DIRECTIONS-Schutzklassenkonzept

- Fassung 0.7 -

Stand 12.06.2024

Weitere DIRECTIONS-Dokumente:

- Zertifizierungsgegenstand
- Kriterienkatalog (https://doi.org/10.5445/IR/1000172025)
- Regelwerk für die Selbstverpflichtungserklärung

Projekt Webseite: www.directions-cert.de

Empfohlene Zitation:
Brecker, Danylak, Helmke, Hornung, Kohpeiß, Link, Lins, Schild, Schindler, Späthe, Sunyaev (2024). DIRECTIONS-Schutzklassenkonzept – Fassung 0.7. Online verfügbar: www.directions-cert.de

Beitrag zum Forschungsprojekt „Data Protection Certification for Educational Information Systems (DIRECTIONS)“, das durch das Bundesministerium für Bildung und Forschung gefördert wird (FKZ 01PP21003).

Das Forschungsprojekt DIRECTIONS basiert auf den Ergebnissen und Dokumenten von AUDITOR (www.auditor-cert.de).

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Autoren (in alphabetischer Reihenfolge)

Kathrin Brecker[b], Philipp Danylak[b], Jan Torben Helmke[a], Gerrit Hornung[a], Marcel Kohpeiß[a], Hendrik Link[a], Sebastian Lins[b], Hans-Hermann Schild[a], Stephan Schindler[a], Eva Späthe[b], Ali Sunyaev[b]

[a] Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

[b] Forschungsgruppe Critical Information Infrastructures (cii) am Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB) des Karlsruher Instituts für Technologie

Inhaltsverzeichnis

DIRECTIONS-Schutzklassenkonzept

Anforderungen an TOM des schulischen Informationssystems werden nach Schutzklassen differenziert. Dabei orientiert sich der DIRECTIONS-Kriterienkatalog an den schon bekannten verschiedenen Schutzklassenkonzepten, die für die Systematisierung von TOM entwickelt worden sind.[1]

1. Struktur und Ziel des Schutzklassenkonzepts

Das Schutzklassenklassenkonzept orientiert sich am Risiko der Datenverarbeitung für die Grundrechte und Grundfreiheiten natürlicher Personen. Daneben hat nach Art. 24, 25 und 32 DSGVO die Auswahl von TOM den Stand der Technik und die Implementierungskosten zu berücksichtigen. In Anlehnung an die EG 75, 76, 85, 90, 91, 94, 95 und 96 DSGVO hat der Verantwortliche jeweils die Risiken einer Verarbeitung personenbezogener Daten für die Rechte und Freiheiten natürlicher Personen vorab zu identifizieren. Auftragsverarbeiter treffen diese Pflichten entweder direkt (z.B. Art. 32 DSGVO) und/oder vermittelt durch die Vereinbarung mit dem Verantwortlichen (Art. 28 Abs. 2 DSGVO). In einem weiteren Schritt ist abzuschätzen, ob die Verarbeitung zu einem materiellen oder immateriellen Schaden, d.h. zu einer Verletzung spezifischer Grundrechte führen könnte, etwa wenn sie zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, einer unbefugten Aufhebung der Pseudonymität oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren (EG 75).

Grundsätzlich bringt die Verarbeitung von Daten das Risiko mit sich, dass die Verarbeitung die autonome Wahrnehmung von Grundrechten unterläuft. Dabei führt die Verarbeitung von personenbezogenen Daten von Kindern zu einem spezifischen Risiko für die Rechte des Kindes (Art. 24 GRCh). Insbesondere darf die Verarbeitung dieser Daten nicht die Pflicht öffentlicher Stellen oder privater Einrichtungen unterlaufen, bei Maßnahmen, die Kinder betreffen, dem Wohl des Kindes stets eine vorrangige Stellung einzuräumen. Im schulischen Kontext kann die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler in der Regel außerdem ein spezifisches Risiko für deren Grundrecht auf Bildung darstellen (Art. 14 GRCh). Dies gilt vor allem dann, wenn die Verarbeitung personenbezogener Daten durch die eingesetzten schulischen Informationssysteme das ohnehin bestehende Abhängigkeitsverhältnis zwischen Lehrkräften und Schülerinnen und Schülern und damit die Gefahr eines Informationsmachtmissbrauchs durch die Lehrkräfte verstärkt. Führt die Verarbeitung der Daten zu Entscheidungen, die den Einstieg in das Berufsleben oder das weitere Fortkommen der betroffenen Personen im Berufsleben unmittelbar bestimmen, so stellt die Verarbeitung auch ein Ri-

