FAQ
Datenschutz an Schulen

Stichworte

1. Aktenvernichter/Shredder
2. Anlage 1- Fragen zur Nutzung privater IT-Ausstattung
3. Aufbewahrungs- und Löschungsfristen
4. Auftragsdatenverarbeitung
5. Authentifizierung im pädagogischen Netz
6. Cloud Computing
7. Datenschutz
8. Datenschutzbeauftragter
9. Vorgehen zur Benennung des Datenschutzbeauftragten
10. Datenübermittlung von Funktionsträgern der Schule
11. Datenübermittlung an Kirchen
12. Domain
13. Einwilligung
14. Umgang mit Einwilligungserklärungen
15. E-Mail-Konten im Unterricht
16. E-Mail-Verteilerlisten
17. Umgang mit bzw. Nutzung von E-Mails
18. Fördervereine
19. Fotografieren und Videografieren bei Schulveranstaltungen durch Schule, Eltern und andere
20. Haftung des Datenschutzbeauftragten
21. Handy
22. Klassenelternvertreter
23. Netzbrief-Pädagogisches Netz
24. Nicht gemanagte Endgeräte
25. Nutzung von privaten Datenverarbeitungsgeräten
26. Personenbezogene Daten
27. Rahmendienstvereinbarung
28. Schließanlagen
29. Schülermitverantwortung
30. Schulcomputer und private Internetnutzung
31. Schulhomepage
32. Schulintranet
33. Schulnoten
34. Terminfindung und Umfragen, Tools
35. Übermittlung von Noten, Leistungsbeurteilungen usw.
36. Verzeichnis von Verarbeitungstätigkeiten
37. Verzeichnis von Verarbeitungstätigkeiten bei privaten Geräten
38. Veröffentlichung im Internet
39. Verschlüsselung
40. Vertretungspläne

FAQ

Datenschutz an Schulen

1. Aktenvernichter / Shredder

Welche Schutzklasse und Sicherheitsstufe sollte ein Aktenvernichter in der Schule aufweisen?

Der Aktenvernichter sollte mindestens die Schutzklasse 2 und Sicherheitsstufe 4 nach DIN 66399 aufweisen.

2. Fragen zur Anlage 1- Nutzung von privater IT Ausstattung durch Lehrkräfte (Anlage 1 zur VwV Datenschutz an öffentlichen Schulen)

a) Müssen alle im Formular aufgeführten Datenschutzmaßnahmen getroffen werden?

In Ausnahmefällen: Nein!

Maßgebend ist alleine die Summe aller Maßnahmen, um insbesondere einen unbefugten Zugriff auf die Daten zu verhindern.
Die Verneinung einer getroffenen technischen und organisatorischen Maßnahme ist per se noch kein Ablehnungsgrund für die Schulleitung. Sie ist jedoch Anlass für eine besondere Prüfung der Verhinderung des Zugriffs von unbefugten Personen auf die personenbezogenen Daten.
Es kann nämlich im Einzelfall auch vorkommen, dass nicht jede Maßnahme getroffen werden muss: So muss eine allein lebende Lehrkraft selbstverständlich den Raum, in dem sich ihr Computer befindet, nicht abschließen, solange der Computer in einer abgeschlossenen Wohnung steht. Zudem kann diese Maßnahme durch Verschlüsselung und passwortgeschützten Zugang zum Computer ersetzt werden. Sollte also nicht jede der im Formular dargestellten technischen und organisatorischen Maßnahmen getroffen worden sein, muss sich die Schulleitung im Einzelfall damit befassen.

Das Formular dient als Grundlage für eine Genehmigung durch die Schulleitung. Es soll eine Basis bieten, um die Entscheidung zu erleichtern und dafür sorgen, dass alle Maßnahmen bedacht werden. Auf eine konkrete Darstellung der getroffenen Maßnahmen wurde verzichtet, da diese vom Einzelfall abhängen. Beispiele zur Umsetzung sind in der Anlage 1 zur VwV "Datenschutz an öffentlichen Schulen" aufgeführt.

b) Muss ich meinen Computer zur Kontrolle bei der Schulleitung abgeben?

Nein!

Eine solche Kontrolle muss ohnehin die Ausnahme sein und sollte nur im begründeten Einzelfall (z.B. um einen Missbrauch bzw. eine Dienstpflichtverletzung aufzuklären) durchgeführt werden. Das Verhältnis von Schulleitung zu Lehrkraft sollte von Vertrauen geprägt sein.

Die Kontrolle erfolgt grundsätzlich im 4-Augen Prinzip in Gegenwart der betroffenen Lehrkraft. Die Lehrkraft bringt hierzu das Gerät in die Schule. Das Kontrollrecht ergibt sich aus der Rolle der Schulleitung als verantwortliche Stelle nach Art. 24 Abs. 1 i.V. Art. 4 Abs. 7 EU-DSGVO.

Tipp: Das Kultusministerium empfiehlt, sämtliche dienstliche Daten auf einem USB-Stick zu speichern (bitte immer verschlüsselt). Durch die Nutzung eines USB-Sticks muss im Fall einer solchen Kontrolle nur der USB-Stick an die Schule gebracht werden.

Im Übrigen besitzt die Schulleitung keine Befugnis zum Betreten der Privatwohnung einer Lehrkraft um dort ggf. eine Kontrolle durchzuführen.

c) Müssen auch bei papiergebundenen Daten (z.B. Notenbücher oder Schülerakten) Datenschutzmaßnahmen getroffen werden?

Ja!

Werden personenbezogene Daten in Akten, Notenbücher, usw. verarbeitet, dann müssen Maßnahmen getroffen werden, um sicherzustellen, dass Unbefugte auf diese Daten bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung nicht zugreifen können (z.B. verschlossene Schublade, abgeschlossenes Zimmer, verschlossene Tasche).

d) Was geschieht, wenn eine Lehrkraft sich weigert, die Datenschutz-Erklärung zur Anlage 1 zur VwV Datenschutz an öffentlichen Schulen zu unterschreiben?

Dann muss die Schulleitung ihr verbieten, schulische personenbezogene Daten auf ihren Privatgeräten elektronisch zu verarbeiten.
Damit ist die Lehrkraft auf eine Verwaltung von Schülerdaten in Papierform (z.B. per Notenbüchlein) beschränkt, und muss - wie jede Lehrkraft - immer und auf jeden Fall dafür sorgen, dass auf ihr Notenbüchlein und anderen Unterlagen mit schulischen personenbezogenen Daten nicht von Unberechtigten zugegriffen werden kann.

3. Welche Aufbewahrungsfristen (Löschungsfristen) gelten für schulische Unterlagen (siehe auch VwV Datenschutz an öffentlichen Schulen)?

Die Aufbewahrungsfristen gelten für alle an der Schule gespeicherten Daten in

elektronischer (PC, Laptop, Tablet, Speichermedien) oder in gedruckter Form, also unabhängig davon, ob die Daten digital oder analog gespeichert werden.
Für die **Löschung** von personenbezogenen Daten von Schülerinnen und Schülern gelten folgende Fristen:

- Schülerkarteikarten und Schülerlisten in Papierform sowie Abschluss- und Abgangszeugnisse müssen spätestens nach 60 Jahren, nachdem die Betroffenen die Schule verlassen haben, gelöscht werden.
- Schülerakten und sonderpädagogische Gutachten, einschließlich Lern- und Förderplänen, Schulübergangsempfehlungen sind zwei Jahre nach Verlassen der Schule zu vernichten beziehungsweise bei elektronischer Führung zu löschen.
- Klassen- und Kurstagebücher sind nach Ablauf der jeweils folgenden fünf Schuljahre zu löschen.
- Schriftliche Einwilligungserklärungen zur Veröffentlichung von Fotos in einem Druckwerk sind fünf Jahre nachdem das Druckwerk in Umlauf gebracht wurde zu löschen.
- Schriftliche Einwilligungserklärungen zur Veröffentlichung von Fotos auf der Homepage sind fünf Jahre nach der Herausnahme aus der Homepage zu löschen.
- Notenlisten beziehungsweise Listen über Lernnachweise und Klassenarbeiten beziehungsweise Lernnachweise, Entschuldigungen oder Fehlzeitenlisten sind nach dem Ende des jeweils nächsten Schuljahres zu löschen, sofern keine Rechtsmittel eingelegt worden sind.
- Prüfungsunterlagen wie Prüfungsniederschriften und Prüfungsarbeiten müssen fünf Jahre nach Feststellung des Prüfungsergebnisses gelöscht werden.
- Personenbezogene Daten von Schülerinnen und Schülern auf privaten Datenverarbeitungsgeräten der Lehrkräfte nach Nummer 1.13. der VwV Datenschutz an öffentlichen Schulen sind spätestens nach dem Ende des jeweils nächsten Schuljahres auf dem privaten Datenverarbeitungsgerät zu löschen, sofern keine Rechtsbehelfe oder Rechtsmittel zum Beispiel gegen ein Abschlusszeugnis eingelegt worden sind.

Während der Aufbewahrungszeit muss die Schule sicherstellen, dass die personenbezogenen Daten vor unbefugtem Zugriff geschützt sind. Elektronisch gespeicherte Daten können hierfür auf verschlüsselten mobilen Festplatten gespeichert werden. Unterlagen mit personenbezogenen Daten wie Klassen- und Kurstagebücher oder Prüfungsniederschriften sind in abschließbaren Räumlichkeiten bzw. Behältnissen aufzubewahren.

4. Verarbeitung personenbezogener Daten im Auftrag (Auftragsdatenverarbeitung)
Was ist das?

Oftmals erfolgt die Durchführung der Datenverarbeitung an Schulen nicht durch die Schule

selbst. Man spricht dann von einer Auftragsdatenverarbeitung (kurz ADV). ADV im Sinne der Europäischen Datenschutzgrundverordnung (EU-DSGVO) ist jede Verarbeitung (Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen oder Verändern, Auslesen, Abfragen, Verwenden, Offenlegen durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfen, Einschränken, Löschen oder Vernichten) personenbezogener Daten durch einen Dienstleister im Auftrag der verantwortlichen Stelle.

Die Dienstleistung wird hierbei durch einen Dritten, den Auftragsverarbeiter, erbracht. Dies kann z.B. die Nutzung der Dienste eines Rechenzentrums sein (beim Schulträger, in einem anderen Rechenzentrum oder auch bei Cloud-Diensteanbietern). Auch die Nutzung vieler webbasierter Technologien (Zugriff erfolgt über Web-Browser) stellt eine ADV dar.

Übrigens: auch die Durchführung von Wartungsarbeiten oder vergleichbarer Hilfstätigkeiten, also z.B. Hardwarewartung an Servern oder Festplattensystemen, Betreuung des Betriebssystems usw. gilt als Datenverarbeitung im Auftrag, sofern dabei der Auftragsverarbeiter auf personenbezogene Daten zugreifen könnte.

Einige Beispiele für ADV:

- Nutzung von Software, welche webbasiert (über Internet oder Intranet) zur Verfügung gestellt wird (z.B. Lernstandserhebung und Förderprogramme, wenn personenbezogene Schüler- oder Lehrerdaten verarbeitet werden).
- Ablagen von personenbezogenen Daten auf extern gehosteten Servern.
- EDV-Dienstleistungen des Schulträgers oder von durch diesen beauftragten Firmen.
- Wartungsdienstleistungen, bei denen nicht ausgeschlossen werden kann, dass während der Wartung personenbezogene Daten zur Kenntnis gelangen, beispielsweise:
    - Wartung von IT-Systemen
    - Wartung von TK-Anlagen.
- Entsorgung von Akten oder Datenträgern durch externe Unternehmen.
- Kompetenzanalyse Profil AC, ASD BW. Hier handelt es sich vom Kultusministerium vorgegebene Software, für die das Kultusministerium den Vertrag nach Art. 28 EU-DSGVO abgeschlossen hat.

