Verarbeitungstätigkeiten zur Verfügung gestellt?	Siehe „Datenschutzmanagement“; Art. 30 DSGVO
6.0	Kommt es zu Datenübertragungen in Drittstaaten? Wenn ja, wie sind diese nach den Maßgaben der Art. 44 bis 49 DSGVO abgesichert?	Siehe „Drittstaatentransfers“; Art. 44-50 DSGVO
7.1	Enthält die im Prozess eingesetzte Anwendung Funktionen, um Ansprüche auf Auskunft fristgerecht bedienen zu können?	Siehe „Rechte der Betroffenen“; Art. 15 DSGVO
7.2	Enthält die im Prozess eingesetzte Anwendung Funktionen, um Ansprüche auf Löschung fristgerecht bedienen zu können?	Siehe „Rechte der Betroffenen“; Art. 17 DSGVO
7.3	Enthält die im Prozess eingesetzte Anwendung Funktionen, um Ansprüche auf Datenübertragung (Datenexoport) bedienen zu können?	Siehe „Rechte der Betroffenen“; Art. 20 DSGVO
7.4	Trifft die im Prozess eingesetzte Anwendung Entscheidungen mit Rechtsverbindlichkeit, die allein auf automatisierten Prozessen beruhen?	Siehe „Rechte der Betroffenen“; Art. 22 DSGVO
7.5	Nutzt die im Prozess eingesetzte Anwendung Funktionen künstlicher Intelligenz? Wenn ja, welche Prozesse konkret sind das?	Siehe „Rechtmäßigkeit der Datenverarbeitung“, „Kooperationen (Gemeinsame Verantwortung)“; KIVO
7.5.1	Wenn KI zum Einsatz kommt, nutzt die Technologie die von ihr verarbeiteten Daten zur weiteren Verbesserung des KI-Modells? Auf welcher Rechtsgrundlage geschieht das?	Siehe „Rechtmäßigkeit der Datenverarbeitung“, „Kooperationen (Gemeinsame Verantwortung)“; KIVO
8.1	Hat der Schulträger eine oder einen Datenschutzbeauftragte*n, die ausreichend qualifiziert ist und in alle datenschutzrelevanten Prozesse eingebunden ist?	Siehe „Datenschutzmanagement“; Art. 37-39 DSGVO

8.2	Nutzt der Schulträger selbst eine Datenschutzmanagementanwendung?	Siehe „Datenschutzmanagement“; Art. 5 Abs. 2 DSGVO
8.2.1	Stellt der Schulträger den Schulen eine Datenschutzmanagementanwendung zur Verfügung und wird diese von den Schulen genutzt?	Siehe „Datenschutzmanagement“; Art. 5 Abs. 2 DSGVO
9.0	Wurde für diese Verarbeitungstätigkeit eine Schwellwertanalyse durchgeführt und dokumentiert, ob für diese Tätigkeit eine Datenschutzfolgenabschätzung erforderlich ist? Mit welchem Ergebnis?	Siehe „Schwellwertanalyse und Datenschutzfolgenabschätzung“; Art. 35 DSGVO, Working Paper 248 des EDSA
9.1	Wenn eine Datenschutzfolgenabschätzung erforderlich ist, wurde diese durchgeführt und dokumentiert? Mit welchem Ergebnis?	Siehe „Schwellwertanalyse und Datenschutzfolgenabschätzung“; Art. 35 DSGVO