[1] S. etwa das Standard-Datenschutzmodell (SDM, derzeit in der Version 3.0 idF des Beschlusses der DSK v. 24.11.2022, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/104DSK_SDM-3-0.html), das auf Basis einer dreistufigen Risikobewertung zu zwei Schutzbedarfsstufen gelangt. Für die Risikobewertung verweist das SDM weiterhin auf *DSK*, Kurzpapier Nr. 18, 2018. In diesem wird eine Risikomatrix vorgeschlagen, die die Schwere möglicher Schäden und ihre Eintrittswahrscheinlichkeit abbildet. Das IT-Grundschutz-Kompendium des BSI (Stand Februar 2023, S. 7) differenziert – für Bedrohungen der IT-Sicherheit – die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“. Eine normative Verankerung findet sich auch in §§ 9 ff. der KDG-DVO (Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz) die Datenschutzklassen I-III festlegt (§§ 11-13 KDG-DVO).

siko für deren Berufsfreiheit dar (Art. 15 GRCh). Kann die Datenverarbeitung zu einer Diskriminierung der betroffenen Personen gemäß der in Art. 21 GRCh genannten Merkmale führen, besteht außerdem ein spezifisches Risiko für dieses Grundrecht. Daneben kann die Datenverarbeitung auch zu spezifischen Risiken des Rechts auf Privatleben der betroffenen Personen führen (Art. 7 GRCh), etwa wenn die Daten nicht im schulischen, sondern in deren familiärem bzw. häuslichem Kontext oder bei der Verwendung von Kommunikationsmedien erhoben werden. Je nach Verwendungskontext und -zweck können auch weitere Risiken für die Meinungsfreiheit bzw. Informationsfreiheit (Art. 11 i.V.m. Art. 24 GRCh) und weitere Grundrechte und Freiheiten entstehen. Die Verarbeitung von personenbezogenen Daten von Schülerinnen und Schülern, Lehrkräften, anderem pädagogischen Personal sowie Erziehungsberechtigten zu kommerziellen Zwecken kann zusätzliche Risiken beinhalten. Eine solche Verarbeitung wird im Schulkontext deshalb ausgeschlossen (s. Kriterium Nr. 11).

Der Verantwortliche und (soweit ihn die Pflichten erfassen) der Auftragsverarbeiter haben gemäß EG 76 Satz 1 DSGVO die Eintrittswahrscheinlichkeit und Schwere des Schadens für die Rechte und Freiheiten der betroffenen Person in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung zu bestimmen. Dieses Risiko sollen sie gemäß dem jeweiligen Verwendungskontext der verarbeiteten personenbezogenen Daten anhand eines objektiven Maßstabs beurteilen. Dabei haben sie nach EG 76 Satz 2 DSGVO festzustellen, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt. Diese Risikoabstufungen werden mit dem DIRECTIONS-Schutzklassenkonzept umgesetzt.

Der Anbieter des schulischen Informationssystems muss angeben, in welche Schutzklasse das schulische Informationssystem fällt. Soweit das Informationssystem aus mehreren selbständigen Verarbeitungsvorgängen besteht, können diese im Rahmen des Schutzklassenkonzeptes eigenständig bewertet werden. Dies gilt nicht, wenn eine sachdienliche Trennung nicht möglich ist oder eine Einzelbetrachtung der einzelnen Verarbeitungsvorgänge nicht ihrer Gesamtwirkung entspricht (z.B. Gesamtheit der Verarbeitungsvorgänge erlaubt Profilbildung, die einzelnen Verarbeitungsvorgänge für sich gesehen nicht; zur Bestimmung der Schutzklasse dürfen nicht nur die einzelnen Verarbeitungsvorgänge betrachtet werden).

Beispiel: Das schulische Informationssystem bietet ein Lernmodul und ein Videokonferenzmodul. Beide Module können unabhängig voneinander genutzt werden. Das Lernmodul und das Videokonferenzmodul (bzw. deren Verarbeitungsvorgänge) können daher ggf. in unterschiedliche Schutzklassen fallen.

Ziel des Schutzklassenkonzepts ist es, den individuellen Maßstab der Datenschutz-Grundverordnung – die Anforderungen an die TOM richten sich nach dem Schutzbedarf der jeweiligen Datenverarbeitung – durch Zuordnung in Schutzklassen zu vereinfachen. Die Schutzklassen haben dabei eine doppelte Funktion: Sie beschreiben zum einen den Schutzbedarf der Datenverarbeitungsvorgänge, zum anderen die Anforderungen an die TOM. Um die unterschiedlichen Funktionen deutlich zu machen, unterscheidet das Schutzklassenkonzept einerseits Schutzbedarfsklassen und andererseits Schutzanforderungsklassen.

Die ***Schutzbedarfsklassen*** definieren den Schutzbedarf für Verarbeitungsvorgänge anhand genereller Merkmale. Dieser ergibt sich aus der Art der Daten, dem Umfang, den Umständen und den Zwecken der konkreten Datenverarbeitung.

Die ***Schutzanforderungsklassen*** definieren in allgemeiner Form die technischen und organisatorischen Anforderungen, die für Verarbeitungsvorgänge der betreffenden Klasse maßgeblich sind. Dabei wird für jede Schutzbedarfsklasse eine korrespondierende Schutzanforderungsklasse definiert.

