eduSeal

Begleitdokument

Risikobewertungs-konzept

Stand 01.03.2026

eduSeal

Weitere Begleitdokumente

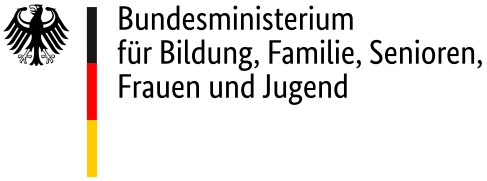
- Zertifizierungsgegenstand
- Kriterienkatalog
- Erläuterungen und Umsetzungshinweise
- Erläuterungen zum Zertifizierungsverfahren für System-Anbieter

Beitrag zum Forschungsprojekt „Data Protection Certification for Educational Information Systems (directions)“, das durch das Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend gefördert wird (FKZ 01PP21003).

Projekt Webseite
www.directions-cert.de

Das Forschungsprojekt directions basiert auf den Ergebnissen und Dokumenten von AUDITOR (www.trusted-cloud.de).

Gefördert vom:



Autoren

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

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

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

[c] Chair of Information Infrastructures an der School of Computation am Campus Heilbronn der Technischen Universität München

[d] Fachgebiet Wirtschaftsinformatik, insb. Enterprise Systems and Platforms der Universität Kassel

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BBG	Bundesbeamtengesetz (letzte berücksichtigte Änderung: 27.02.2025)
BeamtStG	Beamtenstatusgesetz (letzte berücksichtigte Änderung: 20.12.2023)
BMG	Bundesmeldegesetz (letzte berücksichtigte Änderung: 25.12.2025)
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
d.h.	das heißt
DS-GVO	Datenschutz-Grundverordnung (letzte berücksichtigte Änderung: 04.03.2021)
DSK	Datenschutzkonferenz
EG	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
f.	folgend
ff.	folgende
ggf.	gegebenenfalls
GRCh	Charta der Grundrechte der Europäischen Union (letzte berücksichtigte Änderung: 12.12.2007)
i.S.d.	Im Sinne des
i.S.v.	Im Sinne von
i.V.m.	In Verbindung mit
ID	Identifier
lit.	Litera
Nr.	Nummer
s.	siehe
S.	Satz
s.a.	siehe auch
SDM	Standard-Datenschutzmodell
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (letzte berücksichtigte Änderung: 2.12.2025)
TOM	technische und organisatorische Maßnahme
u.a.	unter anderem
UAbs.	Unterabsatz
Urt.	Urteil
z. B.	zum Beispiel

Hinweis zur geschlechtsneutralen Formulierung:

Alle personenbezogenen Bezeichnungen in diesem Dokument sind geschlechtsneutral zu verstehen. Zum Zweck der besseren Lesbarkeit wird daher auf die geschlechtsspezifische Schreibweise verzichtet, so dass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z. B. ist bei der Bezeichnung *System-Anbieter* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

A. Einführung

1. Ziel der Risikobewertung

Die DS-GVO folgt einem risikobasierten Ansatz.[1] Dies zeigt sich insbesondere in Art. 24, 25 und 32 DS-GVO, die die Anforderungen an TOM von den Risiken für die Rechte und Freiheiten natürlicher Personen abhängig machen, in Art. 33 und 34 DS-GVO, die Melde und Benachrichtigungspflichten bei Verletzungen des Schutzes personenbezogener Daten vorsehen, wenn Risiken für die Rechte und Freiheiten natürlicher Personen bestehen, sowie in Art. 35 und 36 DS-GVO, die bei hohen Risiken für die Rechte und Freiheiten natürlicher Personen eine Datenschutz-Folgenabschätzung verlangen (s.a. EG 75, 76, 85, 90, 91, 94, 95 und 96 DS-GVO).

Um den risikobasierten Ansatz umsetzen zu können, bedarf es einer Risikobewertung durch den Systemanbieter, die er für die verschiedenen Verarbeitungsvorgänge seines schulischen Informationssystems vorzunehmen hat.

Das folgende Risikobewertungskonzept orientiert sich an bekannten Konzepten, die insbesondere für die Gestaltung von TOM entwickelt worden sind, und knüpft an den Risikobegriff der DS-GVO sowie Überlegungen der Datenschutzaufsichtsbehörden an.[2] Es soll als Hilfestellung bei der Bewertung bestehender Risiken dienen, ohne aber einen Anspruch auf Vollständigkeit zu erheben. Daher sind bei der Risikobewertung auch Erwägungen zulässig, die in dem Risikobewertungskonzept nicht aufgeführt werden, solange sie plausibel und nachvollziehbar sind.