Welche Folgen hat das?

Vorweg: Die datenschutzrechtliche Verantwortung bleibt bei der Schule. D.h. die Schule ist verantwortlich für den Datenschutz, das Treffen von technischen und organisatorischen Datenschutzmaßnahmen und auch die Auskunftserteilung gegenüber Betroffenen. Ferner dafür, dass die Daten zum gegeben Zeitpunkt auch gelöscht werden.

Zwischen Auftraggeber - also der Schule - und dem Auftragsverarbeiter - dem Dienstleister - ist zwingend eine schriftliche Beauftragung abzuschließen.
In diesen Auftrag sind nach Art. 28 Abs. 2 EU-DSGVO mindestens folgende Punkte aufzunehmen:

- Gegenstand und Umfang der Datenverarbeitung
  Es ist darzustellen, welche personenbezogenen Daten auf welche Weise zu welchem

Zweck/mit welchem Ziel verarbeitet werden. Welche Software wird dazu eingesetzt?
- Etwaige Unterauftragsverhältnisse und Bedingungen für die Inanspruchnahme
- Dabei ist zu regeln, ob Unterauftragsverhältnisse gewünscht bzw. zugelassen sind. Empfehlung: Festlegen, dass eine Erteilung eines Unterauftrags nur nach vorheriger Zustimmung der Schule erfolgen darf
- Befugnis der Schule hinsichtlich der Verarbeitung personenbezogener Daten Weisungen zu erteilen
- Die zu treffenden technischen und organisatorischen Maßnahmen
    - Die Maßnahmen sind konkret und detailliert festzulegen
    - Vom Auftragnehmer sollte man sich ein Datenschutz- und Sicherheitskonzept mit den von ihm getroffenen Maßnahmen vorlegen lassen
- Pflicht, den Verantwortlichen nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei zu unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung Rechte der betroffenen Person nachzukommen
- Pflicht, nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löscht oder zurückgibt

Eine vom Kultusministerium erstellte Vorlage für einen solchen Vertrag finden Sie hier.

Darüber hinaus ändert eine ADV nichts an der Pflicht der Schule, ein Verzeichnis der Verarbeitungstätigkeiten zu führen und das per ADV genutzte Verfahren darin zu dokumentieren.

5. Dürfen im pädagogischen Netz sowohl schuleigene als auch private Geräte (BYOD) im gleichen Netz betrieben werden?

Ja!

Es dürfen jedoch grundsätzlich keine personenbezogenen Daten - wie im Netzbrief dargestellt - verarbeitet werden, außer Name und Klassenzugehörigkeit von Schülerinnen und Schülern und die hierfür erforderlichen technischen Daten.
Für alle Benutzer muss zwingend eine persönliche Authentifizierung für den Netzzugang erfolgen. Über ein Berechtigungssystem muss zudem sichergestellt werden, dass ein erfolgreich authentifizierter Benutzer nur Zugriff auf die für ihn autorisierten Daten hat.
Beim drahtlosen Netz-Zugang (WLAN) ist WPA2-Enterprise nach 802.11 i mit personenbezogener Authentifizierung nach 802.1X erforderlich. Die Authentifizierung hat dabei gegen eine zentrale Benutzerdatenquelle zu erfolgen - z.B. über einen RADIUS-Server gegen den Server des pädagogischen Netzes. Der vermittelnde RADIUS-Server hat sich dabei gegenüber den Clients durch ein X.509- Zertifikat auszuweisen bei dem dieser das Zertifikat ohne Fehler überprüfen kann. Die Datenübertragung zwischen Authentifizierungsserver und Client erfolgt über einen verschlüsselten Tunnel - Realisierung z.B. mit Protected EAP (PEAP).

6. Was ist Cloud Computing und was muss bei der Nutzung beachtet werden?

Bei Cloud-Computing werden IT-Infrastrukturen wie z. B. Rechenleistung, Datenspeicher, Netzwerkkapazitäten oder auch komplette Anwendungssoftware, sowie die Verarbeitung von Daten der Kunden mittels dieser Software - von einem Dienstleister dynamisch an den Bedarf angepasst - über ein Netz zur Verfügung gestellt. Dadurch ergeben sich mehr Flexibilität und meist niedrigere Kosten. Für den Nutzer erscheint die zur Verfügung gestellte Infrastruktur fern und undurchsichtig, wie von einer „Wolke" (engl. Cloud) verborgen. Beispiele für Cloud-Computing sind Dropbox, Microsoft Cloud Services (z.B. Office365, Azure), Google Drive, iCloud sowie weitere Web 2.0 Anwendungen.

Bei Cloud Computing liegt grundsätzlich eine Datenverarbeitung im Auftrag vor (siehe hierzu auch FAQ Auftragsdatenverarbeitung).

- Die datenschutzrechtliche Verantwortlichkeit verbleibt bei der Schule.
- Der Auftrag ist schriftlich zu erteilen. Der Inhalt des Vertrages richtet sich nach Art. 28 Abs. 3 EU-DSGVO.

Viele Anbieter von Cloud-Computing erfüllen nicht die datenschutzrechtlichen Anforderungen, weil

- es meist nicht möglich ist, einen Vertrag entsprechend den gesetzlichen Vorgaben abzuschließen.
- sich der Sitz der Dienstleister oft außerhalb des Geltungsbereichs der EU-DSGVO und das dortige Datenschutzniveau nicht dem ein dem EU-Recht vergleichbares Schutzniveau aufweist.

Viele Cloud-Computing-Anbieter kommen aus diesen Gründen für Schulen nicht in Frage.

Eine Liste von alternativen, nutzbaren Dienstleistern finden Sie unter www.it.kultus-bw.de unter der Rubrik „IT Datenschutz und Sicherheit" - „Cloud-basierte Dienste". Dort und in den FAQ zur Verschlüsselung finden Sie auch Hinweise zur Speicherung von verschlüsselten personenbezogenen Daten in Clouds.

Aktuelle Ergänzung:
Einige Dienstleister hatten als rechtliche Grundlage für die Beauftragung die sogenannten Safe Harbor Principles oder das EU-US-Privacy-Shield genannt. Diese wurden zwar von der Europäischen Kommission anerkannt, eine Datenverarbeitung war deshalb zulässig. Vom Europäischen Gerichtshof (EuGH) wurde jedoch beide als nicht ausreichend bewertet und eine Datenverarbeitung auf dieser Grundlage (Urteil vom 6. Oktober 2015 und 16. Juli 2020) als unzulässig bewertet. Es ist zudem davon auszugehen, dass auch die EU Model Clauses, die andere Dienstleister anführen, ähnlich zu bewerten sind. Daher ist von einer Beauftragung von Dienstleistern aufgrund dieser Rechtsgrundlage abzuraten.

Zu beachten ist auch, dass die sog. Standardvertragsklauseln die Behörden des Drittlandes nicht binden können und daher in den Fällen, in denen die Behörden nach dem Recht des Drittlandes befugt sind, in die Rechte der betroffenen Personen einzugreifen, ohne zusätzliche Maßnahmen der Vertragspartner keinen angemessenen Schutz darstellen. In einem solchen Fall muss der Verantwortliche zusätzliche Garantien bieten, die einen Zugriff

durch die US-amerikanischen Geheimdienste effektiv verhindern und so die Rechte der betroffenen Personen schützen; dies wäre etwa in folgenden Fällen denkbar:

- Verschlüsselung, bei der nur der Datenexporteur den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann
- Anonymisierung aller personenbezogenen Daten

Das KM empfiehlt:

- ausschließlich mit Dienstleistern zusammenzuarbeiten, die Ihren Sitz (dies gilt auch für deren Mutterkonzerne) im Geltungsbereich der EU-DSGVO haben, dabei ist auch auf Unterauftragnehmer zu achten.
- sich im Vertrag schriftlich zusichern zu lassen, dass keine Verarbeitung personenbezogener Daten außerhalb der EU erfolgt und auch keine Daten an Stellen außerhalb der EU (auch an staatliche Stellen, Behörden) übermittelt werden.

7. Was bedeutet Datenschutz und wer ist für den Datenschutz an öffentlichen Schulen verantwortlich?

Das Bundesverfassungsgericht hat in seinem "Volkszählungsurteil" von 1983 klargestellt, dass das Recht auf informationelle Selbstbestimmung ein Grundrecht ist. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Alle am Schulleben Beteiligten müssen die Vorgaben des Datenschutzes beachten. Alleine die Schulleitung (also Schulleiterin bzw. Schulleiter) ist für den Datenschutz an der Schule verantwortlich. Zu ihrer Unterstützung muss ein Datenschutzbeauftragter benannt sein (Art. 37 Abs.1 lit. a EU-DSGVO).

8. Muss für die Schule ein Datenschutzbeauftragter benannt sein?

Ja!

Für jede öffentliche Schule muss ein behördlicher Datenschutzbeauftragter (bDSB) benannt werden.
Für mehrere Schulen kann unter Berücksichtigung ihrer Organisationsstruktur und Größe ein gemeinsamer bDSB benannt werden. Der bDSB für eine Schule kann auch eine Person aus der Schulaufsicht sein. Dies gilt insbesondere für kleine Schulen wie z. B. mehrere Grundschulen, die einen gemeinsamen bDSB identifizieren könnten. Der bDSB wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt.

Die Schule veröffentlicht die Kontaktdaten des Datenschutzbeauftragten in der Regel auf der Homepage der Schule und teilt diese Daten zudem der Aufsichtsbehörde, also dem

Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LfDI) und ihrer unmittelbar vorgesetzten Schulaufsichtsbehörde (Schulamt oder Regierungspräsidium) mit.

Zu den Aufgaben des bDSB gehören insbesondere:

- Unterrichtung und Beratung der Schule, insbesondere der Schulleitung und der dort Beschäftigten, hinsichtlich ihrer datenschutzrechtlichen Pflichten,
- Überwachung der Einhaltung der datenschutzrechtlichen Vorschriften sowie der Datenschutz-Strategien des Verantwortlichen oder des Auftragsverarbeiters einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen,
- Beratung - auf Anfrage - im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung,
- Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

Die Schule muss gewährleisten, dass der bDSB ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird. Dies gilt insbesondere für die Einführung neuer Software, mit der personenbezogene Daten verarbeitet werden. Die Schule muss sicherstellen, dass der bDSB bei der Erfüllung seiner Aufgaben keine Weisungen bezüglich der Ausübung der Aufgaben erhält.

Betroffene Personen (also u. a. Schülerinnen und Schüler, Eltern oder Lehrkräfte der Schule) können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß den datenschutzrechtlichen Bestimmungen im Zusammenhang stehenden Fragen zu Rate ziehen.

9. Vorgehen bei der Benennung des Datenschutzbeauftragten

Wie benenne ich einen Datenschutzbeauftragten?
Die Benennung eines behördlichen Datenschutzbeauftragten sollte schriftlich erfolgen und der Örtliche Personalrat muss der Maßnahme zustimmen. Es sollte, wenn möglich, eine datenschutzrechtlich und IT-technisch versierte Person als behördlicher Datenschutzbeauftragten benannt sein. Eine Interessenskollision bei der Bestellung sollte allerdings vermieden werden (kein Mitglied der Schulleitung oder Netzwerkbetreuer sollte zum behördlichen Datenschutzbeauftragten bestellt werden).
Folgende Punkte sind zu beachten:

- Die unter der Rubrik *Formulare* bereit gestellte „Vorlage Benennung DSB“ sollte verwendet werden
- Der zuständige örtliche Personalrat wurde beteiligt und hat schriftlich zugestimmt.