Die Einteilung der Schutzbedarfs- und Schutzanforderungsklasse ist durch den System-Anbieter vorzunehmen. Diese Aufgabe korrespondiert mit den Rollen, Verantwortungssphären und Einsichtsmöglichkeiten von Auftraggeber und Auftragnehmer im Rahmen des Einsatzes von schulischen Informationssystemen.

Der System-Anbieter hat im schulischen Umfeld oftmals die Entwicklungs- oder (Vor-)Konfigurationsverantwortung für das schulische Informationssystem. Der Anbieter entwickelt demnach das System entsprechend vorab geplanter Benutzungszwecke, oder (vor)konfiguriert das System für solche Zwecke. Er hat im Rahmen dieser Rolle die Einsichtmöglichkeit über die im System (typischerweise) stattfindenden Datenverarbeitungsprozesse, sowie deren inherentes Risiko für die Rechte und Freiheiten natürlicher Personen, welches maßgeblich von den vorab bestimmten Benutzungszwecken und den dafür notwendigerweise zu verarbeitenden personenbezogenen Daten abhängt. Folglich kann der System-Anbieter bei der Festlegung der Schutzbedarfsklasse bereits anhand des Benutzungszwecks des Systems und der dafür notwendigerweise, oder typischerweise zu verarbeitenden personenbezogenen Daten eine verlässliche Einstufung des Schutzbedarfs vornehmen.

Dies wird oft unproblematisch sein, soweit der System-Anbieter ein spezifisches schulisches Informationssystem anbietet, das lediglich zu einem konkreten Verarbeitungszweck und mit bereits konkret bekannten Datentypen operiert. Lassen sich hingegen – was im schulischen Alltag der Ausnahmefall sein wird – mit dem zu beauftragenden System unterschiedliche Verarbeitungszwecke verfolgen und damit auch unterschiedliche Datenarten verarbeiten,[2] so trifft den System-Anbieter die Pflicht, den Schutzbedarf so festzulegen, das die höhere in Betracht kommende Schutzbedarfsklasse ausgewählt wird und dementsprechend eine höhere Schutzanforderungsklasse erfüllt sein muss.

Der System-Anbieter kann diese Einstufung aufgrund seiner fachlichen Expertise und oft uneingeschränkten Einsichtmöglichkeit der Datenverarbeitungsprozesse des Systems zwangsläufig exakter vornehmen als der System-Kunde. Der System-Kunde wird also in seiner Auswahl und Bewertung von angebotenen schulischen Informationssystemen entlastet.

Aufgrund der genannten Faktoren obliegt dem System-Anbieter die Prüfung und Festlegung der Schutzbedarfsklasse und der daraus resultierenden Schutzanforderungsklasse. Dies wird durch die Zertifizierungsstelle überprüft. Im Zertifikat wird damit die Eignung des schulischen Informationssystems für eine konkrete Schutzanforderungsklasse zum Ausdruck gebracht.

2. Die Schutzklassen des DIRECTIONS-Kriterienkatalogs

Der DIRECTIONS-Kriterienkatalog beruht auf der Unterscheidung von zwei Schutzklassen (1 und 2). Für diese Schutzklassen werden sowohl der Schutzbedarf (Schutzbedarfsklassen) als

[2] Beispiel: ein schulisches Informationssystem unterstützt ganz allgemein den Präsenzunterricht. Soll es in einem Fach eingesetzt werden, in dem Daten über politische Meinungen, religiöse oder weltanschauliche Überzeugungen verarbeitet werden (ggf. Schutzbedarfserhöhung nach der Wertung des Art. 9 Abs. 1 DSGVO), so muss der System-Anbieter dies bei der Festlegung des Schutzbedarfs berücksichtigten.

auch Schutzanforderungen (Schutzanforderungsklassen) beschrieben. Diese Schutzklassen orientieren sich insbesondere an

1. der Art der verarbeiteten Daten (z.B. besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO oder Daten, die an „verpönte“ Merkmale i.S.v. Art. 21 GRCh und Art. 3 Abs. 3 GG anknüpfen),
2. dem Anlass und den Umständen der Verarbeitung der Daten (z.B. Verarbeitung im Rahmen der Schulpflicht oder im Rahmen freiwilliger Nutzung, Dauer der Speicherung, Nutzung zur Profilbildung, heimliches oder offenes Vorgehen etc.),
3. den einzelnen Verwendungszwecken der Verarbeitung,
4. dem betroffenen Personenkreis (z.B. Daten von Kindern, Daten von Lehrkräften, Daten von Erziehungsberechtigten etc.) sowie
5. der außerhalb der Datenschutz-Grundverordnung kategorisierten Schutzbedürftigkeit betroffener Personen (z.B. Berufsgeheimnisträger wie etwa Schulpsychologen; Fernmeldegeheimnisse).

