

Handreichung zum Datenschutz an den Schulen der Edith-Stein- Schulstiftung -Anlage zum Datenschutzkonzept

1. Vorbemerkung

Der Umgang mit personenbezogenen Daten gehört seit jeher selbstverständlich zum Schulalltag. Von der Schulanmeldung bis zum Abschlusszeugnis gibt es kaum einen Vorgang in der Schule, bei dem es nicht um einzelne Menschen geht. In der sich rasant digitalisierenden Welt sind Daten eine wertvolle Ressource. Aber nicht alle Informationen sind für jeden bestimmt. Das Recht auf informationelle Selbstbestimmung besagt, dass jeder Mensch über das Recht verfügt, über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen und selbst zu entscheiden, wann und wie bestimmte Informationen veröffentlicht werden. Es handelt sich hier um ein verfassungsmäßig verankertes Grundrecht, welches nicht durch individuelle Absprachen der beteiligten Personen abgeändert werden kann (unveräußerliches Recht). Je mehr Funktionen und Einsatzmöglichkeiten die modernen Technologien bieten, desto mehr Daten werden verarbeitet - auch solche, die gesetzlich besonders geschützt sind. Durch die neuen Technologien können aber auch mit relativ wenig Aufwand sehr große Datenmengen „geklaut“ werden. Deshalb ist die Einhaltung gesetzlicher Vorgaben besonders wichtig.

Nahezu alle Akteure in der Schule sind täglich mit Daten konfrontiert und an der Datenverarbeitung beteiligt: Die Stiftungsverwaltung (z.B. Abrechnung der Finanzhilfe und Schulgeld), die Schulleitung (z. B. bei der Meldung von Auslastungszahlen an Schulbehörden), Sekretariate und Gebäudemanagement (z. B. zur Organisation von Räumen), LehrerInnen (z. B. bei der Erhebung von Noten), SchülerInnen (z. B. bei Beobachtungsaufgaben) und Eltern (z. B. bei Krankmeldungen).

Vor diesem Hintergrund ist eine Aufgabe von Schule die Entwicklung und Förderung der Medienkompetenz ihrer SchülerInnen sowie gleichzeitig dafür Sorge zu tragen, dass die Daten aller Beteiligten im Tätigkeitsbereich Schule angemessen geschützt werden. Der Schutz personenbezogener Daten ist ein hochrangiges Rechtsgut und erfordert hohe Sensibilität und Engagement.

Seit dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO) im Gebiet der Europäischen Union. Sie dient der Vereinheitlichung und Erhöhung der Transparenz und regelt unter welchen Bedingungen sogenannte personenbezogenen Daten erhoben und in welcher Weise diese dann genutzt werden dürfen. Die Schulen im Land Sachsen-Anhalt müssen sie anwenden. **Gemäß Art. 140 GG gilt für den kirchlichen Bereich hingegen das Kirchliche Datenschutzgesetz (KDG). Die Kirche hat eine eigene Aufsichtsbehörde. Entsprechend ist für die Edith-Stein-Schulstiftung, als Teil der Kirche, das KDG rechtlich bindend. Das KDG, in Kraft getreten am 24. Mai 2018, basiert auf der DSGVO und steht im Einklang mit dieser.**

Die Schulen der Edith-Stein-Schulstiftung (ESS) verstehen es als ihre Aufgabe die rechtlichen Bestimmungen zum Datenschutz umzusetzen und ihre SchülerInnen, Lehrkräfte und MitarbeiterInnen zum verantwortungsvollen Umgang mit personenbezogenen Daten zu befähigen. Dies erfordert ein engagiertes Zusammenwirken aller Beteiligten: SchulleiterInnen, Lehrkräfte, Schulträger und Datenschutzbeauftragte müssen gemeinsam

dafür sorgen, dass die Schulen für den rechtskonformen Umgang mit personenbezogenen Daten und damit zukunftssicher aufgestellt werden.

Diese Handreichung hat das Ziel, alle Beteiligten dabei zu unterstützen. Sie ist als Hilfestellung gedacht, um den Umgang mit Datenschutzfragen an der Schule zu erleichtern, zum sicheren Umgang mit praxisrelevanten Fragestellungen zu befähigen und die Umsetzung der gesetzlichen Vorgaben zu erleichtern. Sie bildet dabei jedoch lediglich die Grundlagen ab. **Darüber hinaus gilt das Datenschutzkonzept der ESS (DSK ESS) als formelle Richtlinie zum Datenschutz.** Bei weiteren Fragen und/oder Schwierigkeiten im Zusammenhang von Schule und Datenschutz, ist die/der betriebliche Datenschutzbeauftragte der ESS für alle Schulen des Trägers Anlaufstelle.

Ergänzung:

Wenn in Texten von staatlichen Organen wie „DSGVO“, „Schule“ und „SchulleiterIn“ die Rede ist, dann muss dies für uns übersetzt werden in:

- DSGVO = KDG,
- Schule = ESS (als Unternehmen, welches Schule betreibt),
- SchulleiterIn = Stiftungsvorstand.