2. Gegenstand der Risikobewertung

Gegenstand der Risikobewertung sind die einzelnen Verarbeitungsvorgänge in dem schulischen Informationssystem des System-Anbieters. Die Verarbeitungsvorgänge sind hinreichend zu beschreiben und von anderen Verarbeitungsvorgängen klar abzugrenzen, so dass keine Lücken bei der Risikobetrachtung entstehen.

3. Begriffe und Vorgehensweise

Ein Risiko i.S.d. DS-GVO „ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Es hat zwei Dimensionen: Erstens die Schwere des Schadens und zweitens die Wahrscheinlichkeit, dass das Ereignis und die Folgeschäden eintreten.“[3]

Der Begriff des Schadens ist umfassend zu verstehen und insbesondere nicht auf monetäre Schäden begrenzt.[4] Zu den möglichen Schäden zählen physische Schäden (einschließlich Schäden für die Gesundheit), aber auch (sonstige) materielle und immaterielle Schäden (EG 75 DS-GVO), was auch ungerechtfertigte Beeinträchtigungen von grundrechtlich geschützten Rechten und Freiheiten natürlicher Personen – einschließlich Art. 8 GRCh – einschließt.[5] Die Eintrittswahrscheinlichkeit und die Schwere möglicher Schäden sind für den Einzelfall unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung zu bestimmen (EG 76 DS-GVO). Eintrittswahrscheinlichkeit meint dabei „mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst

[1] S. z. B. Simitis/Hornung/Spiecker gen. Döhmann/ *Hornung/Spiecker gen. Döhmann*, Einl. Rn. 276 f.
[2] S. etwa das Standard-Datenschutzmodell (SDM, derzeit in der Version 3.1 idF des Beschlusses der DSK v. 14.5.2024, https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/), das auf Basis einer dreistufigen Risikobewertung zu zwei Schutzbedarfsstufen gelangt („normaler Schutzbedarf“ und „hoher Schutzbedarf“). Für die Risikobewertung verweist das SDM weiterhin auf DSK, Kurzpapier Nr. 18. In diesem wird eine Risikomatrix vorgeschlagen, die die Schwere möglicher Schäden und ihre Eintrittswahrscheinlichkeit abbildet („geringes Risiko“, „Risiko“, „hohes Risiko“). Das IT-Grundschutz-Kompendium des BSI (Stand Februar 2023, Glossar S. 7) differenziert – für Bedrohungen der IT-Sicherheit – die Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“. Im Zusammenhang mit Art. 35 DS-GVO setzt sich Art.-29-Gruppe, WP 248 Rev. 01 mit der Frage auseinander, wann ein „hohe Risiko“ gegeben ist. 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).
[3] DSK, Kurzpapier Nr. 18, S. 1 unter Bezugnahme auf EG 75 und 94 S. 2 DS-GVO.
[4] DSK, Kurzpapier Nr. 18, S. 2.
[5] DSK, Kurzpapier Nr. 18, S. 1.

auch ein Schaden sein kann) eintritt und mit welcher weiteren Wahrscheinlichkeit es zu Folgeschäden kommen kann".[6]

Das Risiko ist anhand einer objektiven Bewertung zu ermitteln (EG 76 DS-GVO). Dafür ist zunächst zu prüfen, welche Schäden im Zusammenhang mit den Verarbeitungsvorgängen überhaupt eintreten können (im Folgenden als Risikoidentifikation bezeichnet, s. B.). Sodann ist das Risiko zu bewerten, wobei die Schwere und Eintrittswahrscheinlichkeit möglicher Schäden in den Blick zu nehmen sind (im Folgenden als Risikobewertung bezeichnet, s. C.).[7] Dabei ist u.a. auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung Bezug zu nehmen (EG 76 DS-GVO). So können etwa folgende Aspekte berücksichtigt werden:

- die Art der verarbeiteten Daten (z. B. besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO oder Daten, die an „verpönte" Merkmale i.S.v. Art. 21 GRCh und Art. 3 Abs. 3 GG anknüpfen),
- der Umfang der Datenverarbeitung (z. B. Zahl betroffener Personen, Datenmenge, Dauer der Speicherung, Zahl zugriffsberechtigter Personen),
- die (sonstigen) Umstände der Datenverarbeitung (z. B. Profilbildung, neue Technologien, Daten von Kindern, Daten von Lehrkräften, Daten von Erziehungsberechtigten etc.; Daten, die bestimmen Geheimhaltungspflichten außerhalb der DS-GVO unterliegen, z. B. dem Berufs- oder Fernmeldegeheimnis).