Wichtig ist dabei insbesondere, dass der jeweilige Zweck der Datenverarbeitung bestimmt wird. So können etwa Adressdaten zu unterschiedlichen Zwecken verarbeitet werden, die im Rahmen des Schutzklassenkonzepts eine unterschiedliche Schutzbedürftigkeit bedingen können (z.B. kann die Datenverarbeitung für Abrechnungszwecke, also der Zusendung der Rechnung oder Mahnung, anders zu beurteilen sein als die Verarbeitung derselben Daten für andere Zwecke, z.B. für die Zuordnung bestimmter Erkrankungen).

Nicht vom Schutzklassenkonzept erfasst werden Verarbeitungsvorgänge, bei denen keine personenbezogenen Daten verarbeitet werden und somit kein datenschutzrechtlicher Schutzbedarf vorliegt.

3. Die Ermittlung des Schutzbedarfs

Der Schutzbedarf wird in folgendem Verfahren ermittelt:

1. Schritt: Der Schutzbedarf wird anhand der oben (2.) sowie unten („Schritt 1: Ermittlung des typisierten Schutzbedarfs “) genannten Kriterien zunächst in typisierter Form bestimmt.

2. Schritt: Es ist zu überprüfen, ob der Schutzbedarf aufgrund der Umstände des Einzelfalles erhöht oder abgesenkt ist.

Im Ergebnis wird der Schutzbedarf der konkreten Datenverarbeitung nach den Schutzbedarfsklassen kategorisiert. Die Einordnung eines Verarbeitungsvorgangs in eine der zwei Schutzbedarfsklassen obliegt dem System-Anbieter, wenn und soweit dieser ein System zertifizieren lassen möchte, dessen Zwecke und zu verarbeitende Daten bereits konkret bekannt sind (s.o.). Der System-Anbieter hat zunächst den typisierten Schutzbedarf zu bestimmen (Schritt 1) und sodann zu prüfen, ob dieser im Einzelfall erhöht oder abgesenkt ist (Schritt 2).

Schritt 1: Ermittlung des typisierten Schutzbedarfs

Anhand des oben umrissenen Verfahrens ist das schulische Informationssystem bzw. sind die selbstständigen Verarbeitungsvorgänge vorab in eine der beiden Schutzbedarfsklassen einzuordnen. Werden Daten aus unterschiedlichen Schutzbedarfsklassen so zusammen verarbeitet, dass keine selbstständigen Verarbeitungsvorgänge vorliegen bzw. eine solche Aufspaltung nicht adäquat erscheint, gilt jeweils die höhere Schutzbedarfsklasse.

Hoher Schutzbedarf (Schutzbedarfsklasse 1)

Beim Einsatz schulischer Informationssysteme sind regelmäßig Daten von Kindern betroffen, die nach dem Schutzkonzept der Datenschutz-Grundverordnung besonders zu schützen sind (vgl. EG 38, 58 Satz 4 DSGVO, Art. 6 Abs. 1 lit. f., Art. 8, Art. 12 Abs. 1 Satz 1 DSGVO). Hinzu kommt das besondere Abhängigkeitsverhältnis insbesondere bei schulpflichtigen Kindern, das ebenfalls einen prinzipiell zu beachtenden risikoerhöhenden Faktor darstellt. Diese Abhängigkeit besteht auch für Erziehungsberechtigte, deren Daten ebenfalls verarbeitet werden. Hinsichtlich der Lehrkräfte besteht ebenfalls ein Abhängigkeitsverhältnis gegenüber dem Dienstherrn bzw. Arbeitgeber. Aus diesen Gründen ist bei schulischen Informationssystemen mindestens von einem hohen Schutzbedarf auszugehen, d.h. es gibt – anders als bei vielen anderen Verarbeitungsvorgängen – keinen „normalen“ Schutzbedarf. Im Einzelfall kann sich eine Erhöhung ergeben.

Beispielhaft besteht bei der Verarbeitung der folgenden, nicht abschließend aufgezählten Daten mindestens ein hoher Schutzbedarf:

- Name, Vorname, Anschrift, Telefonnummer, E-Mail-Adresse, Geburtsjahr, Alter, Geschlecht, Staatsangehörigkeit, Beruf (von Schülerinnen und Schülern, Lehrkräften, Erziehungsberechtigten).
- Verwandtschaftliche Beziehungen und Bekanntenkreis (z.B. Listen oder einzelne Kontaktdaten, aus denen sich eine Beziehung zwischen natürlichen Personen ergibt, wie u.a. Notfallkontakte von Schülerinnen und Schülern, Lehrkräften und anderen Mitarbeitenden, Telefonlisten, die für Notfälle durch Klassenverbände oder die Schulleitung erstellt werden).
- Login-Daten (z.B. Nutzernamen, E-Mail-Adressen).
- Arbeitszeitdaten von Lehrkräften und anderen Mitarbeitenden.
- Lohnabrechnungsdaten und Einkommensdaten von Lehrkräften und anderen Mitarbeitenden (z.B. Gehaltsklassen, Erfahrungsstufen, Daten über Sozialleistungen, Steuerabgaben usw.).
- Daten über Geschäfts- und Vertragsbeziehungen (z.B. Daten über die Einbindung und Beziehung von Drittangeboten durch Nutzer oder Kunden des schulischen Informationssystems, im Rahmen des Nachmittagsmarktes z.B. Daten, die zur Eingehung eines Vertragsverhältnisses notwendig sind, wie bspw. Zahlungsinformationen).