In diesem Spannungsfeld wurde der vorliegende Text geschrieben und zur besseren Verständlichkeit werden die sonst üblichen allgemeinen Texte und Formulierungen hier „übersetzt“.

2. Allgemeines

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine Rechtsgrundlage für die Verarbeitung vorliegt. Die Datenverarbeitung muss also durch eine Rechtsvorschrift erlaubt oder angeordnet sein oder die betroffene Person muss in die Verarbeitung wirksam eingewilligt hat. Neben dem Vorliegen einer Rechtsgrundlage müssen, im Rahmen der Zulässigkeit einer Datenverarbeitung, stets die Grundsätze eingehalten werden (**siehe auch DSK ESS Nr. 3 – 5**).

3. Welche begrifflichen Grundlagen sind beim Thema Datenschutz relevant?

(1) Personenbezogene Daten

Datenschutz bezieht sich nicht auf alle Daten, sondern vorrangig auf die spezielle Kategorie der personenbezogenen Daten. Darunter fallen alle Angaben, durch die eine Person eindeutig identifiziert oder identifizierbar ist. Identifizierbar ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann. Hierzu gehören beispielsweise Name, Vertragsdaten, Wohnadresse, Telefonnummer, IP-Adresse, Foto- oder Videoaufzeichnungen einer Person.

Darüber hinaus zählen aber auch weitere Informationen, die mittelbar und in Kombination mit anderen Daten einen Rückschluss auf eine Person möglich machen, z. B. Geburtsdatum, physische Merkmale, Klassenzugehörigkeit, Angaben über Familienverhältnisse, Vereinsmitgliedschaften oder Hobbys, zur Kategorie der personenbezogenen Daten.

Im Schulbetrieb gehören insbesondere Beobachtungen, Bewertungen von Leistungen, Berichte sowie Bild- und Videoaufzeichnungen aus Unterricht und Schulalltag zu den personenbezogenen Daten.

(2) Besondere Kategorien personenbezogener Daten

Personenbezogene Daten können aufgrund spezifischer Risiken auch als sensible Daten gelten, beispielsweise dann, wenn es sich um Gesundheitsdaten oder ärztliche Diagnosen handelt. Diese Daten werden als besonders schützenswerte Daten verstanden. Zu den besonderen Kategorien gehören personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Im Tätigkeitsbereich Schule zählen Stammdaten (allgemeine Daten zur Person, z. B. Name, Klasse, Geburtstag, Anschrift, Name der Eltern, Konfession, etc.), Leistungsdaten (Daten, die sich speziell auf erbrachte Leistungen der SchülerInnen beziehen) und Mitarbeiterdaten (Daten, die über MitarbeiterInnen gespeichert und verarbeitet werden, um beispielsweise den Arbeitsvertrag zu erfüllen) zu besonderen Kategorien personenbezogener Daten. Weil Daten von Kindern mit höheren Risiken für deren Rechte und Freiheiten verbunden sind, werden diese generell als besonders schützenswert betrachtet. Alle Akteure in einer Schule tragen daher eine hohe Verantwortung bei der Verarbeitung personenbezogener Daten ihrer SchülerInnen.

(3) Betroffene Personen

Betroffene Personen sind Menschen, deren Daten verarbeitet werden. Dazu zählen unter anderem SchülerInnen, LehrerInnen, weitere MitarbeiterInnen, Eltern sowie Gäste während Veranstaltungen.

(4) Datenverarbeitung

→ **siehe auch DSK ESS Nr. 17**

Datenverarbeitung beginnt dort, wo Informationen erstmals festgehalten bzw. erhoben werden. Verarbeitung meint daher jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung das Löschen oder die Vernichtung. Dabei wird weder zwischen klassisch analogen Daten (z. B. auf Papier) oder digitalen Daten, noch in der Art der Anwendung unterschieden (z. B. ob im Kopiergerät vervielfältigt oder auf den USB-Stick übertragen).

Gründe für die Verarbeitung personenbezogener Daten sind:

- die rechtmäßige Erfüllung des Erziehungs- und Bildungsauftrages der Schulen,
- der Zweck oder die Durchführung schulorganisatorischer Maßnahmen oder
- die Einwilligung mit Nachweispflicht.

(5) Einwilligung

→ **siehe auch DSK ESS Nr. 3 – 5**

Die Verarbeitung von personenbezogenen Daten, welche nicht durch Gesetze oder Verordnungen geregelt ist, erfordert die informierte Einwilligung der betroffenen Person bzw. deren gesetzlichen VertreterInnen. Erst wenn eine betroffene Person über die geplante

Datenverarbeitung informiert ist und dieser zustimmt, dürfen Daten erhoben und verarbeitet werden. Bei Verweigerung einer Einwilligung dürfen der betroffenen Person keinerlei Nachteile entstehen.