Sowohl die Schwere als auch die Eintrittswahrscheinlichkeit möglicher Schäden können gering, mittel oder hoch ausfallen. Darauf aufbauend sind die Verarbeitungsvorgänge dahingehend einzuordnen, ob ein geringes, mittleres oder hohes Risiko besteht (s. D.).[8] In bestimmten Verarbeitungssituationen ergibt sich bereits aus den Wertungen des Gesetzgebers, dass von einem bestimmten – insbesondere einem hohen – Risiko auszugehen ist (z. B. bei der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 35 Abs. 3 lit. b DS-GVO).

Die Ermittlung des jeweiligen Risikos ist die Aufgabe des System-Anbieters. Diese Aufgabe korrespondiert mit seiner Rolle, Verantwortungssphäre und Einsichtsmöglichkeit im Rahmen des Einsatzes von schulischen Informationssystemen. Der System-Anbieter hat im schulischen Umfeld oftmals die Entwicklungs- und/oder (Vor-)Konfigurationsverantwortung für das schulische Informationssystem. Er entwickelt das System entsprechend vorab geplanter Benutzungszwecke und/oder konfiguriert es für solche Zwecke. Er hat im Rahmen dieser Rolle die Einsichtsmöglichkeit in die im System (typischerweise) stattfindenden Verarbeitungsvorgänge sowie deren inhärente Risiken für die Rechte und Freiheiten natürlicher Personen. Folglich kann meist nur der System-Anbieter eine verlässliche Einstufung des Risikos vornehmen.

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

B. Risikoidentifikation

Der System-Anbieter hat zunächst mögliche Schäden zu identifizieren.

1. Mögliche Schäden

Physische, materielle und immaterielle Schäden bei Schülerinnen und Schülern – aber auch Lehrkräften, anderem pädagogischen Personal sowie Erziehungsberechtigten – können aus der vorgesehenen Datenverarbeitung selbst oder aus eigen- oder fremdverursachten Abweichungen von

[6] DSK, Kurzpapier Nr. 18, S. 4.
[7] DSK, Kurzpapier Nr. 18, S. 2.
[8] S.a. DSK, Kurzpapier Nr. 18, S. 2: „geringes Risiko", „Risiko", „hohes Risiko".

der vorgesehenen Datenverarbeitung (z. B. durch unbefugten Zugriff Dritter auf die Daten, Naturkatastrophen, Hardwarestörungen) entstehen.[9] Zu denken ist insbesondere an (s. EG 75 und 85 Satz 1 DS-GVO[10]):

- Diskriminierung (vgl. auch Art. 21 GRCh),
- Identitätsdiebstahl oder -betrug,
- finanzielle Verluste,
- Rufschädigungen,
- körperliche oder psychische Verletzungen,
- Verlust der Privat- oder Intimsphäre (vgl. Art. 7 GRCh),
- Verlust der Vertraulichkeit von dem Berufsgeheimnis oder anderen Geheimhaltungsvorgaben,
- Erschwerung der Rechtsausübung und Verhinderung der Kontrolle personenbezogener Daten sowie
- (sonstige) wirtschaftliche oder gesellschaftliche Nachteile.

Speziell im schulischen Kontext kann auch die Beeinträchtigung der Schulkarriere bzw. des schulischen Fortkommens der Schülerinnen und Schüler oder der beruflichen Karriere von Lehrkräften ein Schaden sein (vgl. Art. 14 und 15 GRCh). Auch kann eine Behinderung des Unterrichts bzw. des Lernens (z. B. durch Ausfall des schulischen Informationssystems) als ein Schaden verstanden werden.

Zudem kann die rechtswidrige Verarbeitung personenbezogener Daten auch für sich gesehen einen Schaden darstellen, da es sich dabei gleichzeitig um eine nicht gerechtfertigte Beeinträchtigung von Art. 8 GRCh (Grundrecht auf Schutz personenbezogener Daten) sowie weiterer Grundrechte handeln kann.[11] Generell kann die Verarbeitung personenbezogener Daten unterschiedliche grundrechtlich geschützte Rechte und Freiheiten beeinträchtigen – und ggf. auch verletzen. Dies betrifft zunächst das Grundrecht auf Schutz personenbezogener Daten (8 GRCh), das bei jeder Verarbeitung personenbezogener Daten betroffen ist, sowie das Grundrecht auf Achtung des Privat- und Familienlebens (Art. 7 GRCh), wenn die verarbeiteten Daten z. B. Einblick in familiäre oder häusliche Sachverhalte erlauben. Im schulischen Kontext können zudem das Grundrecht auf Bildung (Art. 14 GRCh) und das Grundrecht auf Berufsfreiheit (Art. 15 GRCh) betroffen sein, wenn die Datenverarbeitung z. B. Einfluss auf den Schulerfolg einschließlich des Schulabschlusses oder den Einstieg in das Berufsleben hat. Kann die Datenverarbeitung zu einer Diskriminierung der betroffenen Personen führen (z. B. wegen Geschlecht, Rasse, Herkunft, Religion, politischer Anschauungen, Behinderung oder Alter), ist das Recht auf Nichtdiskriminierung (Art. 21 GRCh) betroffen. Je nach Verarbeitungsvorgang können weitere Grundrechte betroffen sein, z. B. die Meinungsfreiheit (Art. 11 GRCh) oder die Rechte von Kindern (Art. 24 GRCh). Beeinträchtigungen dieser Grundrechte führen zu Schäden, wenn sie nicht gerechtfertigt sind.[12]