- Meldung der Kontaktdaten an den Landesbeauftragten für Datenschutz und Informationsfreiheit, am einfachsten über https://www.baden-wuerttemberg.datenschutz.de/dsb-online-melden/
- Veröffentlichung der Kontaktdaten in der Regel auf der Schulhomepage (hier genügt die schuleigene Email-Adresse des Datenschutzbeauftragten z.B. datenschutz@xy-schule.de).
- Über das Service Center Schulverwaltung kann auch eine Email-Adresse für den Datenschutzbeauftragten erstellt werden (datenschutz@xy.schule.bwl.de)
  Tel: 0711 / 89246-0

10. Dürfen Daten von Vorsitzenden des Elternbeirats bzw. Schülersprechers an Stellen außerhalb der Schule kommuniziert wer- den?

Ja, allerdings nur mit deren Einwilligung.

Bei den Vorsitzenden des Elternbeirats und den Schülersprechern handelt es sich um sog. Funktionsträger, die ein öffentliches Ehrenamt innehaben. Deren Namen und Funktion dürfen nach außen kommuniziert, also z.B. auf der Homepage der Schule eingestellt werden. Genannt werden dürfen deren Namen und die Funktion, sofern der Betroffene eingewilligt hat. Sollen weitere Daten genannt werden, wie z.B. Kontaktdaten oder Fotos, so darf das auch nur nach vorheriger schriftlicher Einwilligung der Betroffenen erfolgen.

Name und Funktion von Klassensprechern oder Klassenelternvertretern, dürfen aber nicht kommuniziert werden, da diese nicht die Schule nach außen vertreten und nur im Schulinnenverhältnis aktiv sind.

11. Ist eine Datenübermittlung personenbezogener Daten von Schülerinnen und Schülern sowie von deren Erziehungsberechtigten an die katholische oder evangelische Kirche ohne Einwilligung u.U. zulässig?

Ja in den in der Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ genannten Fällen.

Eine Übermittlung personenbezogener Daten der Schülerinnen und Schüler und deren Erziehungsberechtigten an die katholische oder evangelische Kirche ist anlässlich der Kommunion oder Konfirmation sowie zur Erfüllung weiterer Aufgaben dieser Kirchen ohne Einwilligung der Betroffenen zulässig.
Eine Datenübermittlung von personenbezogenen Daten an weitere Religions- oder Weltanschauungsgemeinschaften ist nur mit Einwilligung der Betroffenen zulässig.
Die Schulen haben gemäß der Verwaltungsvorschrift die Übermittlungen zu dokumentieren, so dass darüber Auskunft erteilt werden kann.

12. Was muss die Schule bei einer Domain beachten?

Für den Betrieb einer Homepage wird ein Name im Sinne einer Internet-Adresse benötigt. Dieser darf natürlich nur einmal vergeben sein. Für Adressen in der Domain .de wacht das Deutsche Network Information Center (DENIC, http://denic.de/) über die Eindeutigkeit. Die DENIC ist für eine Adressregistrierung und -vergabe zuständig.
Die Registrierungsbedingungen der DENIC sind in den DENIC-Domainrichtlinien und den DENIC-Domainbedingungen festgehalten. Sie lassen sich im Wesentlichen wie folgt zusammenfassen:
Bei der Zuteilung einer Domain herrscht das Prioritätsprinzip. Die DENIC registriert eine Domain für denjenigen, der dies zuerst beantragt („First come, first served"). Eine Berechtigungsprüfung dahingehend, ob der Anmelder mit der Registrierung oder Nutzung der Domain beispielsweise Kennzeichenrechte Dritter verletzt, findet dabei grundsätzlich nicht statt. Die DENIC behält sich eine Ablehnung des Antrags nur bei offenkundiger Rechtswidrigkeit vor. Die Registrierung von .de-Domains steht auch ausländischen Personen offen. Die DENIC hält eine Datenbank für die von ihr vergebenen .de-Domains auf ihrer Homepage bereit. Für die Durchsetzung von Ansprüchen ist dies hilfreich, weil Namensträger und Kennzeicheninhaber, die sich durch die Registrierung einer Domain in ihren Rechten verletzt sehen, durch eine Abfrage der Datenbanken schnell und einfach ermitteln können, wer Inhaber der jeweiligen Domain und damit passivlegitimiert ist.

13. Welche Anforderungen werden an eine wirksame Einwilligung nach Art. 7 EU-DSGVO gestellt?

Nach Art. 7 EU-DSGVO ist die Verarbeitung personenbezogener Daten nur zulässig, wenn die EU-DSGVO, das LDSG oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat.

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Die Einwilligung ist also schriftlich oder elektronisch einzuholen, eine bloße mündliche Einwilligung reicht nicht aus.
Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen. Die Einwilligung sollte von evtl. anderen Sachverhalten z. B. durch eine andere Schriftart klar unterscheidbar sei. Zudem muss die Einwilligung in jede Verarbeitungsart einzeln erfolgen können. Das bedeutet, dass die betroffene Person die Möglichkeit haben muss, einzeln bspw. in die Veröffentlichung seines Bildes auf der Homepage und davon unabhängig in die Veröffentlichung seines Namens in der örtlichen Tageszeitung durch Ankreuzen des jeweiligen Sachverhaltes einzuwilligen.
Die betroffene Person ist darüber zu informieren, dass sie das Recht hat, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der

aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung allerdings nicht berührt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

Der Landesbeauftragte für den Datenschutz hatte in einem Einzelfall darauf hingewiesen, dass selbst eine Verarbeitung personenbezogener Daten mit ausdrücklicher Zustimmung des Betroffenen nicht ausreicht und noch **keine** wirksame Einwilligung darstellt, wenn folgende Voraussetzungen nicht erfüllt sind: Die Voraussetzungen einer wirksamen Einwilligung sind das Aufklären über den oder die Empfänger der Daten und der Hinweis auf die Möglichkeit, die Einwilligung unter Darlegung der Folgen zu verweigern. Mustervorlagen finden Sie hier unter Formulare und auf dem Lehrerfortbildungsserver.

14. Umgang mit Einwilligungserklärungen

Wo erfolgt die Aufbewahrung der Einwilligungserklärungen?
Einwilligungserklärungen sind stets durch diejenige Stelle aufzubewahren, der gegenüber die Einwilligung erklärt wurde.
Der Grund hierfür liegt in der Nachweispflicht. Denn betroffene Personen werden im Zweifelsfall bei derjenigen Stelle anfragen, die personenbezogene Daten übermittelt hat. Diese Stelle kann die Rechtmäßigkeit der Übermittlung nun dann nachweisen, wenn sie die Einwilligungserklärung besitzt.

So wird die Einwilligungserklärung zur Einwilligung in eine Weitergabe von Kontaktdaten Eltern an Klassenelternvertreter wird von der Schule verwahrt, sofern die Schule die Daten weitergibt.

15. Was ist bei der Einrichtung von E-Mail-Konten im Unterricht zu beachten?

Grundsätzlich gilt die strikte Trennung von privater und unterrichtlicher E-Mail- Nutzung. Der Bildungsauftrag für die Schulen umfasst nicht das Einrichten/ Nutzen von E-Mail-Konten von Schülerinnen und Schülern zum privaten Gebrauch. Werden personenbezogene E-Mail-Konten über den lokalen Mail-Server (z. B. paedML) im Schulnetz oder auf BelWü eingerichtet, kann die Schule im Missbrauchsfall den Zugang löschen.
Da E-Mail-Nutzung Inhalt des schulischen Bildungs- und Erziehungsauftrags ist, ist bei minderjährigen Schülerinnen und Schülern hierfür keine Einwilligung der gesetzlichen Vertreter erforderlich.

16. Was ist bei der Verwendung von E-Mail-Verteilerlisten zu beachten?

Gerade wenn wiederholt Nachrichten oder Newsletter per E-Mail an einen größeren Empfängerkreis gesendet werden sollen (Gruppen-Kommunikation), bietet sich die Nutzung von sogenannten E-Mail-Verteilerlisten an.

Aber Achtung!
Denn aus datenschutzrechtlicher Sicht besteht bei der Nutzung ein Risiko:
Trägt man nämlich den E-Mail-Verteiler als Empfänger (bei Feld „An“ oder „Cc“) ein, können alle Empfänger lesen, wer sonst noch diese Nachricht bekommen hat. Aus datenschutzrechtlicher Sicht werden dabei die im Verteiler hinterlegten E-Mail-Adressen (zusammen mit dem sich aus dem Inhalt der Nachricht ergebenden Sachverhalt) an Dritte übermittelt - und das ist grundsätzlich unzulässig, wenn es sich um E-Mail-Adressen von einzelnen Personen handelt!

Ausweg:
Trägt man den E-Mail-Verteiler im Feld „Bcc“ ein, können die Empfänger nicht erkennen, wer die Nachricht sonst noch erhalten hat, weil dadurch keine anderen E-Mail-Adressen mehr übermittelt werden.

Hinweis:
Selbstverständlich darf im Rahmen der Kommunikation innerhalb einer Schule oder Behörde auch eine Nachricht z.B. an alle Lehrkräfte so gesendet werden, dass jede Lehrkraft erkennen kann, an welche anderen Lehrkräfte diese noch ging, sofern dienstliche E-Mail-Adressen verwendet werden und der Inhalt der Nachricht nicht persönliche Informationen über eine oder zu einer bestimmten Person enthält.

17. Umgang mit bzw. Nutzung von E-Mails

Beim Umgang von E-Mails muss sichergestellt werden, dass diese gegen unbefugten Zugriff und jegliche unzulässige Änderung geschützt sind. Aus datenschutzrechtlicher Sicht ist dafür der Absender verantwortlich, weil er dies sicherstellen kann. Generell sind ausschließlich die dienstlichen E-Mail-Accounts zu verwenden.

Dienstliche Nachrichten müssen generell mit den dienstlichen E-Mail-Accounts versendet werden. Personenbezogene Daten dürfen nur dann per E-Mail versendet werden, wenn Folgendes beachtet wird:

- Absender und Empfänger besitzen ein E-Mailkonto **innerhalb der Verwaltungsnetze** Baden-Württembergs oder bei BelWue. Dann muss für die Übermittlung keine zusätzliche Verschlüsselung getroffen werden, weil es sich dabei um eigene, vom Internet getrennte Netze handelt. Die Verwaltungsnetze Baden-Württemberg bestehen aus dem Landesverwaltungsnetz (LVN) und dem Kommunalen Verwaltungsnetz (KVN). Im LVN befinden sich alle Ministerien, alle RPen, SSÄ, das Landesmedienzentrum, das Landesinstitut für Schulentwicklung, das Landesinstitut für Schulsport, die Landesakademie für Schulkunst, die Landesakademie für Fortbildung, alle Seminare und Fachseminare und zukünftig das Zentrum für Schulqualität und Lehrerbildung (ZSL) und das Institut für Bildungsanalysen Baden-Württemberg (IBBW). Auch die KISS Infrastruktur ist Bestandteil des LVN. Ebenso befinden sich Postfächer bei BelWue in der sicheren Umgebung. Im KVN befinden sich einige - aber nicht alle Kommunen Baden-Württembergs.