Eine solche Einwilligung erfordert bestimmte Inhalte und Angaben, um rechtlich wirksam zu sein. Grundsätzlich muss die Zustimmung als freie, informierte Einwilligung erfolgen, d. h. die betroffenen Personen müssen in transparenter und verständlicher Form darüber informiert werden, in was sie einwilligen. Eine Schriftform der Einwilligung ist zwar nicht unbedingt notwendig, ist aber aufgrund der Nachweispflicht zu empfehlen. Die Information zu einer Einwilligung sollte mindestens folgende Angaben enthalten:

- die für die Datenverarbeitung verantwortliche Person, an welche die Eltern (bzw. SchülerInnen ab dem 16. Lebensjahr*) ihre Zustimmung richten (z. B. die Schulleitung),
- konkrete Angaben über Zweck (z. B. Kurzfilmprojekt), Umfang (z. B. Erhebungszeitraum) und Art (z. B. Foto- und Stimmaufnahme) der erhobenen Daten sowie über den weiteren Weg der Datenverarbeitung (Ort und Dauer der Speicherung, Löschfristen),
- den Hinweis auf Freiwilligkeit zur Datenerhebung sowie das ausdrückliche Recht auf Auskunft, Widerruf und Datenlöschung.

Bei Personen ohne oder mit eingeschränkter Einsichtsfähigkeit ist eine Einwilligung nur dann gültig, wenn diese durch die Träger elterlicher Verantwortung erteilt wurde. Die für die Datenverarbeitung verantwortliche Person ist verpflichtet sich zu vergewissern, dass die Einwilligung tatsächlich von Trägern elterlicher Verantwortung stammen.

**Anmerkung: Bezüglich des Alters gibt es verschiedene und teils widersprüchliche Aussagen. Statt dem 16. Lebensjahr gibt es die Auffassung, dass kein konkretes Alter gilt, sondern die Einsichtsfähigkeit für eine bewusste Entscheidung und die kann durchaus auch schon vor dem 16. Lebensjahr sein. Beispielsweise wird bei Bildern oft die Einsichtsfähigkeit für die Tragweite der Entscheidung ins Feld geführt und weniger das Alter.*

(6) Verantwortlichkeit

Die ESS ist juristisch ein Unternehmen und dort haftet der Vorstand. Der Vorstand delegiert einzelne Teilaufgaben an die SchulleiterInnen, doch als Rechtsperson kann nur der juristische Vertreter verklagt werden (Stiftungsvorstand). Darüber hinaus wird die ordnungsgemäße Anwendung an die Schulleitung und LehrerInnen der jeweiligen Schule delegiert. Sie tragen die Verantwortung für die sachgemäße Berücksichtigung der Datenschutzbestimmungen im Rahmen ihrer Aufgabe. Des Weiteren steht allen Akteuren ein/e betriebliche/r Datenschutzbeauftragte/r als Ansprechperson zur Seite.

4. Welche Grundsätze sind bei der Datenverarbeitung im Schulkontext zu beachten?

(1) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Die Datenverarbeitung muss auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben, in einer für die betroffene Person nachvollziehbaren Weise ausgeführt werden.

Rechtmäßigkeit: Die Verarbeitung der Daten beruht auf einer Rechtsgrundlage oder auf einer Einwilligung der betroffenen Person (z. B. Einwilligungserklärung für Tonaufnahmen im Unterricht).

Verarbeitung nach Treu und Glauben: Die betroffene Person muss umfassend über die Verarbeitung informiert sein (z. B. schriftliche Information über Zweck, Dauer, Speicherfrist der Tonaufnahmen).

Transparenz: Die verantwortliche Stelle muss jederzeit umfassende Informationen an die betroffene Person geben können, welche Daten durch wen und zu welchen Zwecken verarbeitet werden und wurden (z. B. Nachweis über Verwendung der Tonaufnahmen). Hieraus ergibt sich die Notwendigkeit zur Erstellung von aussagefähigen Verzeichnissen.

(2) Zweckbindung

→ **siehe auch DSK ESS Nr. 4**

Das Gebot der Zweckbindung bedeutet, dass die erhobenen Daten tatsächlich nur für den eingangs zugesicherten Zweck verwendet werden (z. B. Videoaufnahmen für Feedback im Sportunterricht). Jegliche davon abweichende, darüberhinausgehende Nutzung oder Weitergabe der Daten ist unzulässig. Sobald eine Aufgabe abgeschlossen ist und der Zweck der Datenerhebung erfüllt wurde, müssen die Daten gelöscht werden, es sei denn eine Rechtsvorschrift erlaubt das weitergehende Vorhalten (z. B. bei Leistungsdokumentationen) oder es liegt eine entsprechende Einwilligung vor (z. B. bei Fotos auf der Schulhomepage).