Checkliste für Schulen

Nr.	Thema/ Fragestellung	Referenz
1.0	Wie ist die Art und Weise der Datenverarbeitung zu beschreiben?	Übergreifend
1.0.1	Gibt es zu dieser Art der Datenverarbeitung konkrete Vorgaben aus dem Kultusministerium?	Übergreifend
1.0.2	Gibt es zu dieser Art der Datenverarbeitung konkrete Vorgaben des Schulträgers?	Übergreifend
1.1	Durch welche Vorschriften im Schul- oder Dienstrecht ist diese Verarbeitung personenbezogender Daten vorgegeben?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 6 Abs. 1 e) DSGVO
1.2	Welchem Zweck dient die Verarbeitung personenbezogender Daten?	Siehe „Rechtmäßigkeit der Datenverarbeitung“
1.3	Von welchen Personengruppen werden durch die Tätigkeit alles Daten verarbeitet?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 13, 14 sowie 30 DSGVO
1.3.1	Werden Daten von Schutzbefohlenen, insbesondere Kindern und Jugendlichen verarbeitet?	Siehe „Schwellwertanalyse“; Working Paper 248 des EDSA
1.4	Welche Kategorien von Daten werden innerhalb des Prozesses verarbeitet?	Siehe Art. 30 DSGVO
1.4.1	Werden durch den Prozess besonders schützenswerte Daten nach Art. 9 Abs. 1 DSGVO verarbeitet?	Siehe „Rechtmäßigkeit der Datenverarbeitung“, „Schwellwertanalyse“, Art. 9, 30, 32, 35 DSGVO
2.0	Wer ist der Verantwortliche für die Verarbeitung personenbezogener Daten? Wer bestimmt über die Zwecke und Mittel der Datenverarbeitung?	Siehe „Verantwortlichkeit nach DSGVO“, Art. 4 Nr. 7 DSGVO

2.1	Ist der Schulträger nicht unmittelbar in die Datenverarbeitung einbezogen, trägt aber als zuständige Behörde für die digitale Ausstattung der Schulen eine indirekte Verantwortung, aus der heraus er die Verarbeitung personenbezogener Daten im Sinne eines Rahmendatenschutzkonzepts für die Schulen die Einhaltung des Datenschutzes prüfen und dokumentieren sollte?	Siehe „Verantwortlichkeit nach DSGVO“, Art. 5 Abs. 2 DSGVO
2.1.1	Wenn ja, hat der Schulträger ein Rahmendatenschutzkonzept erstellt und den Schulen zur Verfügung gestellt?	Siehe „Verantwortlichkeit nach DSGVO“, Art. 5 Abs. 2 DSGVO
2.2	Gibt es Auftragsverarbeiter und wurde mit ihnen eine Vereinbarung über die Auftragsverarbeitung geschlossen? Ist der Schulträger als Auftragsverarbeiter eingebunden?	Siehe „Dienstleisterbindung (Auftragsverarbeitung)“, Art. 28 DSGVO
2.3	Verarbeitet der Schulträger oder eine andere Partei personenbezogene Daten in gemeinsamer Verantwortung? Wenn ja, wer sind die weiteren Parteien der gemeinsamen Verantwortung?	Siehe „Verantwortlichkeit nach DSGVO“, „Kooperationen (Gemeinsame Verantwortung)“, Art. 26 DSGVO
2.3.1	Liegt eine Vereinbarung zur Verarbeitung in gemeinsamer Verantwortung vor?	Siehe „Kooperationen (Gemeinsame Verantwortung)“, Art. 26 DSGVO
3.0	Liegt eine Rechtsgrundlage für die Datenverarbeitung vor? (siehe oben zur Norm im Schul- oder Dienstrecht, die die Verarbeitung vorgibt)	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 6 Abs. 1 e), 9 Abs. 2 DSGVO
3.1	Ist die Datenverarbeitung in der geplanten Form zur Zweckerreichung erforderlich, insbesondere könnte der Zweck auch durch eine Art der Datenverareitung erreicht werden, der die Rechte und Freiheiten der Betroffenen weniger einschränkt?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 5 Abs. 1, 6 Abs. 1, 9 Abs. 2 DSGVO
3.2	Wenn Art-9-Daten verarbeitet werden, liegt eine Rechtsgrundlage nach Art. 9 Abs. 2 DSGVO vor?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 9 Abs. 2 DSGVO
3.3	Werden Daten auf Grundlage einer Einwilligung verarbeitet?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 6 Abs. 1 a), 7, 8, 9 Abs. 2 a) DSGVO