Hinweise:

- Beide Seiten der Kommunikation, Absender und Empfänger, verwenden ausschließlich die von BelWü zur Verfügung gestellte Webmail-Oberfläche im Browser.
- Die Einrichtung einer Mail-Weiterleitungen zu anderen Mailadressen (GMX, Web.de, T-Online, GMail, ...) ist unzulässig.
- Da der BelWü-Webmailer keine 2-Faktor-Authentifizierung unterstützt, darf die Anmeldung am BelWü-Webmailer nur in dafür vorgesehen Netzen stattfinden, also konkret in Verwaltungsnetz und Lehrkräftenetz (siehe Netzbrief), sowie das heimische Netz sofern eine Genehmigung für die Nutzung privater DV-Geräte bei der Schulleitung eingeholt wurde. Die Nutzung im pädagogischen Netz ist für diesen Zweck nicht erlaubt.
- Das Mailpasswort beider Kommunikationspartner entspricht den Richtlinien für sichere Passwörter. Außerdem unterscheidet sich das jeweilige Passwort vom Passwort der Lehrkraft im Schulnetz. Eine Verwendung eines identischen Passworts ist nicht erlaubt.
- Der Absender hat die vorigen Punkte vor der ersten Kommunikation mit unverschlüsselten personenbezogenen Daten selbst zu erfüllen, und muss diese vorab mit dem Empfänger abklären. Beide Seiten ändern anschließend diese Einstellungen und Verfahren nicht mehr.

oder

- Die zu versendenden personenbezogenen Daten sind **verschlüsselt**. Für eine Verschlüsselung können Produkte wie VeraCrypt, AxCrypt oder 7-Zip eingesetzt werden, wobei VeraCrypt auf Windows-, Linux- und Mac-Plattformen lauffähig ist. Bei 7-zip ist sogar die Erstellung einer selbstentpackenden Datei möglich, das bedeutet, dass der Empfänger selbst keine Verschlüsselungssoftware installiert haben muss. Der Austausch der Passwörter sollte dann mit einem anderen Medium, bspw. per Telefon erfolgen.

- Alternativ bleibt ein Versand per Briefpost oder per Fax.

- Soweit E-Mails außer den E-Mail-Adressen von Absender und Empfänger keine weiteren personenbezogenen Daten beinhalten, ist ein unverschlüsselter Versand zulässig. Dies umfasst bspw. die Einladung zu oder das Angebot eines Termins oder Gesprächs, die Bitte um Rückruf, das Zusenden von allgemeinen unpersönlichen Broschüren, Faltblättern und dergleichen, ferner allgemeine Hinweise auf Literatur, die Übermittlung von nicht personenbezogenen Testergebnissen und Hinweise auf Fortbildungen.

Nicht erlaubt ist die Verwendung von Mailprogrammen (z. B. Outlook, Thunderbird, Groupwise, Mail, ...), Mail-Apps auf mobilen Endgeräten (z. B. Mail, R2Mail2, K9Mail, ...) sowie anderweitige Webmail-Oberflächen die externe Mailkonten einbinden können (z. B. eGroupware, CAS, Nextcloud-Mail-App, GMail, …)
AUSNAHME:

- die Verwendung eines lokal installierten Mailprogrammes ist zulässig, wenn es entweder auf einem verschlüsselten Datenträger als portable Version installiert ist (z.B. verschlüsselte/r USB Stick oder -Festplatte) oder der Datenträger des Gerätes auf dem das Mailprogramm installiert ist, komplett verschlüsselt ist (z.B. Bitlocker – Windows, LUKS – Linux, MacOS - FileVault).
- Eine Übermittlung von Mails darf sowohl beim Absender wie auch beim Empfänger ausschließlich über die verschlüsselten, netzbasierten Mail-Protokolle SMTPS, POP3S oder IMAPS stattfinden

Bei einem Versand an mehrere Empfänger ist grundsätzlich darauf zu achten, dass die Empfänger nicht die E-Mail-Adressen der anderen Empfänger sehen können. Für solche Fälle ist es wichtig, die Verteilerlisten nicht als Empfänger bei „An“ oder „cc“ einzugeben, sondern stets bei „bcc Blind Carbon Copy" (Blindkopie) einzutragen.

18. Dürfen öffentliche Schulen und ihre Fördervereine zusammenarbeiten, indem sie personenbezogene Daten austauschen?

Die Fördervereine sind auf neue Mitglieder angewiesen und möchten deshalb von den Schulleitungen eine Liste der jährlich neu hinzukommenden Erziehungsberechtigten haben. Dies ist datenschutzrechtlich jedoch nur zulässig, sofern die Erziehungsberechtigten vorher schriftlich hierzu eingewilligt haben. Bei Fördervereinen handelt es sich um Stellen außerhalb des öffentlichen Bereichs. Um eine personenbezogene Datenübermittlung zu vermeiden, kann die öffentliche Schule mit dem Förderverein vereinbaren, dass den Erziehungsberechtigten bei der Aufnahme von Schülerinnen und Schülern in die öffentliche Schule entsprechendes Informationsmaterial und Beitrittserklärungen des Fördervereins ausgehändigt werden.

19. Dürfen bei Schulveranstaltungen Fotos oder Videos durch die Schule oder durch Eltern und andere angefertigt werden?

Im Rahmen von schulischen Veranstaltungen müssen verschiedene Situationen betrachtet werden:

<u>1. Fotografieren/Aufnehmen von auftretenden Schülerinnen und Schülern durch die Schule</u>

Für das Fotografieren oder Aufnehmen eines Videos von Schülerinnen und Schülern durch die Schule bei schulischen Veranstaltungen (Einschulung, Zeugnisübergabe, Schulball, usw.) wird eine Einwilligung benötigt. Bei Veranstaltungen wie Zirkusvorstellungen oder Theaterstücken, bei denen Schülerinnen oder Schüler auftreten, darf dies schon aus urheberrechtlichen Gründen (Recht des ausübenden Künstlers) nicht ohne Einwilligung der Schülerinnen und Schüler bzw. deren Erziehungsberechtigten erfolgen.

Sollen also Aufnahmen durch die Schule gefertigt und/oder sollen diese z. B. zur

Erinnerung weitergegeben oder veröffentlicht werden, so ist hierfür eine Einwilligung der Schülerinnen und Schüler bzw. deren Erziehungsberechtigten erforderlich. Die Zwecke, zu denen die Fotos/Videos angefertigt werden, die möglichen Empfänger und die Speicherdauer sind genau anzugeben, und die Schülerinnen und Schüler sind über ihre Betroffenenrechte (siehe Merkblatt Betroffenenrechte) zu unterrichten. Ist für das Fotografieren/Videografieren ein Fotograf engagiert worden, so muss mit diesem ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen werden (siehe Vorlage auf it.kultus-bw.de).
Bitte beachten Sie: Die Aufnahme von urheberrechtlich geschützten Werken, während sie live vorgetragen, vorgespielt oder vorgeführt werden, ist nur mit Zustimmung des Urhebers möglich. Sollten also urheberrechtlich geschützte Werke aufgeführt, und diese Aufführung aufgenommen werden, so muss die Zustimmung des Berechtigten vorliegen. Bei Theaterstücken kann diese z. B. im Rahmen der ohnehin notwendigen Aufführgenehmigung miteingeholt werden.

2. Fotografieren/Aufnehmen von auftretenden Schülerinnen und Schülern durch Eltern und andere Personen

Häufig bei besonderen Anlässen wie beispielsweise bei Einschulungen, Schulfeiern oder schulischen Theateraufführungen kommt es vor, dass Eltern und andere Personen Bilder von Schülerinnen und Schülern, aber auch von Lehrkräften anfertigen wollen. Personenbezogene Daten dürfen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten von Privatpersonen erhoben/verarbeitet werden. Das trifft auf das Fotografieren auf Schulveranstaltungen zu rein privaten Zwecken zu. Doch dabei werden auch Rechte von anderen Schülerinnen und Schülern und den Lehrkräften berührt. Besonders problematisch ist dabei, dass für die betroffenen Personen oftmals faktisch gar keine Möglichkeit besteht, dem Fotografiertwerden zu entgehen, weil, wie etwa bei Einschulungsfeiern, eine Anwesenheitspflicht besteht.

Wie kann eine Schule nun ihren Beitrag dazu leisten, dass die Rechte der betroffenen Personen gewahrt bleiben?

Das Kultusministerium schlägt zwei Lösungsvarianten vor:

Variante1:
Die Schule verbietet generell jede Fotoaufnahme während der Veranstaltung. Dies kann sie aufgrund des Hausrechts, über das die Schule verfügt, tun. In der Realität dürfte dieses Verbot jedoch meist auf wenig Zustimmung derjenigen, die gerne fotografieren möchten, stoßen.

Variante 2:
Die Schule bittet die Eltern darum, während der Veranstaltung nicht zu fotografieren und bietet gleichzeitig an, am Ende der Veranstaltung an einem bestimmten Ort der Schule Fotos anfertigen zu können. Auf diese Weise ist möglich, dass Schülerinnen oder Schüler und andere Personen, die es nicht wollen, auch nicht fotografiert werden, indem sie diesem Ort fernbleiben.

Im Übrigen ist es auch Privatpersonen untersagt, urheberrechtlich geschützte Werke ohne Einwilligung des Berechtigten/Urhebers aufzunehmen, während sie live vorgetragen, vorgespielt oder vorgeführt werden, sofern keine Zustimmung des Rechteinhabers hierfür vorliegt.
Zu Beginn der Veranstaltung, an denen urheberrechtlich geschützte Werke aufgeführt werden sollen, sollte das Publikum darüber informiert werden, dass das Fotografieren/Filmen nicht erlaubt ist.

3. Fotografieren /Videografieren des Publikums bei Veranstaltungen durch die Schule
Eine Anfertigung und Veröffentlichung von Veranstaltungsfotos und –videos des Publikums aufgrund „berechtigter Interessen“ (Art. 6 Abs. 1 Satz 1 lit. f DSGVO) ist möglich, da das Fotografieren der Veranstaltung zwar nicht zur Aufgabenerfüllung der Schule erforderlich ist, die Schule aber durchaus ein berechtigtes Interesse daran hat, die Öffentlichkeit über die Veranstaltung zu informieren. Dies wird bei Schulfesten, Sportveranstaltungen usw. regelmäßig der Fall sein.
Die Schule benötigt jedoch „Fotohinweise“, um ihren Informationspflichten nach Art. 13 und 14 EU-DSGVO zu genügen.

Es ist also genau über die Zwecke, für die die Fotos/Videos verarbeitet werden, die Speicherdauer, sowie über die Rechtsgrundlage zu informieren. Auch ist darüber zu informieren, ob die Fotos ggf. an Dritte weitergegeben werden. Ferner ist über das Recht auf Auskunft bzw. Berichtigung und Löschung, auf das Widerspruchsrecht gegen die Verarbeitung sowie über das Bestehen eines Beschwerderechts bei einer Datenschutzaufsichtsbehörde (dem LfDI) zu informieren.

Erfolgt die Verarbeitung auf Grundlage des Art. 6 Abs. 1 lit f) DS-GVO, so ist im Rahmen der Informationspflichten auch auf das berechtigte Interesse des Verantwortlichen hinzuweisen.

Die Information könnte etwa durch einen Aufdruck auf der Einladung oder durch gut erkennbaren Aushang an den Eingängen zu der Veranstaltung erfolgen, der die erforderlichen Angaben enthält und insbesondere darüber informiert, an wen man sich wenden kann, wenn man nicht abgelichtet werden möchte und dazu von seinem Widerspruchsrecht Gebrauch macht.

Diese Informationspflichten können auch „gestuft“ erfüllt werden: So können in einem ersten Schritt zunächst ausgewählte „Basisinformationen“ aufgeführt werden (z.B. Name und Kontaktdaten des Verantwortlichen, Zwecke, für die die Bilder verwendet werden, Rechtsgrundlage der Verarbeitung, Speicherdauer, Bestehen von Betroffenenrechten und sein Widerspruchsrecht), während weitergehende Informationen in einem nachgelagerten Schritt etwa über eine Webseite oder detailliertere Informationsblätter gegeben werden.