(3) Datenminimierung

→ **siehe auch DSK ESS Nr. 3 + 6**

Der Grundsatz der Datenvermeidung bzw. Datensparsamkeit zielt darauf ab, so wenig personenbezogene Daten zu erheben wie möglich. Somit ist es unzulässig, alle auffindbaren Daten zu sammeln, um sie etwa für mögliche spätere Nutzungen schnell verfügbar zu haben. In Bezug auf die im obigen Beispiel genannten Videoaufnahmen im Sportunterricht, sollte beispielsweise nicht die komplette Unterrichtsstunde aufgezeichnet und über längere Zeit aufbewahrt werden, wenn sich der Zweck der Aufnahmen ausschließlich auf Feedbackgespräche zu bestimmten Bewegungsabläufen bezieht.

(4) Richtigkeit

Die gespeicherten Daten müssen sachlich richtig und aktuell sein. Darüber hinaus müssen entsprechende Maßnahmen zur unverzüglichen Löschung oder Berichtigung von falschen Daten bereitgehalten werden. Dieser Grundsatz trifft zum Beispiel bei einem Umzug eines Schülers zu. Die alte Adresse muss umgehend gelöscht und durch die neue Adresse ersetzt werden.

(5) Speicherbegrenzung

Die Speicherung von Daten unterliegt einer zeitlichen Begrenzung. Personenbezogene Daten dürfen in einer Form gespeichert werden, die die Identifizierung der betroffenen Person nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Beispielsweise dürfen Fotos, die mit dem Zweck der Präsentation auf der Schulhomepage erstellt wurden, nicht länger gespeichert werden, wenn diese durch andere Fotos mit dem gleichen Zweck auf der Homepage ersetzt werden.

(6) Integrität und Vertraulichkeit

Die Sicherheit der personenbezogenen Daten muss stets gegeben sein. Angemessene Sicherheit ist durch geeignete technische (z. B. Datenverschlüsselung, Pseudonymisierung) und organisatorische Maßnahmen (z. B. abschließbare Aktenschränke) zu gewährleisten – einschließlich Schutz vor unbefugter und rechtswidriger Weitergabe und Verarbeitung (Vertraulichkeit) sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung und Schädigung, wie beispielsweise Bildmanipulation (Integrität).

(7) Rechenschaftspflicht

Die verantwortliche Stelle (z. B. die Stiftungs-/Schulleitung) ist für die Einhaltung des Datenschutzes verantwortlich und muss die Einhaltung datenschutzrechtlicher Vorgaben belegen können. Zu beachten ist dabei, dass die Verarbeitung personenbezogener SchülerInnen- und Elterndaten im Tätigkeitsbereich Schule ein ständiger Prozess ist.

(8) Informations- und Auskunftspflicht

Die ESS/ die Schulen sind verpflichtet, betroffene Personen über die Verarbeitung personenbezogener Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu informieren. Dies gilt insbesondere für

Informationen, die sich speziell an Kinder richten (z. B. in Form einer schriftlichen Einwilligungserklärung).

5. Was bedeutet Auftragsdatenverarbeitung in Schulen?

Unter einer Auftragsverarbeitung versteht man jede Verarbeitung personenbezogener Daten von Dienstleistern im Auftrag der Schule. Die Dienstleistung wird hierbei durch einen Dritten, den Auftragsverarbeiter, erbracht (z. B. Nutzung der Dienste eines Rechenzentrums, Nutzung webbasierter Technologien). Bevor schulfremde Dienstleister personenbezogene Daten einsehen und verarbeiten können, muss die Schule mit dem Anbieter einen Vertrag zur Auftragsdatenverarbeitung abschließen. Die ESS ist für die Schulen kein fremder Dienstleister, da die Schulen ein Teil der ESS sind.

In einem Vertrag zur Auftragsdatenverarbeitung werden unter anderem folgende Dinge geregelt:

- Gegenstand und Umfang der Datenverarbeitung,
- Art, Zweck und Verarbeitungsweise personenbezogener Daten,
- Unterauftragsverhältnisse mit Dritten (Dienstleister des Dienstleisters),
- Technische und organisatorische Maßnahmen der Datenverarbeitung.

Wenn ein solcher Vertrag abgeschlossen wird, bleibt die datenschutzrechtliche Verantwortung weiterhin bei der Stiftung, die gegenüber der betroffenen Person auskunftspflichtig ist. Die Stiftung/ Schule ist dementsprechend auch verantwortlich für das Treffen von technischen und organisatorischen Datenschutzmaßnahmen sowie die Löschung der Daten zum gegebenen Zeitpunkt.

6. Welche Rechte haben Personen, deren Daten im Stiftungs-/Schulkontext verarbeitet werden?

→ siehe auch DSK ESS Nr. 14

(1) Recht auf Auskunft

Der betroffenen Person steht grundsätzlich das Recht auf Auskunft zu. Die betroffene Person kann in angemessenen Abständen Auskunft über die Datenverarbeitung, vor allem über den Zweck, darüber welche Daten verarbeitet werden und über den Empfänger verlangen.