Sehr hoher Schutzbedarf (Schutzbedarfsklasse 2)

Unter den sehr hohen Schutzbedarf fallen Verarbeitungsvorgänge, wenn u.a. die folgenden Voraussetzungen erfüllt sind. Im Einzelfall können sich Abweichungen ergeben (s.u. 3.2).

a) Es handelt sich um besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO bzw. „verpönte“ Merkmale i.S.v. Art. 21 GRCh und Art. 3 Abs. 3 GG. Diese Datenarten bergen generell ein sehr hohes Missbrauchsrisiko, unabhängig davon, wie sie verwendet werden. Im Wege einer Einzelfallprüfung kann von dieser Vermutung abgewichen und die Verarbeitung dieser Daten einer niedrigeren Schutzklasse zugeordnet werden (s.u. 3.2).

Dies betrifft zum Beispiel:

- Daten über die ethnische Herkunft von Kindern, Lehrkräften, Erziehungsberechtigten oder anderen Personen. Hierzu zählt nicht die Staatsangehörigkeit.
- Daten über politische Meinungen von Kindern, Lehrkräften, Erziehungsberechtigten oder anderen Personen (z.B. politische Orientierungen der Schülerinnen und Schüler, die sich aus geschriebenen Texten oder anderen Unterrichtsbeiträgen zu politischen Themen ergeben).
- Nicht veränderbare Personendaten, die lebenslang als Anker für Profilbildungen dienen können wie genetische Daten i.S.v. Art. 4 Nr. 13 DSGVO oder biometrische Daten i.S.v. Art. 4 Nr. 14 DSGVO. Die Verarbeitung von Lichtbildern fällt als solche grundsätzlich nicht unter den Begriff der biometrischen Daten (EG 51 Satz 3 DSGVO).
- Daten über religiöse oder weltanschauliche Überzeugungen von Kindern, Lehrkräften oder Erziehungsberechtigten (z.B. religiöse oder weltanschauliche Überzeugungen, die sich aus geschriebenen Texten oder anderen Unterrichtsbeiträgen ergeben, ebenso wie die Daten über die Zugehörigkeit zu oder Mitarbeit in einer religiösen oder weltanschaulichen Gruppierung). Bei Schülerinnen und Schülern über 14 Jahren ist dabei zu beachten, dass die Daten dem Kind zugerechnet werden müssen. Bei jüngeren Schülerinnen und Schülern sind diese Daten ggf. gleichzeitig und insbesondere die Daten der Erziehungsberechtigten.
- Daten zum Sexualleben oder zur sexuellen Orientierung von Kindern, Lehrkräften, Erziehungsberechtigten oder anderer Personen.
- Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DSGVO

b) Es handelt sich um Datenverarbeitungsvorgänge zur Überwachung, Bewertung und Profilbildung.[3] Diese Datenverarbeitungsvorgänge bergen das sehr hohe Risiko, das ohnehin bestehende Abhängigkeitsverhältnis zwischen Schülerinnen und Schülern und Lehrkräften, sowie anderen Schulbeschäftigten durch einen Informationsmachtzuwachs zu verstärken. Durch diesen Informationszuwachs wird auch das Missbrauchsrisiko von Informationen durch Lehrkräfte oder andere Schulbeschäftigte erhöht (Art. 14 GRCh). Dies gilt vor allem, wenn Lehrkräfte oder andere Schulbeschäftigte aufgrund der zusätzlichen Information für die Schülerinnen und Schüler nachteilige Schlussfolgerungen ziehen können, insbesondere wenn diese das weitere Fortkommen der Schülerinnen und Schüler nachteilig beeinflussen kann (Art. 15 GRCh). Solche Entscheidungen können außerdem zu Diskriminierungen i.S.v. Art. 21 GRCh führen. Die Datenverarbeitung darf außerdem keine Benachteiligungen aufgrund verpönter Merkmale i.S.d. Art. 21 GRCh entstehen lassen.

[3] Normativer Anhaltspunkt hierfür ist u.a. Art. 35 Abs. 3 lit. a DSGVO, s. näher die Konkretisierung der Art.-29-Gruppe, WP 248, 2018, S. 10 ff.