Das Kultusministerium hat hierfür unter der Rubrik „Formulare“ zwei Aushänge bereitgestellt:

- *Aushang Veranstaltungen Datenschutz Foto-Videoaufnahmen*

- *Aushang Betroffenenrechte*

Diese sollten gut erkennbar, beispielweise im Eingangsbereich oder am Empfang, ausgehängt werden.

20. FAQ: Haftet der Datenschutzbeauftragte?

Immer wieder wird die Frage gestellt ob und inwiefern ein Datenschutzbeauftragter (DSB) für sein Handeln und seine Empfehlungen haftet.

Gemäß EU-DSGVO obliegt es alleine der verantwortlichen Stelle, die datenschutzrechtlichen Vorgaben umzusetzen. Damit liegt auch die datenschutzrechtliche Verantwortung und damit auch Haftung nicht beim DSB sondern bei der Leitung der verantwortlichen Stelle.
Haftungsfragen sind in Art. 82 EU-DSGVO geregelt. Demnach kann eine Person, der aufgrund eines datenschutzrechtlichen Verstoßes eine materieller oder immaterieller Schaden entstanden ist, einen Anspruch auf Schadenersatz gegenüber dem Verantwortlichen oder, sofern vorhanden, dem Auftragsverarbeiter geltend machen. Der DSB wird in dieser Norm nicht erwähnt.

Dem DSB kommt in erster Linie eine beratende, unterstützende Rolle zu. Daneben ist es auch Aufgabe des DSB, die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen. Bei seiner Aufgabenerfüllung ist der DSB weisungsfrei, d.h. der DSB darf keine Weisungen erhalten, auf welche Weise er seinen Aufgaben nachzukommen hat. Der DSB ist also zur pflichtgemäßen Durchführung seiner Überwachungs- und Beratungstätigkeit verpflichtet, aber nicht persönlich zur Durchsetzung der datenschutzrechtlichen Pflichten des Verantwortlichen verpflichtet.
Bussgelder sind gemäß Art. 83 Abs.7 EU-DSGVO i.V. § 28 LDSG weder gegenüber öffentlichen Stellen noch gegenüber dem DSB vorgesehen.

Die Frage einer Haftung ist beim DSB gemäß den beamtenrechtliche Vorschriften genauso wie bei jedem anderen Beamten auch, zu beantworten. Das bedeutet, dass wenn ein Beamter während der Ausübung eines öffentlichen Amtes und damit infolge hoheitlicher Tätigkeit eine Pflichtverletzung begangen hat, sich für ihn eine Haftungspflicht für eingetretene Schäden ergeben kann. Im Außenverhältnis gegenüber Dritten haftet grundsätzlich der Dienstherr für eine schuldhafte Pflichtverletzung bei öffentlich-rechtlichem Handeln des Beamten. Ein Regressanspruch besteht nur bei vorsätzlichem oder grob fahrlässigem Handeln.

21. Kann die Lehrkraft im Missbrauchsfall die Herausgabe des Mobilfunktelefons von Schülern verlangen?

Ja!

Eine Lehrkraft kann die Herausgabe eines Handys immer dann verlangen, wenn es schulordnungswidrig verwendet wird. Dies ist z. B. dann der Fall, wenn Schüler beim Anschauen von Gewalt- oder Pornovideos angetroffen werden oder wenn die Schul- und Hausordnung verletzt wird. Da Handys aber Inhalte aus dem Privatleben der Schülerin bzw. des Schülers gespeichert haben können, ist es allerdings nicht zulässig, dass die Lehrkraft selbst die gespeicherten Inhalte abruft. Neben dem Eigentumsgrundrecht können auch die Grundrechte auf informationelle Selbstbestimmung sowie das Post- und Fernmeldegeheimnis berührt sein. Die Schule ist daher verpflichtet, das Handy bei Verdacht von strafbarem Verhalten der Polizei oder bei sonstigen Verstößen den Erziehungsberechtigten zu übergeben mit der Bitte, dem Verdacht nachzugehen. Ermittlungen nach § 90 SchG sind allerdings möglich, da diese nur durch die Schule erfolgen können (z. B. schulordnungswidriger Gebrauch des Handys). **Empfehlenswert** ist das Erstellen einer Nutzungsordnung für Mobilfunktelefone an der öffentlichen Schule.

22. Dürfen Klassenelternvertreter, also Mitglieder des Elternbeirats auf die personenbezogenen Daten von anderen Schülern, nicht der eigenen Kinder, im Rahmen ihrer Aufgabenerfüllung zugreifen?

Nein!

Angelegenheiten einzelner Schüler können die Elternvertretungen nur mit der Zustimmung von deren Eltern behandeln.

23. Darf der Computer (auch Laptop, mobiles Endgerät) einer Lehrkraft, auf dem personenbezogene Daten (z.B. Noten von Schülern) gespeichert sind, in das pädagogische Netz eingebracht werden?

Ja!

Soweit auf dem Computer bereits personenbezogene Daten gespeichert bzw. vorhanden sind, darf dieses Gerät zwar in das pädagogische Netz eingebunden werden, die personenbezogenen Daten müssen dabei in jedem Fall verschlüsselt sein. Eine Verarbeitung (Speichern, Öffnen der verschlüsselten Datei, jegliche Bearbeitung, Verschieben usw.) darf jedoch generell nicht erfolgen.
Personenbezogene Daten dürfen im pädagogischen Netz nämlich grundsätzlich nicht verarbeitet werden.

Warum?
Es ist relativ einfach, beispielsweise durch den Einsatz von Keyloggern, das Passwort für die Verschlüsselung auszuspähen: Im unsicheren pädagogischen Netz könnte eine Keylogger Software auf den Lehrer-Computer aufgebracht werden (dies ist ganz einfach möglich z.B. über den USB Anschluss. Wird nun das Passwort eingegeben dann speichert der Keylogger das Passwort.

Welche Alternativen zur Verarbeitung gibt es?

1) Speichern der personenbezogenen Daten auf einem USB Stick in verschlüsselter Form.
2) Speicherung der personenbezogenen Daten im Lehrernetz. In diesem Fall darf ein Zugriff auf die Daten vom pädagogischen Netz aus nicht ermöglicht werden.
3) Speicherung der personenbezogenen Daten entsprechend der Vorgaben des Netzbriefs zur Unterrichtsumgebung (Stichwort: eigenes Servernetz) oder außerhalb der Schule bei einem Dienstleister (Auftragsdatenverarbeitung!). In beiden Fällen ist die Verwendung einer zwei Faktoren Authentifizierung sowie einer Ende-zu Ende-Verschlüsselung vorgeschrieben.

Hinweis: Kompetenzraster an Schulen

- Die Kompetenzen von Schülerinnen und Schüler können in Moodle vom unterrichtlichen pädagogischen Netz aus erfasst werden, da Moodle die Vorgaben des Netzbriefs erfüllt.
- Die in Moodle gespeicherten Daten dienen als Vorlage / Anlage für den Lernentwicklungsbericht.
- Der Lernentwicklungsbericht / Zeugnis darf nicht im pädagogischen, sondern **nur im separaten Lehrernetz oder auf einem entsprechend geschützten PC zu Hause von der Lehrkraft** erzeugt bzw. weiter verarbeitet werden.

24. Wie ist mit nicht gemanagten Geräten zu verfahren?

Erläuterung zu Nummer 1.13. und zur Anlage 1 der Verwaltungsvorschrift Datenschutz an öffentlichen Schulen

Geräte, die ohne zentrales Gerätemanagement und unkonfiguriert insbesondere vom Schulträger oder der Schule Lehrkräften zur Verfügung gestellt werden, sind wie private Datenverarbeitungsgeräte nach Nummer 1.13. der VwV Datenschutz an öffentlichen Schulen zu behandeln.
Das bedeutet, dass mittels Anlage 1 die Nutzung dieses Gerätes durch die Schulleitung genehmigt werden muss. Nur so kann die Schulleitung Ihrer Aufgabe als datenschutzrechtlich Verantwortlicher nachkommen und bspw. erkennen, ob und welche Datenschutzmaßnahmen auf diesem Gerät getroffen wurden.
Ferner, wie auch in Anlage 1 vermerkt, sind mindestens folgende Aspekte zu berücksichtigen:

- Das Gerät muss mittels Passwort oder vergleichbarer Funktionalität gegen unbefugte Benutzung geschützt werden.
- Firewall und Virenschutz müssen vorhanden und stets aktualisiert sein.
- Sofern personenbezogene Daten auf dem Gerät gespeichert werden, darf dies nur in verschlüsselter Form erfolgen. Dabei ist der Stand der Technik zu berücksichtigen.

- Auf privaten Datenverarbeitungsgeräten dürfen personenbezogene Daten, deren Kenntnis für die Lehrkraft nicht zur Aufgabenerfüllung erforderlich ist, nicht verarbeitet werden. Besonders schutzwürdige Daten (z. B. über Krankheiten oder Erziehungs- und Ordnungsmaßnahmen gegenüber Schülerinnen und Schülern) dürfen darauf nicht gespeichert werden. Näheres siehe Nummer 1.13.3. der VwV Datenschutz an öffentlichen Schulen.
- Auch für die Arbeit auf einem solchen Gerät gilt, dass eine Speicherung personenbezogener Daten in einer Cloud nur zulässig ist, wenn mit dem Cloudanbieter ein Vertrag nach den Vorgaben des Art. 28 DSGVO abgeschlossen wurde. Die Regelungen zu Übermittlung an Drittländer gemäß Kapitel V DSGVO sind zu beachten. Gegebenenfalls sollte der Cloudzugang deaktiviert werden.

25. Wie mache ich es mir einfach bei der Nutzung von privaten Datenverarbeitungsgeräten?

Ist die Verwendung von privateigenen Datenverarbeitungsgeräten (wie PersonalComputer, Laptop, Notebook, usw.) beabsichtigt, dann müssen die Vorgaben in der VwV "Datenschutz an öffentlichen Schulen" (Abschnitt I, Nr. 11) und Anlage zur VwV berücksichtigt werden. Sie müssen umfangreiche technische und organisatorische Datenschutzmaßnahmen treffen, um insbesondere jeden unbefugten Zugriff - beispielsweise auch bei einer Mitnutzung des Gerätes durch Familienangehörige - zu verhindern. Die Nutzung dieser Geräte ist durch die Schulleitung zu genehmigen. Hierzu steht das Formular "Antrag auf Nutzung privater Datenverarbeitungsgeräte für dienstliche Zwecke" auf diesem Portal bereit. Sowohl der Schulleitung als auch dem Landesbeauftragten für den Datenschutz steht ein Kontrollrecht zu.

Doch Sie können es sich einfacher machen!

Indem Sie sämtliche personenbezogenen Daten ausschließlich auf einem **USB- Stick** abspeichern und diesen USB-Stick verschlüsseln, z.B. mittels der Software VeraCrypt, verringern Sie Ihren Aufwand erheblich. Dadurch wird z.B. wirksam ein unbefugter Zugriff auf die Daten verhindert, sie müssen also keine aufwändigen Berechtigungsstrukturen hinterlegen. Ferner können Sie auf diese Weise leicht dem Auskunftsanspruch Ihrer Schulleitung oder des Landesbeauftragten für den Datenschutz nachkommen, da Sie dann nur den USB-Stick - und nicht den ganzen Computer, auf dem sich u.U. auch private Daten befinden - vorweisen müssen. Bitte denken Sie auch an die Sicherungskopie auf einem weiteren USB-Stick.
Bei der Genehmigung durch die Schulleitung sind jedoch alle eingesetzten Geräte genehmigen zu lassen: wenn Sie also zwar alle dienstlichen Daten auf einem USB-Stick speichern, die Verarbeitung dieser Daten aber mittels Ihres privaten Computers durchführen, müssen Sie auch diesen Computer und den USB-Stick genehmigen lassen.