(2) Recht auf Berichtigung

Resultiert eine Datenverarbeitung in unrichtigen personenbezogenen Daten der betroffenen Person, so hat diese ein Recht auf die unverzügliche Berichtigung. Dabei ist jedoch der

Zweck der Verarbeitung zu berücksichtigen, sodass etwa bei Datenverarbeitungen im öffentlichen Interesse eine längere Zeitspanne bis zur Berichtigung angesetzt werden kann.

(3) Recht auf Einschränkung der Verarbeitung

Die betroffene Person hat ein Recht auf die Einschränkung der Verarbeitung ihrer personenbezogenen Daten. Dieses Recht greift, wenn die betroffene Person die Richtigkeit der Daten in Frage stellt, die Verarbeitung unrechtmäßig ist, die Daten zur Geltendmachung von Rechtsansprüchen benötigt werden, nachdem der Zweck der Datenverarbeitung sich erledigt hat oder die betroffene Person Widerspruch eingelegt hat.

(4) Recht auf Widerspruch

Das Widerspruchsrecht beinhaltet zum einen die Möglichkeit, der Verarbeitung eigener Daten zu werblichen Zwecken zu widersprechen. Darüber hinaus kann beim Vorliegen besonderer Gründe auch einer ursprünglich rechtmäßigen Datenverarbeitung zu anderen Zwecken widersprochen werden.

(5) Recht auf Datenlöschung

Die betroffene Person hat das Recht, von der ESS / der Schule zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden. Allerdings greift diese Regelung nur, wenn einer der folgenden Gründe eingreift:

- Das Speichern der Daten ist zur Zweckerreichung der Datenerhebung nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung in die Datenverarbeitung.
- Die Daten wurden unrechtmäßig verarbeitet.
- Die ESS/ die Schule ist aufgrund einer gesetzlichen Pflicht zur Löschung der Daten verpflichtet.

Bei der Datenverarbeitung auf Grundlage von schulrechtlichen Vorschriften greifen die Löschrufen des Schulgesetzes. Diese Fristen dienen der näheren Bestimmung, wie lange die betreffenden personenbezogenen Daten für die gesetzliche Aufgabenerfüllung der ESS/der Schule grundsätzlich erforderlich sind.

7. Was müssen Schulen beachten, um Anforderungen an die Datensicherheit zu erfüllen?

Die ESS / die Schulen haben geeignete technische und organisatorische Maßnahmen zu erbringen, damit die Verarbeitung personenbezogener Daten datenschutzkonform abläuft. Alle Maßnahmen müssen in dem jeweiligen Verzeichnis für Verarbeitungstätigkeiten enthalten sein. Zu den Maßnahmen gehören beispielsweise:

- verschlüsselte Kommunikation (veröffentlicht oder erhebt eine Schule beispielsweise personenbezogene Daten auf ihrer Homepage, z. B. mittels eines Kontaktformulars, muss die Seite mit einer Verschlüsselung abgesichert sein),
- verschlüsselte Datenträger (z. B. durch Passwortschutz),
- Bereitstellung eines Widerrufsformulars (z. B. auf der Schulhomepage),
- Zugriffsregelungen,
- verschließbare Räume/ Aktenschränke,
- Übersetzung der Maßnahmen in konkrete Handlungsanweisungen,
- die Fähigkeit, personenbezogene Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall (z. B. Systemausfall) rasch wiederherzustellen (z. B. mittels regelmäßiger Backups der Datenbestände*),

- klare Zuständigkeiten bei Auskunftersuchen (z. B. Regelung von Verantwortlichkeiten).

Die technischen und organisatorischen Maßnahmen müssen angemessen sein, das heißt sie berücksichtigen den Stand der Technik und das Risiko eines möglichen Schadens für die betroffene Person (z. B. bei Datenverlust). Je nach Schwere und Eintrittswahrscheinlichkeit eines Schadens muss die Datensicherheit auf ein akzeptables Niveau gehoben werden. Beispielsweise kann die Verschlüsselung von Daten im Falle des Verlusts eines Datenträgers das Risiko enorm verringern, dass Unbefugte die gespeicherten Informationen einsehen können.

Im Hinblick auf die Anforderungen zur Datensicherheit ist die regelmäßige Überprüfung der entsprechenden Maßnahmen hinsichtlich ihrer Wirksamkeit erforderlich.