Dies betrifft zum Beispiel:

- Datenverarbeitungen, die die jederzeitige Ermittlung des Aufenthaltsortes von Schülerinnen und Schülern ermöglichen (bspw. durch Feststellung des Standortes von Endgeräten, um die Nutzung eines schulischen Informationssystems in der Schule zu überwachen).
- Fehl- bzw. Anwesenheitszeiten von Schülerinnen und Schülern, Lehrkräften sowie anderen Mitarbeitenden (z.B. Zeitstempel der aktiven Nutzung eines schulischen Informationssystems), soweit diese Daten zur Verhaltens- und Leistungskontrolle mit rechtlichen Konsequenzen (z.B. Ordnungsmaßnahmen, Abmahnungen, Überprüfung der Dienstfähigkeit beim Amtsarzt) genutzt werden können.
- Die Sammlung und Interpretation verschiedenster Daten von Schülerinnen und Schülern, um Lernfortschritte zu messen, zukünftige Leistungen vorauszuberechnen und potenzielle Problembereiche aufzudecken (Learning Analytics).
- Die Sammlung und Interpretation verschiedenster Daten von Schülerinnen und Schülern, die für die Bewertung der schulischen Leistungen einer einzelnen Schülerin und eines einzelnen Schülers oder auch von Schülerinnen- und Schülergruppen herangezogen werden sollen.
- Beurteilung von Prüfungsleistungen, Prüfungsergebnisse sowie Zeugnisse.
- Persönlichkeitsprofile, z.B. Bewegungsprofile, Beziehungsprofile, Interessenprofile oder Kaufverhaltensprofile, die spezifische Bewertungen der Persönlichkeit der betroffenen Person ermöglichen (vor allem ihr Verhalten analysieren und prognostizieren); dazu gehören insbesondere: Nutzungsprofile, die einen Rückschluss auf die Art und Weise der Nutzung des schulischen Informationssystems zulassen und nicht ausschließlich zur Personalisierung oder Verbesserung des Systems verwendet werden. Entsprechende Profile können sich insbesondere aus den oben genannten Datenmehrheiten ergeben.

c) Es handelt sich um Datenverarbeitungsvorgänge mit inhärenter Intransparenz für die betroffenen Personen. Auch diese Datenverarbeitungsvorgänge bergen das sehr hohe Risiko, das ohnehin bestehende Abhängigkeitsverhältnis zwischen Schülerinnen und Schülern und Lehrkräften sowie anderen Schulbeschäftigten durch einen Informationsmachtzuwachs zu verstärken. Durch diesen Informationszuwachs wird auch das Missbrauchsrisiko von Informationen durch Lehrkräfte oder andere Schulbeschäftigte erhöht (Art. 14 GRCh). Dies gilt insbesondere, wenn diese Personen aufgrund der zusätzlichen Information für die Schülerinnen und Schüler nachteilige Schlussfolgerungen ziehen können.

Dies betrifft zum Beispiel:

- Anwendung von Algorithmen bei der Auswertung von Nutzungsverhalten zur Personalisierung des schulischen Informationssystems.
- Anwendung von Algorithmen, die zur Erreichung der in vorhergehendem Buchstaben b) gelisteten Verarbeitungszwecke eingesetzt werden.

d) Es handelt sich um Verarbeitungsvorgänge, die eine außerhalb der Datenschutz-Grundverordnung kategorisierte Schutzbedürftigkeit betreffen, z.B. das Fernmeldegeheimnis oder eine andere Geheimhaltungspflicht. Dies betrifft zum Beispiel:

- Kommunikationsinhalte und Verkehrsdaten (z.B. E-Mail, Brief, Telefonat), die durch das Fernmeldegeheimnis i.S.v. § 3 TTDSG besonders geschützt sind.
- Personalverwaltungsdaten aus Beschäftigungsverhältnissen inkl. Angaben zur dienstlichen Beurteilung und beruflichen Laufbahn in der Personalakte, die nach Beamtenrecht besonders zu schützen sind (vgl. § 106 BBG, § 50 BeamtStG sowie tlw. weitergehende Regelungen der Bundesländer wie § 86 Abs. 3 HBG).
- Daten, die durch Berufsgeheimnisvorschriften zusätzlich geschützt sind.

Die sehr hohe Schutzbedürftigkeit ergibt sich daraus, dass die betroffene Person nicht ohne Weiteres kontrollieren kann, ob die zur Wahrung des Geheimnisses verpflichtete Person dies auch tatsächlich einhält. Korrespondierende Schutzanforderungen zielen daher in der Regel auf Mechanismen ab, die sicherstellen sollen, dass der Dritte die Vertraulichkeit trotz der fehlenden Möglichkeit einer unmittelbaren Kontrolle durch die betroffene Person wahrt (siehe „Sehr hohe Schutzanforderungen (Schutzanforderungsklasse 2)“).

e) Es handelt sich um Verarbeitungsvorgänge, die Einblicke in die familiären Verhältnisse und/oder in das Zuhause der betroffenen Personen gewähren (Art. 7 GRCh). Der sehr hohe Schutzbedarf ergibt sich hier aus dem Umstand, dass es sich bei Einblicken in das Privatleben der betroffenen Personen innerhalb dieser Kontexte um den Kern des Rechts auf Privatleben handelt. Werden diese Daten im jeweiligen Kontext direkt, außerhalb des schulischen Bereichs erhoben, zielen die Schutzanforderungen in der Regel auf die klassische Ausschlussfunktion der Privatsphärengarantien ab, sprich die Möglichkeit der betroffenen Person, diese Einblicke etwa durch Nichtabgabe einer erforderlichen Einwilligung zu verhindern.