26. Was sind personenbezogene Daten?

Personenbezogene Daten sind nach Art. 4 Abs. 1 EU-DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Zu diesen Daten gehören z. B. Name, Anschrift, Geburtsdatum, Telefonnummer, Fotos, Email-Adresse, Kontonummer, Noten usw.

27. Dürfen beim Einsatz von Lern-, Informations- und Kommunikationsplattformen Verhaltens- und Leistungskontrollen, statistische Auswertungen der Beschäftigten erfolgen?

Nein!

Nach § 6 Absatz 1 der Rahmendienstvereinbarung zum Einsatz von Lern-, Informations- und Kommunikationsplattformen (vom 26.01.2012) findet **keine** Verhaltens- und Leistungskontrolle bzw. -bewertung der Beschäftigten mittels automatisierter Verarbeitung personenbezogener Daten und sonstige statistische Erfassung und Auswertung statt.

28. Welche Stelle trägt die datenschutzrechtliche Verantwortung bei der Ausstattung und dem Betrieb sog. elektronischer Schließsysteme an Schulen?

Schulträger ersetzen zunehmend mechanische durch elektronische Schließanlagen an Schulen (§ 48 SchG). Sofern mit Komponenten einer elektronischen Schließanlage (Schließmedium, Türzylinder, Programmiergerät, Verwaltungssoftware) personenbezogene Daten verarbeitet werden (z.B. Stammdaten, Ereignisprotokolle) stellt sich die Frage der datenschutzrechtlich verantwortlichen Stelle (Art. 4 Abs. 7 EU-DSGVO).
Betreibt der Schulträger im Rahmen des technischen Gebäudemanagements eine elektronische Schließanlage ist er für eine personenbezogene Datenverarbeitung verantwortlich. Sofern der Schulträger die Verwaltung der Schließanlage ganz oder teilweise auf den Schulleiter delegiert, nimmt dieser im Rahmen seiner Aufgaben nach § 41 SchG (Aufsicht über die Schulanlage und das Schulgebäude, Verwaltung und Pflege der der Schule überlassenen Gegenstände) Aufgaben des Schulträgers wahr und ist dabei an dessen Anordnungen gebunden. Da der Schulleiter im Rahmen der Anordnung des Schulträgers handelt, bleibt der Schulträger die datenschutzrechtlich verantwortliche Stelle.
Ausführliche Informationen finden Sie auch auf dem Lehrerfortbildungsserver, http://lehrerfortbildung-bw.de

29. Dürfen Schüler, die im Schülerrat oder der Schülermitverantwortung aktiv sind, auf personenbezogene Daten von anderen Schülern im Rahmen ihrer Aufgabenerfüllung zugreifen?

Nein!

Ein Zugriff auf personenbezogene Daten ist nur nach vorheriger Einwilligung durch die Betroffenen zulässig.

30. Dürfen die Schulcomputer, die an das Internet angeschlossen sind, privat genutzt werden?

Aus datenschutzrechtlicher Sicht ja, aber das Kultusministerium rät davon ab!

Die öffentliche Schule kann selbst entscheiden, ob sie die private Internetnutzung gestattet oder untersagt. Sobald die öffentliche Schule den Lehrkräften bzw. den Schülerinnen und Schülern die private Internetnutzung gestattet, wird sie zum Diensteanbieter nach dem Telemediengesetz (vgl. §§ 2, 11 Abs. 1 Telemediengesetz; §§ 3, 88 Abs. 2 Telekommunikationsgesetz) was zu einer Haftung als Provider führt. Ferner sind die **haushaltsrechtlichen Folgen** zu beachten. In diesem Fall müsste die Schule nämlich für die private Inanspruchnahme dienstlicher IuK-Infrastruktur ein entsprechendes Entgelt erheben. Die öffentliche Schule sollte in einer Nutzungsordnung bzw. Dienstanweisung die datenschutzrelevanten Fragen bei der Internetnutzung (Protokollierung, Auswertung und Löschung der Daten) regeln.

Allerdings ist eine private Internetnutzung der Computer, die nicht für den Unterricht - sondern für Verwaltungszwecke eingesetzt werden (z. B. KISS-Rechner), nicht gestattet.

31. Was ist bei der Veröffentlichung personenbezogener Daten auf der Schulhomepage zu beachten?

Die personenbezogenen Daten von Schülerinnen, Schülern und Lehrkräften dürfen ohne Einwilligung der Betroffenen im Internet **nicht** veröffentlicht werden. Dasselbe gilt für Fotografien, Film und Tonaufnahmen.

Eine Veröffentlichung der dienstlichen Erreichbarkeitsdaten (aber keine Fotos) der Schulleiterin bzw. des Schulleiters und deren Stellvertreterin bzw. deren Stellvertreter ist als dienstlich erforderlich und somit auch ohne deren Einwilligung als zulässig anzusehen. Dies gilt aber nicht für das übrige Personal der Schule (Lehrerkollegium, Hausmeister und Schulsekretärin).

32. Dürfen personenbezogene Daten (Privatanschrift und Telefonnummer) von allen Lehrkräften, ohne deren Einwilligung, von der Schulleitung in das Schulintranet eingestellt werden?

Nein!

Zu den Aufgaben des Schulleiters gehört u. a. die Anordnung von Vertretungen. Deshalb muss er die persönlichen Daten der Lehrkräfte kennen. Nach dem Grundsatz der Zweckbindung und Datensparsamkeit ist es jedoch nicht gestattet und auch nicht erforderlich, dass z. B. für Vertretungsfälle alle Lehrkräfte im Intranet die privaten Anschriften und Telefonnummern der Kolleginnen und Kollegen einsehen können. Die von der Schulleitung erhobenen Privatdaten der Lehrkräfte dürfen nur dann in das Schulintranet eingestellt werden, wenn sie in diese Verarbeitungsform schriftlich eingewilligt haben.

33. Dürfen einzelne Schulnoten vor der gesamten Klasse bekannt gegeben werden?

Nein!

Grundsätzlich ist dies nicht zulässig. Die Bekanntgabe der Noten kann ebenso unter vier Augen stattfinden; zur Orientierung der Schülerinnen und Schüler genügt ein Notenspiegel (zahlenmäßiger Überblick über die Notenverteilung ohne Namensnennung). Aus pädagogischen Gründen sind Ausnahmen nur in Einzelfällen denkbar, z.B. bei einer besonderen Verbesserung eines Schülers im Sinne einer Vorbildwirkung.

34. Terminfindung und Umfragen, Tools

Wie lässt sich schnell und einfach ein gemeinsamer Termin aus einer Auswahl finden, ohne doodle zu nutzen?
Sie als Schulleitung können mit Ihrer *@*.schule.bwl.de oder *@*.bw.schule.de unter folgendem Link Umfragen zur Terminfindung erstellen:
https://oft.kultus-bw.de/Termin
Teilnehmen können auch Personen ohne entsprechende Email-Adresse.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) hat auf seiner Homepage zudem eine quelloffenes und lizenzfreies Produkt empfohlen.

35. Wie können Noten, Leistungsbeurteilungen übermittelt werden?

Für die Übermittlung von Noten oder Leistungsbeurteilungen an Schüler sind mehrere Vorgehensweisen denkbar:

1. Versand per Post in verschlossenem Umschlag

2. Mitteilung von Noten oder Bewertungen in Moodle
Durch technische und organisatorische Maßnahmen muss dabei sichergestellt sein, dass die Schülerbewertungen Unbefugten nicht zugänglich werden.

- Die Verschlüsselung ist durch den Zugriff per https für jedes bei BelWue gehostete Moodle gewährleistet
- Eine sichere Authentifizierung muss auf entsprechend hohem Niveau (Passwortlänge und Komplexität) gewährleistet sein, bei Lehrkräften ist zwingend eine 2-Faktoren-Authentifizierung erforderlich.
- In Moodle müssen hierfür entsprechende Module gewählt werden, die nur der bewertenden Lehrkraft und dem jeweiligen SuS alleine den Zugriff gewähren. (Grundsätzlich sollten Fachlehrer untereinander nicht die Noten des Kollegen sehen können. D.h. in dem Kurs, in dem die Noten bekannt gegeben werden, sollte nur die Lehrkraft als Trainer eingetragen sein. Ggf. kann eine Erforderlichkeit bestehen, dass die Klassenlehrkraft die Noten sehen kann.)

3. Versand per eMail
Die Noten oder Beurteilungen müssen dabei verschlüsselt sein indem entweder diese in einen Anhang gepackt werden, der dann verschlüsselt wird oder der Inhalt der Mail selbst verschlüsselt wird. Das verwendete Passwort darf nur dem Absender und dem Empfänger bekannt sei.

36. Muss die Schule ein Verzeichnis von Verarbeitungstätigkeiten führen?

Ja!

Jede Schule führt ein schriftliches oder elektronisches Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dies gilt auch für den Fall, dass die Schule eine Datenverarbeitung durch eine andere Person, Behörde, Einrichtung oder Stelle durchführen lässt (Auftragsdatenverarbeitung).

Die Verantwortung, für das Führen des Verzeichnisses von Verarbeitungstätigkeiten liegt bei der Schulleitung, die selbstverständlich diese Aufgaben delegieren kann. Im Vergleich zum Landesdatenschutzgesetz in seiner alten Fassung geht es nicht nur um automatisierte Verfahren, sondern um jede Verarbeitung, die ganz oder teilweise automatisiert erfolgt oder die personenbezogene Daten in Dateisystemen speichert. Unter Dateisystem sind dabei

auch papiergebundene Akten zu verstehen, sofern diese nach bestimmten Kriterien geordnet sind.
Das Verzeichnis für jede Verarbeitungstätigkeit einzeln enthält sämtliche der folgenden Angaben:

1. Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
2. Zweck der Verarbeitung,
3. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
4. Kategorien von Empfängern (auch andere Lehrkräfte der eigenen Schule), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen,
5. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 EU-DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien,
6. die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
7. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 EU DSGVO, diese Maßnahmen schließen u. a. Folgendes ein:
   - o Pseudonymisierung und Verschlüsselung personenbezogener Daten,
   - o Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen,
   - o Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
   - o Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
8. Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Art 5. EU-DSGVO (Aus Gründen der gesetzlich vorgeschriebenen Rechenschaftspflicht wird empfohlen, in dem Verzeichnis auch die Umsetzung der datenschutzrechtlichen Grundprinzipien zu dokumentieren):
   - 8.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz,
   - 8.2 Zweckbindung (Siehe Verzeichnis der Verarbeitungstätigkeit Nr. 2 „Zwecke der Verarbeitung“),
   - 8.3 Datenminimierung,
   - 8.4 Richtigkeit,
   - 8.5 Speicherbegrenzung (Siehe Verzeichnis der Verarbeitungstätigkeit Nr. 6 „Löschfristen“),
   - 8.6 Integrität und Vertraulichkeit (Siehe Verzeichnis der Verarbeitungstätigkeit Nr. 7, „Beschreibung der techn.-org. Maßnahmen“).

Die Angaben sind so konkret und detailliert zu machen, dass eine kundige Person in der Lage ist, diese nachzuvollziehen.
Das Kultusministerium hat auf der webbasierten Plattform vvbw.kultus-bw.de viele Muster bereitgestellt (u. a. für Schulverwaltungssoftware, Stundenplansoftware, Kompetenzanalyse usw.). Daneben sind umfangreiche Hinweise und Tipps für das Ausfüllen vorhanden. Es wird empfohlen, dass die Schule dort ihr Verzeichnis führt.