**Dies gilt auch für verschlüsselte USB-Sticks.*

8. Welche Informationen sind für ein Verzeichnis von Verarbeitungstätigkeiten relevant?

→ **siehe auch DSK ESS Nr. 15**

Die ESS (jede Schule) ist dazu verpflichtet, die Verarbeitung personenbezogener Daten so zu organisieren, dass die rechtlichen Grundsätze der Datenverarbeitung eingehalten werden und dies nachgewiesen werden kann. In der Praxis bedeutet das, ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen, in dem die Erfassung, Speicherung und Löschung aller Daten, bezogen auf einzelne Verfahren, beschrieben wird. Ein solches Verfahrensverzeichnis ist hinsichtlich der Erfüllung datenschutzrechtlicher Verpflichtungen essenziell, da es einen Überblick über alle anfallenden Verarbeitungstätigkeiten in seinem Zuständigkeitsbereich beinhaltet. Dadurch können gezielte Maßnahmen abgeleitet werden, die zum Schutz der Daten zu ergreifen sind.

Folgende Informationen muss ein Verzeichnis unter anderem enthalten:

- Name und Kontaktdaten des Verantwortlichen, dessen Vertretung sowie des Datenschutzbeauftragten,
- Zwecke und Rechtsgrundlagen der Verarbeitung,
- erhobene Daten und betroffene Personen,
- interne Empfänger,
- Löschrufen,
- Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherheit.

Generell ist dieses Verzeichnis, für die gesamte schulische IT-Infrastruktur zu erstellen. Bei Projekten oder neuen Unterrichtsszenarien muss überprüft werden, ob eine Ergänzung der Prozessbeschreibungen notwendig ist. Auch bei einer Auftragsdatenverarbeitung ist es die Pflicht der jeweiligen Schule, ein Verzeichnis der Verarbeitungstätigkeiten zu führen und das per Auftragsdatenverarbeitung genutzte Verfahren darin zu dokumentieren.

9. Was für Aufgaben hat ein/e Datenschutzbeauftragte/r im Zusammenhang mit Schulen?

Die ESS hat für die Stiftungszentrale und alle Schulen eine/n Datenschutzbeauftragte/n zu benennen. Der Datenschutzbeauftragte bzw. die Datenschutzbeauftragte hat eine Überwachungsfunktion inne und ist von der Stiftungsleitung und den Schulleitungen für die Umsetzung gesetzlicher Vorgaben hinzuzuziehen. Die Verantwortung des Stiftungsvorstandes für die Beachtung der datenschutzrechtlichen Vorschriften bei der Verarbeitung personenbezogener Daten bleibt durch die Person des Datenschutzbeauftragten unverändert.

Zu den Aufgaben der/des Datenschutzbeauftragten gehören unter anderem:

- die Unterrichtung und Beratung des Stiftungsvorstandes, der Schulleitung und der Lehrkräfte hinsichtlich ihrer Pflichten nach den datenschutzrechtlichen Vorgaben und der schulspezifischen Regelung,
- Überwachung der Einhaltung aller Datenschutzvorschriften einschließlich Überprüfung, Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeitenden,
- Anlaufstelle für Anfragen von Verwaltungskräften, Lehrkräften, SchülerInnen und Eltern in mit der Verarbeitung ihrer personenbezogenen Daten und der Ausübung ihrer Rechte zusammenhängenden Fragen.

10. Wodurch wird der Schutz personenbezogener Daten verletzt?

→ **siehe auch DSK ESS Nr. 7 – 9**

Bei der Verletzung des Schutzes personenbezogener Daten handelt es sich um eine Verletzung der Sicherheit, die unbeabsichtigt oder unrechtmäßig zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung/ Weitergabe von personenbezogenen Daten führt. Als Beispiele für Datenschutzverstöße zählen unter anderem verlorene oder gestohlene Datenträger oder Dokumente, unrichtige Entsorgung von Dokumenten, Hacking, Malware, Phishing oder die unbeabsichtigte Veröffentlichung (z. B. auch bei Löschung durch eine nicht autorisierte Person).

11. Wann ist eine Datenschutzverletzung zu melden?

Bei (vermuteter) Verletzung des Schutzes personenbezogener Daten muss unverzüglich die entsprechende Anlaufstelle für den Datenschutz der Schulen informiert werden. Möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde, ist diese der zuständigen

Aufsichtsbehörde (Diözesandatenschutzbeauftragte/r) zu melden. In diesem Zusammenhang ist zu beachten, dass nicht jede Verletzung des Schutzes personenbezogener Daten dazu führt, dass die betroffene Person auch informiert werden muss. Diese Information ist nur dann erforderlich, wenn die Verletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten für die betroffene Person birgt.

12. Beispiele für Praxisrelevanz von Datenschutzrichtlinien in der Schule

(1) Umgang mit Bildern im Schulalltag

Nutzung von Bildern im Schulalltag: z. B. Portfolioarbeit, Dokumentation von Projekten, Bilder für die Schulhomepage, Facebook-Seiten, Fotos von Veranstaltungen, Klassenbild im Raum, Stammakte

möglicherweise auftretende Probleme:

- Bilder anderer Kinder und weiteren Personen,
- Veröffentlichung der Bilder in sozialen Medien (Abtreten der Bildrechte an soziale Medien),
- z. T. unbewusstes Speichern in einer Cloud (z. B. Google Fotos, iCloud).