3.3.1	Wenn Daten auf Grundlage einer Einwilligung verarbeitet werden, waren die Einwilligenden ausreichend über die Umstände der Datenverarbeitung informiert und haben in einer klaren und dokumentierten Form eingewilligt?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 7 DSGVO
3.3.2	Wurde den Schulen eine Mustereinwilligungserklärung zur Verfügung gestellt?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 7 DSGVO
3.3.3	Bestehen Zweifel, dass die Einwilligung freiwillig abgegeben wurde?	Siehe „Rechtmäßigkeit der Datenverarbeitung“; Art. 7 DSGVO
4.0	Wurde ein Sicherheitskonzept für diese Verarbeitung oder die für diese Verarbeitung genutzte Anwendung erstellt?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.1	Besteht ein Berechtigungskonzept basierend auf technischen Rechten und organisatorischen Rollen für diese digitale Anwendung?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO
4.1.1	Unterstützt das Berechtigungskonzept die Beschränkung der Zugänge auf das für die Zweckerreichung erforderliche Minimum?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO
4.1.2	Umfasst das Berechtigungskonzept Prozesse zur Einschränkung der Verarbeitung von Daten, die in der aktiven Nutzung nicht mehr benötigt werden und allein aus Aufbewahrungspflichten weiter gespeichert bleiben?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO
4.1.3	Steht die Anwendung mehreren Schulen zur Verfügung und wurde daher ein Mandantenkonzept erstellt und umgesetzt?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO
4.1.4	Prüft die Schule regelmäßig (zumindest jährlich) die Zuweisung der Rollen an die einzelnen Nutzenden der Anwendung und entzieht nicht mehr benötigte Rechte?	Siehe „Berechtigungskonzept und Mandantenkonzept“; Art. 24, 25, 32 DSGVO

4.2	Sind alle Lehrkräfte und Mitarbeitenden der Schulen durch das Dienstrecht ausreichend auf die Vertraulichkeit verpflichtet oder bedarf es spezieller Vertraulichkeitsverpflichtungen?	Siehe „Vertraulichkeitsverpflichtung“; Art. 24, 32 DSGVO
4.2.1	Sind alle Lehrkräfte und Mitarbeitenden der Schulen ausreiched in Fragen der Vertraulichkeit und Datensicherheit geschult?	Siehe „Vertraulichkeitsverpflichtung“; Art. 24, 32 DSGVO
4.2.2	Sind alle Administratoren in ausreichender Weise auf ihre besonderen Pflichten im Hinblick auf Vertraulichkeit und Datensicherheit verpflichtet und geschult?	Siehe „Vertraulichkeitsverpflichtung“; Art. 24, 32 DSGVO
4.3	Besteht ein Protokollierungskonzept für diese Anwendung und wurde dessen Rechtmäßigkeit zur Vermeidung übermäßiger Überwachung geprüft?	Siehe „Protokollierungskonzept“; Art. 24, 25, 32 DSGVO
4.4	Sind die Aufbewahrungsfristen für die Speicherung personenbezogener Daten in diesem Prozess bzw. dieser Anwendung festgelegt?	Siehe „Löschkonzept“; Art. 24, 25, 32 DSGVO
4.4.1	Sind Löschprozesse für diese Verarbeitungstätigkeit definiert? Handelt es sich um automatisierte oder manuelle Löschungen?	Siehe „Löschkonzept“; Art. 24, 25, 32 DSGVO
4.4.2	Sind Verantwortliche für das Löschen festgelegt und wird das Löschen in Löschprotokollen dokumentiert?	Siehe „Löschkonzept“; Art. 24, 25, 32 DSGVO
4.4.3	Kommt als Alternative zum Löschen das Anonymisieren von Daten zum Einsatz? Wenn ja, wurde die Wirksamkeit des Anonymisierens überprüft?	Siehe „Löschkonzept“; Art. 24, 25, 32 DSGVO
4.5	Welche Form des Zugangsschutzes kommt bei dieser Anwendung zum Einsatz? Anbindung an einen zentralen Verzeichnisdienst (Single-Sign-on z.B. über ein Active Directory), Passwortschutz, Zwei-Faktor-Authentifizierung oder Passkey-Technologie?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.6	Wurde auf allen eingesetzten Endgeräten die Festplattenverschlüsselung aktiviert?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO

4.7	Steht der Schule eine redundante Netzanbindungen zur Verfügung?	Siehe „Datensicherheit“; Art. 24, 32 DSGVO
4.8	Wurden die Server der eingesetzten Anwendung einem Lasttest unterzogen mit zufriedenstellenden Ergebnissen?	Siehe „Datensicherheit“; Art. 24, 32 DSGVO
4.9	Wie sieht der Backup-Prozess aus?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.9.1	Befinden sich Backups an verschiedenen Orten?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.9.2	Gibt es Backups über verschiedenen Zeitintervalle?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.9.3	Wird die Wiederherstellung der Daten aus den Backups regelmäßig überprüft? Mit welchem Ergebenis?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.10	Sind alle Datenübertragungen Ende-zu-Ende-verschlüsselt?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.10.1	Kommen im Rahmen dieses Prozesses Datenübertragungen per E-Mail zum Einsatz und ist für die Daten in diesem Prozess das Schutzniveau der Transportverschlüsselung ausreichend?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.11.	Kommt in diesem Prozess die Pseudonymisierung von Daten zum Einsatz? Wenn ja, wie ist sie organisiert? Wo ist das Zuordnungverzeichnis von Pseudonym zu Person gespeichert?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
4.12	Werden die Schutzmaßnahmen aus der Datensicherheit regelmäßig überprüft (auditiert) und das Ergebnis dokumentiert? Wie ist die letzte Überprüfung ausgefallen?	Siehe „Datensicherheit“; Art. 24, 25, 32 DSGVO
5.0	Wird die Aktualität der Datenschutzdokumente regelmäßig evaluiert und werden die Dokumente nach Bedarf aktualisiert? Was sind die Ergebnisse der letzten Evaluation?	Siehe „Datenschutzmanagement“; Art. 32 DSGVO

5.1	Wurde den Schulen für diese Verarbeitungstätigkeit eine Musterblock für ihre Datenschutzinformation zur Verfügung gestellt?	Siehe „Datenschutzinformation“; Art. 12-14 DSGVO
5.1.1	Hat die Schule eine Datenschutzinformation zu dieser Verarbeitungstätigkeiten gegenüber allen Betroffenengruppen bereitgestellt?	Siehe „Datenschutzinformation“; Art. 12-14 DSGVO
5.2	Wurde den Schulen für diese Verarbeitungstätigkeit ein Mustereintrag für ihr Verzeichnis der Verarbeitungstätigkeiten zur Verfügung gestellt?	Siehe „Datenschutzinformation“; Art. 12-14 DSGVO
5.2.1	Hat die Schule die Verabreitungstätigkeit in ihr VVT aufgenommen?	Siehe „Datenschutzinformation“; Art. 12-14 DSGVO
6.0	Kommt es zu Datenübertragungen in Drittstaaten? Wenn ja, wie sind diese nach den Maßgaben der Art. 44 bis 49 DSGVO abgesichert?	Siehe „Drittstaatentransfers“; Art. 44-50 DSGVO
7.1	Enthält die im Prozess eingesetzte Anwendung Funktionen, um Ansprüche auf Auskunft fristgerecht bedienen zu können?	Siehe „Rechte der Betroffenen“; Art. 15 DSGVO
7.2	Enthält die im Prozess eingesetzte Anwendung Funktionen, um Ansprüche auf Löschung fristgerecht bedienen zu können?	Siehe „Rechte der Betroffenen“; Art. 17 DSGVO
7.3	Enthält die im Prozess eingesetzte Anwendung Funktionen, um Ansprüche auf Datenübertragung (Datenexoport) bedienen zu können?	Siehe „Rechte der Betroffenen“; Art. 20 DSGVO
7.4	Trifft die im Prozess eingesetzte Anwendung Entscheidungen mit Rechtsverbindlichkeit, die allein auf automatisierten Prozessen beruhen?	Siehe „Rechte der Betroffenen“; Art. 22 DSGVO
7.5	Nutzt die im Prozess eingesetzte Anwendung Funktionen künstlicher Intelligenz? Wenn ja, welche Prozesse konkret sind das?	Siehe „Rechtmäßigkeit der Datenverarbeitung“, „Kooperationen (Gemeinsame Verantwortung)“; KIVO
7.5.1	Wenn KI zum Einsatz kommt, nutzt die Technologie die von ihr verarbeiteten Daten zur weiteren Verbesserung des KI-Modells? Auf welcher Rechtsgrundlage geschieht das?	Siehe „Rechtmäßigkeit der Datenverarbeitung“, „Kooperationen (Gemeinsame Verantwortung)“; KIVO