Dieses Verzeichnis ist vor der ersten Verarbeitung personenbezogener Daten zu erstellen. Während das alte Verfahrensverzeichnis in weiten Teilen noch auf Antrag jedermann zugänglich zu machen war, besteht diese Pflicht bei den Verzeichnissen von Verarbeitungstätigkeiten nur noch gegenüber den Aufsichtsbehörden auf Anfrage.

Art. 39 EU-DSGVO beschreibt generell die Aufgabe des bDSB, die Behörde im Bereich des Datenschutzes zu unterstützen und zu beraten. Daneben ist es Aufgabe des bDSB, den Verantwortlichen bei der Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen. Daraus folgt, dass das Erstellen des Verzeichnisses der Verarbeitungstätigkeiten nicht zur den Aufgaben des bDSB gehören kann, sonst würde dieser ja sich selbst überwachen müssen.

Der Input für das Verzeichnis muss also zumindest bei größeren Schulen von den jeweiligen Verfahrensverantwortlichen geleistet werden. Die notwendigen Angaben für das Verzeichnis müssten bei den für die einzelnen Verfahren zuständigen Personen erhoben werden, beispielsweise technische Informationen vom EDV-Administrator bzw. vom Netzwerkbetreuer. Im Regelfall ist an den Schulen zur Erstellung des Verzeichnisses der Verarbeitungstätigkeiten eine Zusammenarbeit zwischen den Verfahrensverantwortlichen und der Beratung durch den bDSB erforderlich.

Neben der datenschutzrechtlichen Dokumentation des automatisierten Verfahrens erfüllt das Verfahrensverzeichnis noch einen weiteren Zweck. Durch die umfassende Dokumentation des jeweiligen Verfahrens ist nämlich der verantwortlichen Stelle eine Eigenkontrolle des Verfahrens möglich. Hierbei kann insbesondere überprüft werden, ob das Verfahren rechtmäßig eingesetzt wird und vor allem ob die getroffenen technischen und organisatorischen Datenschutz-Maßnahmen wirksam und ausreichend sind.

Zusammenfassend kann festgehalten werden, dass die Schulleitung für die Erstellung des Verfahrensverzeichnisses verantwortlich ist, weil sie die Gesamtverantwortung für die Einhaltung des Datenschutzes an der Schule trägt.

37. Verzeichnis Verarbeitungstätigkeiten bei privaten Geräten. Muss auch für Software auf privaten Geräten ein Eintrag für das Verzeichnis von Verarbeitungstätigkeiten erstellt werden?

Sofern durch Lehrkräfte auf privaten Geräten personenbezogene Daten zur Erfüllung schulischer Aufgaben verarbeitet werden, ist ein solcher Eintrag **zwingend erforderlich.**

Eingetragen werden müssen die in Art. 30 Abs. 1 DSGVO dargestellten Informationen. Das Kultusministerium hat hierzu verschiedene Handreichungen erstellt, u. a.
-> „ *Verzeichnis Verarbeitungstätigkeiten: Hinweise allgemein EUDSGVO“* und „*Verzeichnis Verarbeitungstätigkeiten: Hinweise Art. 30 EUDSGVO*“.

Zu beachten sind ferner folgende Aspekte:

- Das private Gerät sowie die eingesetzte Software müssen nach Nr. 1.13. und der Anlage 1 der Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ gegenüber der Schulleitung angezeigt und von dieser genehmigt sein.

- Die eingesetzte Software, meist eine App, muss datenschutzrechtlich geeignet und zulässig sein.

- Auch bei einer Verarbeitung von personenbezogenen Daten zu schulischen Zwecken auf privaten Geräten bleibt die Schule, diese vertreten durch die Schulleiter, datenschutzrechtlich verantwortlich.

38. Veröffentlichung von Fotos, Filmen und anderen digitalen Medien im Internet/Intranet oder in Printmedien. Was ist bei der Veröffentlichung zu beachten?

Die Veröffentlichung von Fotos, Filmen und anderen digitalen Medien im Internet/Intranet oder in Printmedien, auf denen Minderjährige abgebildet sind, ist immer nur mit vorheriger schriftlicher oder elektronischer Einwilligung der Erziehungsberechtigten zulässig. Nach Vollendung des 14. Lebensjahres der Schülerin oder des Schülers muss **zusätzlich** deren/dessen Einwilligung eingeholt werden. Es handelt sich nicht um ein Rechtsgeschäft, weshalb die Einwilligung der Eltern nur bei fehlender Einsichtsfähigkeit des Schülers erforderlich ist. Ab 16 Jahren ist der Schüler üblicherweise einsichtsfähig.
Die Einwilligungserklärung gilt bis zum Ende des Schulbesuchs und kann jederzeit ohne Angaben von Gründen widerrufen werden.
Mustervorlagen finden Sie hier.

Einwilligung nach VwV Datenschutz an Schulen und KunstUrhG § 22

<table>
<tr><th>Alter
SuS</th><th>Veröffentlichung von Fotos, Filmen, sonstigen digitale Medien</th><th>Veröffentlichung von Namen</th></tr>
<tr><td>bis 14 Jahre</td><td colspan="2">nur Einwilligung der Erziehungsberechtigten erforderlich</td></tr>
<tr><td>14 - 16 Jahre</td><td rowspan="2">Einwilligung der Erziehungsberechtigten und der SuS erforderlich
(falls erforderliche Einsichtigkeit vorhanden)</td><td>nur Einwilligung der Erziehungsberechtigten erforderlich</td></tr>
<tr><td>16 -18 Jahre</td><td>SuS üben alle Rechte selbst aus.
(falls erforderliche Einsichtigkeit vorhanden</td></tr>
<tr><td>18 Jahre</td><td colspan="2">SuS üben alle Rechte selbst aus.</td></tr>
</table>

39. Wann und wie müssen Daten verschlüsselt werden?

Mittels Verschlüsselung kann unbefugte Kenntnisnahme, unbefugtes Kopieren oder Verändern von personenbezogenen Daten bei der Speicherung, dem Transport und der Übertragung verhindert werden.

Personenbezogene Daten von Schülerinnen und Schülern oder Lehrkräften, die auf **mobilen Speichergeräten** wie z.B. externen Festplatten, USB Speichermedien, CD-ROMs, usw. abgelegt werden, aber auch auf Laptops, Notebooks, Tablets, Smartphones, PDAs, usw. müssen **immer** verschlüsselt sein. Ein alleiniger passwortgeschützter Gerätezugang reicht nicht aus! Auch für den Fall, dass personenbezogene Daten per **E-Mail** über das Internet übertragen werden sollen, ist eine Verschlüsselung vorgeschrieben. Darüber hinaus ist eine Verschlüsselung aller gespeicherten dienstlicher personenbezogener Daten auf privaten Datenverarbeitungsgeräten vorgeschrieben.

Die Verschlüsselung muss grundsätzlich mindestens gemäß **AES-256** erfolgen. Bis auf weiteres kann auch eine Verschlüsselung nach AES-128 genutzt werden, sofern eine Applikation nur diese Verschlüsselung beinhaltet. Das Kultusministerium empfiehlt die Nutzung der kostenlosen Software **VeraCrypt**. Hinweise und konkrete Empfehlungen auch zu weiterer geprüfter Verschlüsselungssoftware gibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) www.bsi.de. Siehe Technische Richtlinie TR-02102 *"Kryptographische Verfahren: Empfehlungen und Schlüssellängen"* und unter der Rubrik *"Produkte und Tools".*
Sollen verschlüsselte personenbezogene Daten beispielsweise in einer Cloud gespeichert werden, sind die Vorgaben des Art. 28 EU-DSGVO zu beachten, weil eine sog. Auftragsdatenverarbeitung stattfindet. Informationen zum Inhalt des Vertrages sowie Vertragsvorlagen finden Sie unter http://www.it.kultus-bw.de, auf dem Lehrerfortbildungsserver und im Intranet der Kultusverwaltung. Die meisten Anbieter von Cloud Computing oder Online-Ablagesystemen ermöglichen es nicht, die datenschutzrechtlichen Bestimmungen des LDSG einzuhalten. Daher ist dort eine Speicherung von personenbezogenen Daten - auch in verschlüsselter Form - **unzulässig**.

40. Dürfen Vertretungspläne auf der Schulhomepage, im Intranet und/oder im Schulgebäude zugänglich sein?

Die ordnungsgemäße Aufgabenerfüllung der Schule bedingt die am Schulleben beteiligten Schüler, Eltern und Lehrkräfte über Stundenplan-änderungen mittels eines Vertretungsplans zu informieren.
Auch ohne Nennung der zu vertretenden bzw. die Vertretung übernehmenden Lehr-kraft (Namen oder Namenskürzel) kann eine Personenbeziehbarkeit des Vertretungs-plans (welche Lehrkraft wird vertreten) nicht ausgeschlossen werden.

Veröffentlichung im Internet/ Intranet:

Vertretungsplan für...	Was ist sichtbar?	Intranet	Internet
Schülerinnen und Schüler	• nur die Vertretungen der eigenen Klasse • keine personenbezogenen Daten wie Namen oder Kürzel *z.B. 5a - Deutsch - 3. Std. - Vertretung*	Jede *Klasse* hat ihren eigenen Benutzernamen und ihr eigenes Klassenpasswort.	im Internet verbietet sich in Ermangelung der Erforderlichkeit, den Vertretungsplan über den Kreis der am Schulleben Beteiligten zur Aufgabenerfüllung öffentlich zugänglich zu machen.
Schülerinnen und Schüler	• nur die Vertretungen der eigenen Klasse • mit personenbezogenen Daten (z.B. Namenskürzel) *z.B. 5a - Deutsch - 3. Stde - Vertretung: Mü - Raum 212*	Jeder *Schüler* hat seinen eigenen Benutzernamen und sein eigenes Passwort.	
Lehrkräfte	• Alle Vertretungen sind aus dienstlichen Gründen für alle Lehrkräfte sichtbar. • mit personenbezogenen Daten • (z.B. Namenskürzel)	Jede *Lehrkraft* hat ihren eigenen Benutzernamen und ihr eigenes Passwort.	

Öffentlich zugänglich im Schulgebäude:

Im Schulgebäude ist der Aushang oder die digitale Anzeige von Vertretungsplänen auch unter Nennung von Namen oder Namenskürzel der vertretenden Lehrkraft als für die Aufgabenerfüllung der Schule (Organisation des Schulbetriebs) erforderlich und somit als zulässig anzusehen. Allerdings muss beachtet werden, dass es sich um einen schulischen Raum handeln muss, der in der Regel der allgemeinen Öffentlichkeit nicht zugänglich ist. Wo schulfremde Personen häufig verkehren, sollten Bildschirmanzeigen/Papieraushänge von Vertretungsplänen möglichst nicht eingesetzt werden. Ein Schuleingangsbereich dürfte sich dann nicht zum Einsatz von Bildschirmanzeigen/Papieraushängen von Vertretungsplänen eignen, wenn dort Besucher bzw. Nutzer anderer Einrichtungen im Gebäude (z.B. wie Kreismedienzentrum oder Kreisbibliothek) verkehren.
In jedem Fall ist die Nennung des Grundes der Vertretung zu vermeiden und eine Bildschirmanzeige/Papieraushang nach Unterrichtsschluss nicht mehr erforderlich.

41. Dürfen zu unterrichtlichen Zwecken Video- und Tonaufnahmen von Personen auf privaten Geräten von Schülerinnen und Schülern erfolgen?

Nein!