Private Bilder bei Veranstaltungen:

- erlaubt für private Erinnerungszwecke, ohne beabsichtigte Veröffentlichung z. B. in sozialen Medien (Anmerkung: Wenn die Eltern ein „privates“ Foto bei einer Veranstaltung machen, dann ist dies kein Problem, sobald sie es aber den Großeltern per WhatsApp schicken, ist dies problematisch, denn die Rechte an dem Bild werden an WhatsApp abgetreten und können in einem ganz anderen Zusammenhang veröffentlicht und genutzt werden*),
- Verantwortung zur Einhaltung der Datenschutzrechte bei privaten Bildern liegt bei Personen, die Bilder erstellen.

Veröffentlichung von Bildern:

- einholen von Einwilligungen im Vorfeld von Bildaufnahmen (Träger elterlicher Verantwortung oder SchülerInnen ab 16 Jahren bzw. mit Einsichtsfähigkeit),
- wenn Person nur Beiwerk in einem Bild, dann keine Einwilligung erforderlich,
- bei professionellen Fotografien oder Aufnahmen, die von der Schule in Auftrag gegeben werden, sind die entsprechenden Rechtsgrundlagen erforderlich,
- Abwägung der Interessen beider Seiten, wobei die Interessen von Kindern besonders geschützt sind.

**Beispiel: Erstklässler mit dem befreundeten Nachbarkind schlecken genüsslich ein Eis. Dieses Bild wird an die Eltern des Nachbarkindes per WhatsApp geschickt und ist zukünftig bei einer Werbekampagne in den USA das Gesicht für leckeres Eis, weil es von WhatsApp an das Werbebüro verkauft wurde.*

(2) Aufbewahrungsfristen

Daten müssen nach Ablauf der Frist gelöscht werden. Grundsätzlich müssen personenbezogene Daten nach Ablauf des Zwecks gelöscht werden, für den sie erhoben wurden. Ausnahmen hierbei sind durch Gesetze gegeben (z. B. 10 Jahre Aufbewahrungsfrist bei Steuerunterlagen). Es sollte regelmäßig geprüft werden, ob die Daten weiterhin aufbewahrt werden müssen. Dies gilt auch für persönliche Unterlagen.

Beispiele für Fristen im Tätigkeitsbereich Schule:

- Stammbblätter: 10 Jahre nach Beendigung der Schule,
- Protokolle: 5-10 Jahre,
- Klassenarbeiten Sekundarstufe I: 1 Jahr nach Ende des Schuljahres,
- Klassenarbeiten Sekundarstufe II: 2 Jahre nach Ende des Schuljahres,
- Abschlusszeugnisse: 45 Jahre,

- Bewerbung: 6 Monate,
- Rechnung: 10 Jahre.

(3) Veröffentlichung von Daten

Werden personenbezogene Daten im Rahmen der schulischen Öffentlichkeitsarbeit verwendet (z. B. Schulhomepage, öffentliche Schulfeste, Pressearbeit), gelangen diese in die Öffentlichkeit. Diese Form der Datenverarbeitung benötigt eine gesonderte Form der Einwilligung, da die weitere Verbreitung dieser Daten nicht mehr gesteuert werden kann.

- Erforderliche Maßnahme: Informierte Einwilligung einholen mit explizitem Hinweis im Informationsteil, dass Daten im Internet möglicherweise uneingeschränkt verarbeitet werden.

(4) Verarbeitung personenbezogener Daten auf privaten Endgeräten

→ siehe auch DSK ESS Nr. 13

Bei der Verarbeitung personenbezogener Daten von SchülerInnen auf privaten Endgeräten und Datenträgern, muss sichergestellt werden, dass Unbefugte nicht auf diese Daten zugreifen können. Die ESS hat sich bewusst gegen die Verarbeitung von personenbezogenen Daten auf privaten Endgeräten entschieden, da dies nur mit erheblichen Aufwand zu kontrollieren wäre und es dabei fließende Grenzen mit den privaten Daten der Lehrkräfte gegeben hätte. Vor diesem Hintergrund ist die Speicherung von personenbezogenen Daten nur auf verschlüsselten dienstlichen USB-Sticks erlaubt (siehe hierzu die gesonderte Vereinbarung „Nutzungsbedingungen von schuleigenen USB-Sticks der Edith-Stein-Schulstiftung“).

(5) Umgang mit dem Auskunftersuchen einer betroffenen Person

- Weiterleiten der Anfrage an verantwortliche Stelle (z. B. Schulleitung oder Datenschutzbeauftragte/r der Stiftung),
- Überprüfen der Identität der antragstellenden Person,
- Überprüfen der Legitimität des Anspruches,
- Zusammenarbeit mit Fachabteilungen,
- Beantwortung des Auskunftersuchens innerhalb 4 Wochen nach Eingang.