7.5	Nutzt die im Prozess eingesetzte Anwendung Funktionen künstlicher Intelligenz? Wenn ja, welche Prozesse konkret sind das?	Siehe „Rechtmäßigkeit der Datenverarbeitung“, „Kooperationen (Gemeinsame Verantwortung)“; KIVO
7.5.1	Wenn KI zum Einsatz kommt, nutzt die Technologie die von ihr verarbeiteten Daten zur weiteren Verbesserung des KI-Modells? Auf welcher Rechtsgrundlage geschieht das?	Siehe „Rechtmäßigkeit der Datenverarbeitung“, „Kooperationen (Gemeinsame Verantwortung)“; KIVO
8.1	Hat die Schule eine oder einen Datenschutzbeauftragte*n, die oder der ausreichend qualifiziert ist und in alle datenschutzrelevanten Prozesse eingebunden ist?	Siehe „Datenschutzmanagement“; Art. 37-39 DSGVO
8.2	Nutzt die Schule eine Datenschutzmanagementanwendung?	Siehe „Datenschutzmanagement“; Art. 5 Abs. 2 DSGVO
9.0	Wurde für diese Verarbeitungstätigkeit eine Schwellwertanalyse durchgeführt und dokumentiert, ob für diese Tätigkeit eine Datenschutzfolgenabschätzung erforderlich ist? Mit welchem Ergebnis?	Siehe „Schwellwertanalyse und Datenschutzfolgenabschätzung“; Art. 35 DSGVO, Working Paper 248 des EDSA
9.1	Wenn eine Datenschutzfolgenabschätzung erforderlich ist, wurde diese durchgeführt und dokumentiert? Mit welchem Ergebnis?	Siehe „Schwellwertanalyse und Datenschutzfolgenabschätzung“; Art. 35 DSGVO

Glossar/Abkürzungsverzeichnis

Abkürzung	Begriff
Abs.	Absatz
Art.	Artikel
BSI	Bundesamt für die Sicherheit in der Informationstechnik
DSFA	Datenschutzfolgenabschätzung (Art. 35. DSGVO)
DSGVO	Datenschutz-Grundverordnung
(die) DSK	Datenschutzkonferenz der deutschen Aufsichtsbehörden
(das) DSK	Datenschutzkonzept
EDSA	Europäischer Datenschutzausschuss (Gremium der EU-Datenschutzaufsichtsbehörden nach Art. 68 DSGVO)
EU	Europäische Union
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifikator
IT	Informationstechnik
IKT	Informations- und Kommunikationstechnik
KI	Künstliche Intelligenz
KIVO	Verordnung über Künstliche Intelligenz
KT	Kommunikationstechnik
LDSG	Landesdatenschutzgesetz(e)
NAS	Network Attached Storage (Kategorie von vergleichsweise einfachen Servern)

OVG	Oberverwaltungsgericht
PGP	Pretty Good Privacy (Verschlüsselungsstandard für E-Mail-Kommunikation)
RDSK	Rahmendatenschutzkonzept
SDM	Standard-Datenschutzmodell der DSK, das auf das IT-Grundschutzkompendium des BSI aufbaut und dieses um zusätzliche Gewährleistungsziele aus dem Datenschutz ergänzt
S/MIME	Secure/ Multipurpose Internet Mail Extensions (Verschlüsselungsstandard für E-Mail-Kommunikation)
SWA	Schwellwertanalyse (Vorstufe zur DSFA nach Art. 35 DSGVO)
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
USA	Vereinigte Staaten von Amerika
VVT	Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)

Autorinnen und Autoren

David Heimburger (PD-Berater der öffentlichen Hand GmbH)

Hinweise

Bei diesem Dokument handelt es sich um einen Leitfaden, dessen Nutzung/ dessen Anwendung auf ein konkretes Vorhaben in der alleinigen Verantwortung der Verwenderin/ des Verwenders liegt, unter Ausschluss jeglicher Gewährleistung der Autorinnen und Autoren, der PD und der am Schul-IT Navigator beteiligten Organisationen. Eine Zusicherung auf Richtigkeit und Vollständigkeit dieser "Handreichung Datenschutz in der Schul-IT" durch die Autorinnen und Autoren, die PD und der am Schul-IT Navigator beteiligten Organisationen, liegt nicht vor.