Schritt 2: Einzelfallbetrachtung

Im Einzelfall kann in Abweichung von der typisierenden Schutzbedarfsermittlung (Schritt 1) ein hoher Schutzbedarf (Schutzbedarfsklasse 1) zu einem sehr hohen Schutzbedarf (Schutzbedarfsklasse 2) erhöht werden bzw. ein sehr hoher Schutzbedarf (Schutzbedarfsklasse 2) auf einen hohen Schutzbedarf (Schutzbedarfsklasse 1) abgesenkt werden. Ein Absinken unter den hohen Schutzbedarf oder ein Übersteigen des sehr hohen Schutzbedarfs ist nicht möglich.

Erhöhung

Zu einer Erhöhung der Schutzbedarfsklasse kann es kommen, wenn:

- große Menge an Daten der Schutzbedarfsklasse 1 verarbeitet werden; dabei können – in Anlehnung an das WP 248 Rev. 01 der Art-29-Gruppe[4] berücksichtigt werden: Zahl der betroffenen Personen; verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente; geografisches Ausmaß der Datenverarbeitung;
- die Wahrscheinlichkeit des Schadenseintritts besonders hoch ist;[5]
- eine sehr lange Speicherdauer vorliegt;

[4] Art.-29-Gruppe, WP 248 Rev. 01, 2017, S. 11.
[5] S. SDM D3 sowie EG 76 DSGVO.

- ein Abgleich oder Zusammenführen von Datensätzen durchgeführt wird.[6]

Absenkung

Zu einer Absenkung der Schutzbedarfsklasse kann es in folgenden Situationen kommen: Verarbeitung besonderer Kategorien personenbezogener Daten (i.d.R. Sehr hoher Schutzbedarf (Schutzbedarfsklasse 2)), von der keine besondere Gefahren ausgehen, z.B.:

- Daten, die einen Rückschluss auf Erkrankungen oder Einschränkungen der betroffenen Person zulassen (Gesundheitsdaten), deren Bekanntwerden der betroffenen Person aber in keinem besonderen Maße unangenehm ist und die nicht zu einer gesellschaftlichen Stigmatisierung der betroffenen Person führt. Dies sind z.B. Daten, die lediglich auf Erkrankungen hinweisen, die eine kurze Verhinderung an der Unterrichtsteilnahme verursachen (bspw. eine Erkältung, Kopfschmerzen etc.) oder auf eine sichtbare und allgemein nicht stigmatisierungsfähige körperliche Einschränkung der betroffenen Person hinweisen (bspw. die Notwendigkeit des Tragens einer Sehhilfe). Sobald dieser Bagatellbereich verlassen wird oder sogar Daten vorliegen, die zu einer gesellschaftlichen Stigmatisierung der betroffenen Person führen können (z.B. Schwerbehinderungsinformationen zur Bedienung des Informationssystems, chronische Erkrankungen, psychische Erkrankungen etc.), kommt eine Absenkung nicht in Betracht.

- Daten, die nur über die Nichtteilnahme oder Teilnahme an einem Religionsunterricht oder einem vergleichbaren Weltanschauungsunterricht (z.B. Ethikunterricht) eine Aussage treffen (Daten über religiöse oder weltanschauliche Überzeugungen i.S.v. Art. 9 Abs. 1 DSGVO).

- Daten, die eine Aussage über die bloße Mitwirkung in schulischen Vertretungsgremien treffen.

- Daten, die eine Aussage über den Personenstand treffen (obwohl dies in Verbindung mit einer Angabe über das Geschlecht des Partners Daten über die sexuelle Orientierung i.S.v. Art. 9 Abs. 1 DSGVO sein können)[7].

- Fernmeldegeheimnis oder andere Geheimhaltungspflichten (i.d.R. Sehr hoher Schutzbedarf (Schutzbedarfsklasse 2))

- Verbindungs- und Verkehrsdaten, die ausschließlich einen Rückschluss auf die Nutzung des schulischen Informationssystems im Unterricht oder die Nutzung während der Schulzeit zulassen (nicht schutzbedarfsmindernd ist also die Erfassung der konkreten Zeiten, z.B. per Zeitstempel, wann die Tools außerhalb der Unterrichtszeit genutzt werden). Dazu gehören auch Verbindungs- und Verkehrsdaten, die Rückschluss auf eine Nutzung im Fernunterricht zulassen. Nicht umfasst davon sind Verbindungsdaten, die eine genaue Ortung der Nutzer ermöglichen, die über die Nutzung eines Internetanschlusses hinausgeht.