(7) Muster-Vorlage informierte Einwilligungserklärung Grundschule

[Name der Schule]

[Adresse der Schule]

[Datum]

Bitte um Einwilligung zur Verarbeitung und Veröffentlichung von Foto-, Video- und Tonaufnahmen

Sehr geehrte Eltern,

junge Menschen müssen lernen, die Möglichkeiten der digitalen Medien (z. B. Computer, Tablets, Smartphones) zu nutzen. Daher sollen sie bereits an unserer Grundschule mit diesen Geräten üben und lernen.

Die digitalen Medien ermöglichen neue Formen des Lehrens und Lernens, insbesondere mit Video-, Foto- und Tonaufnahmen. Wenn solche Aufnahmen von Ihrem Kind entstehen, handelt es sich um die Verarbeitung personenbezogener Daten.

Entsprechend der gesetzlichen Datenschutzregelungen erfolgt diese Datenverarbeitung nur dann, wenn Sie dieser im Vorfeld zustimmen. Die erhobenen personenbezogenen Daten werden ausschließlich von Lehrkräften, Mitarbeiterinnen und Mitarbeitern genutzt, die an unserer Schule tätig sind und diese Daten für ihre jeweiligen Aufgaben benötigen. Die erhobenen Daten werden nicht zur Bewertung oder Benotung herangezogen. Eine Weitergabe an Dritte ohne Ihre Zustimmung ist ausgeschlossen. Die Foto-, Video- bzw. Tondateien werden von uns gelöscht, sobald der jeweilige Zweck erfüllt ist. Ihre Einwilligung ist freiwillig. Wenn Sie nicht zustimmen oder Ihre Einwilligung widerrufen, entstehen weder Ihnen noch Ihrem Kind Nachteile. Nach Kirchlichen Datenschutzgesetz haben Sie jederzeit gegenüber der ESS/der Schule ein Recht auf Auskunft über die Daten Ihres Kindes, zudem haben Sie ein Recht auf Berichtigung, Löschung, Einschränkung, Widerspruch und Datenübertragung.

Wenden Sie sich hierzu oder bei generellen Fragen zum Datenschutz an die Schulleitung. Unseren Datenschutzbeauftragten erreichen Sie unter (Holger.Jeschke@Bistum-Magdeburg.de, Tel. 0391 59 61-125). Zudem steht Ihnen ein Beschwerderecht bei der uns zuständigen Datenschutzstelle zu, dem Diözesandatenschutzbeauftragten (matthias.ullrich@datenschutzbeauftragter-ost.de, Tel. 039287287181).

Bitte füllen Sie das Formular unten aus und bringen Sie es uns wieder zurück.

Mit freundlichen Grüßen [Schulleiterin / Schulleiter]

Einwilligung “Videoaufzeichnungen”

Betrifft mein Kind:

[Name, Vorname, Geburtsdatum und Klasse der Schülerin / des Schülers]

Erhebung und lernbezogene Nutzung

Hiermit willige ich ein, dass von meinem Kind folgende personenbezogenen Daten erhoben und verarbeitet werden können: (Bitte kreuzen Sie an, wenn Sie zustimmen)

Videoaufnahmen im Sportunterricht, [Zweck]

13. Weiterführende Informationen

Betrieblicher Datenschutzbeauftragter der ESS (einschließlich aller Schulen)

- Holger Jeschke [Stand August 2020]
- Tel.: 0391/5961125
- E-Mail: holger.jeschke@bistum-magdeburg.de
- <https://www.edith-stein-schulstiftung.de/>

Diözesandatenschutzbeauftragter Ostdeutscher Bistümer

- Matthias Ullrich [Stand August 2020]

- Adresse: Badepark 4, 39281 Schönebeck
- Tel.: 03928/7287181
- E-Mail: matthias.ullrich@datenschutzbeauftragter-ost.de
- <https://www.kdsa-ost.de>

Kirchliches Datenschutzgesetz (KDG)

- <https://bit.ly/2OqPTVz> [Stand August 2020]

Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)

- <https://bit.ly/2OQ2OPN> [Stand August 2020]

Datenschutz-Grundverordnung (DSGVO)

- <https://dsgvo-gesetz.de/> [Stand August 2020]

Datenschutzgesetz Sachsen-Anhalt

- https://www.landtag.sachsen-anhalt.de/fileadmin/Downloads/Rechtsgrundlagen/2018_Datenschutzgesetz-DSG-LSA.pdf [Stand August 2020]

Schulgesetz des Landes Sachsen-Anhalt (SchG LSA)

- <https://www.landesrecht.sachsen-anhalt.de/bsst/document/jlr-SchulGST2018rahmen> [Stand August 2020]

Handreichung Datenschutz an Schulen (Ministerium für Bildung des Landes Sachsen-Anhalt)

- <https://bit.ly/2OvKYmk> [Stand August 2020]