Auch bei der Nutzung von privaten Schülergeräten bleibt die jeweilige Schule die datenschutzrechtlich verantwortliche Stelle und hat somit insbesondere sicherzustellen,

dass technisch-organisatorische Datenschutzmaßnahmen getroffen wer-den.
In der Regel ist jedoch die (technische) Konfiguration eines schülereigenen Gerätes der Lehrkraft nicht bekannt, eine Überprüfung ist zudem kaum möglich. Damit ist unklar, ob und ggf. welche technisch-organisatorischen Datenschutzmaßnahmen getroffen wurden.
Ferner haben Lehrkräfte keine oder nur sehr wenige Möglichkeiten, zu überprüfen, was mit diesen Daten geschieht. So ist es kaum möglich, festzustellen, ob diese Daten gelöscht wurden. Darüber hinaus ist es gerade bei Smartphones sehr einfach, diese Aufnahmen in eine Cloud oder ein soziales Netzwerk hochzuladen.
Aus diesen Gründen ist von einer Nutzung von privaten Geräten der Schülerinnen und Schüler abzuraten. Auch mit einer von den Betroffenen eingeholten Einwilligung ist von der Nutzung von privaten Schülergeräten abzusehen, weil auch in einem solchen Fall die Schule ihre datenschutzrechtliche Verpflichtung, u.a. technisch-organisatorische Datenschutzmaßnahmen zu ergreifen, nicht erfüllen kann.
Es kann allenfalls zugelassen werden, dass die Schülerinnen und Schüler mit dem eigenen Gerät Video- und Tonaufnahmen von sich selbst anfertigen, aber keinesfalls von weiteren Personen.

Die Verwendung von schuleigenen Geräten, auch von an Schüler ausgegebene Tablets oder die Nutzung der Privatgeräte der Lehrkräfte (nach Genehmigung durch die Schulleitung (Siehe Anlage 1 der VwV „Datenschutz an öffentlichen Schulen“) ist jedoch zulässig.

42. Sind Video- und Tonaufnahmen im Schulunterricht zur Leistungsbeurteilung oder Notenbildung oder zur Dokumentation von Fehlverhalten zulässig?

Video- und Tonaufnahmen von Schülern stellen eine Erhebung personenbezogener Daten dar. Diese ist zulässig, wenn hierfür eine Rechtsgrundlage vorliegt oder die betroffene Person eingewilligt hat. Das Verarbeiten personenbezogener Daten ist zudem nur zulässig, wenn die strengen Anforderungen, die die EU-DSGVO an die Datenverarbeitung durch Behörden stellt, durch eine uferlose Einwilligung nicht ausgehebelt werden.

In § 115 Abs. 3 SchG neu wird geregelt, dass z**ur Erfüllung des Erziehungs- und Bildungsauftrages** Bild- und Tonaufnahmen der Schülerinnen und Schüler hergestellt und weiterverarbeitet werden können. Im Rahmen der Leistungsfeststellung gilt dies jedoch nur, wenn die jeweilige Aufzeichnung die zu bewertende Schülerarbeit ist. Damit ist nun die Anfertigung von Bild- und Tonaufnahmen auch ohne Einwilligung zulässig, allerdings gilt dies nur soweit dies zur Erfüllung des schulischen Erziehungs- und Bildungsauftrages erforderlich ist. Soll also beispielsweise im Sportunterricht ein Schüler unterstützt werden, indem dieser bei einer Sportübung gefilmt wird, um danach seinen Bewegungsablauf zu besprechen, wäre dies auch ohne Einwilligung möglich. Gleiches gilt z. B. für die Verbesserung der Redefähigkeiten bei einem mündlichen Vortrag.
Der betroffenen Person steht jedoch ein Widerspruchsrecht nach Art. 21 EU-DSGVO zu, weil keine Pflicht der Schule besteht, solche Aufzeichnungen anzufertigen. Es kann nämlich Gründe geben, die sich aus der besonderen privaten Situation der betroffenen

Person ergeben (z. B. starke Nervosität während einer Aufzeichnung, körperliche Merkmale, die für die betroffene Person peinlich sind, …). Im Falle eines Widerspruchs muss eine solche Aufzeichnung unterbleiben. Es wird empfohlen, einen evtl. kommunizierten Widerspruch grundsätzlich zu beachten und in einem solchen Fall die betroffene Person über mögliche Folgen zu informieren (z. B. weniger effektive Beratungsmöglichkeiten). Die betroffene Person muss auf dieses Recht vor Anfertigung der Aufzeichnung hingewiesen werden, in der Anlage 4 zur Verwaltungsvorschrift „Datenschutz an öffentlichen Schulen“ ist dieses Widerspruchsrecht erläutert.

Sofern eine Leistungsbeurteilung mittels Bild- oder Tonaufzeichnungen vorgesehen ist, muss strikt beachtet werden, dass dies nur dann zulässig ist, wenn die Aufzeichnung selbst (und nicht etwa der Inhalt der Aufzeichnung) die zu bewertende Schülerleistung ist. So darf beispielsweise weder ein Vortrag einer Schülerin oder eines Schülers noch eine Sportübung anhand einer Aufzeichnung bewertet werden. Das Filmprojekt an sich (z.B. Regieführung, Schnitt) darf benotet werden. Nicht jedoch das darauf festgehaltene Verhalten von Schülerinnen und Schülern.
Übrigens: die Einholung einer Einwilligung, um eine Leistungsbeurteilung dennoch durchführen zu können, ist unzulässig.

Die Aufzeichnungen sind unverzüglich nach Aufgabenerledigung, bzw. die zur Leistungsfeststellung erstellten Aufzeichnungen sind spätestens am Ende des darauffolgenden Schuljahres zu löschen.

Nicht erforderlich und damit unzulässig ist auch das Filmen der Klasse - auch das Anfertigen von Tonaufnahmen - um **Fehlverhalten** (insbesondere in Abwesenheit der Lehrkraft) vorzubeugen oder zumindest aufzuklären. Hier scheint schon die Legitimität des Verfahrens zweifelhaft; jedenfalls sind mildere - pädagogische - Mittel ohne weiteres denkbar.

43. Welche Regeln sind zum Einsatz von Videoüberwachung an Schulen zu beachten?

Der Einsatz von optischer und/oder elektronischer Videoüberwachung an Schulen (dies umfasst auch die Videobeobachtung, nicht nur die Videoaufzeichnung) ist ein besonders **schwerwiegender Eingriff** in das Recht auf informationelle Selbstbestimmung. Der Gesetzgeber hat daher (in Art. 35 Abs. 3 lit c EU-DSGVO und § 18 LDSG) sehr restriktive Bedingungen für den Einsatz von Videoüberwachung festgelegt.

Die Überwachung öffentlich zugänglicher Räume muss erforderlich sein um Rechtsgüter (wie Leben, Gesundheit, Freiheit oder Eigentum), Einrichtungen oder Objekte zu schützen. In jedem Einzelfall muss zudem streng geprüft werden, ob es nicht datenschutz-freundlichere Alternativen gibt, die den Einsatz einer Videoüberwachung entbehrlich machen.
Beim Einsatz einer Videoüberwachung dürfen ferner keine Anhaltspunkte dafür bestehen,

dass schutzwürdige Interessen der Betroffenen überwiegen; daher kein Einsatz in Umkleideräumen, Toiletten usw. zur Wahrung der Intimsphäre der Betroffenen. Betroffene können neben Schülerinnen und Schülern auch Lehrkräfte und ggf. Eltern und weitere Personen sein. Zu berücksichtigen ist dabei, dass gerade Schülerinnen und Schüler und Lehrkräfte u. U. überhaupt nicht die Möglichkeit haben, der Videoüberwachung zu entgehen, da sie verpflichtet sind, an der Schule zu sein. Für Schülerinnen und Schüler aufgrund der Schulpflicht, für Lehrkräfte aus arbeits- bzw. beamtenrechtlichen Gründen.

Für öffentliche Schulen gilt daher, dass der Einsatz von Videoüberwachung während des Schulbetriebes auf dem Schulhof sowie allen für den Schulbetrieb genutzten Räumlichkeiten, also allen Unterrichtsräumen, Aufenthaltsbereichen, Fluren, Toiletten, Sporthalle usw. grundsätzlich nicht zulässig ist.

Eventuelle Strafverfolgungsmaßnahmen sind zudem nicht Aufgabe der Schule sondern sollten den dafür zuständigen Behörden, also der Polizei überlassen werden.

Für die öffentlich zugänglichen Bereiche und die Außenhaut des Gebäudes samt Stellflächen für PKW und Fahrräder entscheidet grundsätzlich der **Schulträger**, ob bei Vorliegen der gesetzlichen Voraussetzungen von der Videoüberwachung Gebrauch gemacht werden soll. Der Schulträger ist hierfür datenschutzrechtlich verantwortlich. Der Datenschutzbeauftragte des Schulträgers ist zwingend bei der Einführung einer solchen Videoüberwachung zu beteiligen

44. Dürfen Lehrkräfte Verträge zur Auftragsverarbeitung abschließen?

Nein! Werden im Zuge der dienstlichen Tätigkeit personenbezogene Daten von einem externen (Software-)Anbieter verarbeitet, so handelt es sich regelmäßig um eine Auftragsverarbeitung (siehe hierzu auch FAQ Auftragsdatenverarbeitung). Die Datenverarbeitung ist nur zulässig, wenn zuvor ein entsprechender Auftragsverarbeitungsvertrag nach den Vorgaben des Art. 28 EU-DSGVO abgeschlossen wurde. Zuständig hierfür ist ausschließlich die Schulleitung als für den Datenschutz verantwortliche Stelle im Sinne der DSGVO (Art. 4 Nr. 7 EU-DSGVO). Ein solcher Vertrag, der durch eine Lehrkraft abgeschlossen wurde, ist ungültig. Die Datenübermittlung an den Anbieter ist damit unzulässig und stellt ggf. einen meldepflichtigen Datenschutzverstoß dar.

Manche Softwareanbieter eröffnen Lehrkräften die Möglichkeit einen Auftragsverarbeitungsvertrag direkt abzuschließen oder fordern die jeweiligen Nutzer ohne Prüfung von deren Befugnis sogar aktiv dazu auf. In diesen Fällen darf der Vorgang nicht abgeschlossen werden! Die Lehrkraft muss vielmehr den Vertrag der Schulleitung vorlegen. Die Software darf bis zum Vertragsabschluss nicht genutzt werden.
Hinweis: die Verträge werden oft unterschiedlich benannt: AV-Vertrag, AVV, DPA (data protection agreement), Vertrag zur Auftragsverarbeitung etc.

45. Dürfen Lehrkräfte alleine über den Einsatz von Software für den Unterricht entscheiden?

Aus der Sicht des Datenschutzes: Ja, soweit damit keine personenbezogenen Daten verarbeitet werden. Grundsätzlich steht es Lehrkräften frei, Mittel und Methoden - auch Software - für ihren Unterricht bzw. ihre dienstliche Tätigkeit selbst zu wählen.

Werden durch die Software jedoch personenbezogene Daten verarbeitet, insbesondere online etwa durch Speicherung in einer Cloud, so bedarf dies immer der Genehmigung durch die Schulleitung sowie eines Auftragsverarbeitungsvertrags (siehe hierzu auch FAQ Auftragsdatenverarbeitung). Zusätzlich muss der von der Schule benannte Datenschutzbeauftragte einbezogen werden.

Software, die gar keine personenbezogenen Daten von SuS und Lehrkräften verarbeitet (z. B. Erstellen von Arbeitsblättern) ist hiervon nicht betroffen und kann von Lehrkräften ohne Rücksprache mit der Schulleitung verwendet werden.

Auf die Notwendigkeit der Genehmigung privater Endgeräte durch die Schulleitung (siehe hierzu auch FAQ zu Anlage 1 zur VwV Datenschutz an öffentlichen Schulen sowie Nutzung privater Datenverarbeitungsgeräte) sowie auf die Pflicht zur Verschlüsselung personenbezogener Daten (siehe hierzu auch FAQ Wann und wie müssen Daten verschlüsselt werden?) wird hingewiesen.