- Inhaltsdaten der Telekommunikation, deren Verarbeitung zur Erfüllung des Bildungs- und Erziehungsauftrages erforderlich ist und bei deren Verarbeitung grundsätzlich

[6] Art.-29-Gruppe, WP 248 Rev. 01, 2017, S. 12.
[7] S. EuGH, Urteil vom 1. August 2022, C-184/20.

nicht davon auszugehen ist, dass unterrichts- oder schulleistungsfremde Inhalte ausgetauscht werden (Beispiel: Eine öffentliche Chat- oder Posting-Funktion, die für die Unterrichtsorganisation oder die Durchführung einer Diskussion zu Unterrichtszwecken genutzt wird. Nicht umfasst sind: Insbesondere Inhaltsdaten von Privatnachrichten, die zwischen Nutzern des schulischen Informationssystems ausgetauscht werden können).

4. Zuordnung der Schutzanforderungsklasse

Aus der ermittelten Schutzbedarfsklasse ergibt sich die passende Schutzanforderungsklasse. Wurde ein hoher Schutzbedarf (Schutzbedarfsklasse 1) ermittelt, gilt die hohe Schutzanforderungsklasse (Schutzanforderungsklasse 1), wurde ein sehr hoher Schutzbedarf (Schutzbedarfsklasse 2) ermittelt, gilt die sehr hohe Schutzanforderungsklasse (Schutzanforderungsklasse 2).

Hohe Schutzanforderungen (Schutzanforderungsklasse 1)

Der System-Anbieter hat risikoangemessene TOM zu ergreifen, um die Datenminimierung, die Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung und Transparenz personenbezogener Daten sowie die Intervenierbarkeit sicherzustellen. Für den Bereich der Datensicherheit bedeutet dies, dass die Daten insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung zu schützen sind sowie die Belastbarkeit des schulischen Informationssystems zu gewährleisten ist.

Die TOM müssen geeignet sein, um im Regelfall solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder seiner Mitarbeitenden oder fahrlässiger Handlungen Dritter auszuschließen. Gegen vorsätzliche Eingriffe ist ein Mindestschutz vorzusehen, der diese erschwert. Jeder Eingriff muss nachträglich festgestellt werden können.

Sehr hohe Schutzanforderungen (Schutzanforderungsklasse 2)

Ein sehr hoher Schutzbedarf führt dazu, dass im Vergleich zum hohen Schutzbedarf zusätzliche oder wirksamere risikoangemessene TOM ergriffen werden müssen, um die Datenminimierung, die Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung und Transparenz personenbezogener Daten sowie die Intervenierbarkeit sicherzustellen. Für die Datensicherheit bedeutet dies, dass die Daten insbesondere gegen Vernichtung, Verlust, Veränderung, unbefugten Zugang und unbefugte Offenlegung zu schützen sind sowie die Belastbarkeit des schulischen Informationssystems zu gewährleisten ist. Gleichzeitig müssen die für die erste Schutzklasse geeigneten Maßnahmen erfüllt und ihre Ausführung an den Schutzbedarf angepasst werden.

Dies kann erreicht werden, indem die Wirkung einer Maßnahme erhöht wird, soweit diese einen Ansatzpunkt für eine solche Skalierung bietet. Ein Beispiel hierfür ist die Erhöhung der Länge eingesetzter kryptografischer Schlüssel oder der Einsatz von Hardware-Token. Weiterhin kann eine Anpassung dadurch erfolgen, dass mit größerer Zuverlässigkeit eine spezifikationsgerechte Ausführung der Maßnahme sichergestellt wird. Dazu müssen mögliche Störeinflüsse bestimmt und die Robustheit der Maßnahmen durch zusätzliche Vorkehrungen – oft organisatorischer Natur – erhöht werden.

Die ergriffenen Maßnahmen müssen geeignet sein, um solche Vorgänge aufgrund technischer oder organisatorischer Fehler, einschließlich Bedienfehler, des System-Anbieters oder seiner Mitarbeitenden, oder fahrlässiger oder vorsätzlicher Handlungen Dritter auszuschließen. Die Maßnahmen müssen auch geeignet sein, Schädigungen durch fahrlässige Handlungen Befugter im Regelfall zu verhindern. Gegen vorsätzliche Eingriffe ist ein Schutz vorzusehen, der zu erwartende Eingriffe hinreichend sicher ausschließt. Dazu gehört insbesondere ein hinreichender Schutz gegen bekannte Angriffsszenarien sowie Maßnahmen, durch die Eingriffe nachträglich festgestellt werden können.