2. Beispielhafte Verarbeitungssituationen

Je nach Verarbeitungsvorgang können im Zusammenhang mit der Verarbeitung verschiedene (spezifische) Schäden auftreten. Die folgenden Überlegungen sind nicht abschließend, sondern lediglich als Anregung zu verstehen, sich mit möglichen Schäden auseinanderzusetzen.

2.1 Login-Daten

Die Verarbeitung von Login-Daten (z. B. Nutzernamen und Passwörter) birgt für sich gesehen zunächst kein besonders Schadenspotential. Erlangen aber unbefugte Personen Zugriff auf verarbeitete Login-Daten, kann dies dazu führen, dass ein schulisches Informationssystem von unbefugten Personen genutzt werden, die sich als befugte Person ausgeben (Identitätsdiebstahl).

[9] DSK, Kurzpapier Nr. 18, S. 2
[10] Zu Schäden s. DSK, Kurzpapier Nr. 18, S. 3.
[11] DSK, Kurzpapier Nr. 18, S. 3.
[12] DSK, Kurzpapier Nr. 18, S. 3.

Diese Personen können durch die unbefugte Nutzung des schulischen Informationssystems zudem Zugriff auf weitere Informationen über Schülerinnen und Schüler oder Lehrkräfte bekommen und so z. B. deren Privatsphäre beeinträchtigen. Eine Störung der Verarbeitung der Login-Daten kann z. B. die Durchführung des Unterrichts behindern, wenn die Schülerinnen und Schüler ein schulisches Informationssystem deshalb nicht nutzen können.

2.2 Schulspezifische Personenattribute

Werden schulspezifische Personenattribute wie Klassenzugehörigkeit, Teilnahme an Unterricht und Kursen, Stundenplandaten, Teilnahme an Arbeitsgemeinschaften und Zugehörigkeit zu anderen schulischen Gruppen, Jahrgangsstufe und gewählter Bildungsgang in einem schulischen Informationssystem verarbeitet, kann es die Durchführung des Unterrichts behindern, wenn diese Informationen unrichtig oder nicht abrufbar sind.

2.3 Kontaktdaten

Werden Kontaktdaten von Schülerinnen und Schülern verarbeitet (z. B. Anschrift, Telefonnummer und E-Mail-Adresse), kann dies – insbesondere, wenn diese Daten unbefugten Personen offengelegt werden – dazu führen, dass unerwünschter Kontakt zu (minderjährigen) Schülerinnen und Schülern aufgenommen wird. Dies wiederum kann die physische und/oder psychische Integrität der Schülerinnen und Schüler gefährden und zu entsprechenden Schäden führen (z. B. bei übergriffigem Verhalten von Erwachsenen oder in Fällen von Mobbing). Die Verarbeitung kann ggf. auch Daten umfassen, bzgl. derer eine Auskunftssperre (z. B. wegen einer Bedrohungssituation) oder ein bedingter Sperrvermerk (§§ 51, 52 BMG) vorliegt.

Bei Verarbeitung von Kontaktdaten (z. B. Anschrift, Telefonnummer und E-Mail-Adresse) von Lehrkräften, sonstigem pädagogischem Personal und Erziehungsberechtigten können vergleichbare Schäden eintreten, wobei erwachsene Personen Übergriffen aber eher entgegentreten können als minderjährige Schülerinnen und Schüler.

Kontaktdaten können zudem – ggf. zusammen mit weiteren Informationen über die betroffenen Personen, etwa Konto- und Kreditkartendaten – für einen Identitätsdiebstahl genutzt werden (z. B. für Onlinebestellungen oder Betätigungen in sozialen Netzwerken unter falschem Namen), woraus sich auch finanzielle Nachteile oder Rufschädigungen für die betroffenen Personen ergeben können.

2.4 Überwachung, Bewertung und Profilbildung

Verarbeitungsvorgänge, die der Überwachung (bzw. dem Monitoring), der Bewertung und der Profilbildung dienen, können – je nach Situation – weitreichende Erkenntnisse über die betroffenen Schülerinnen und Schüler oder Lehrkräfte (etc.) hervorbringen und zu einem Verlust von Privatsphäre führen (wenn z. B. überwacht wird, wer wann und wie oft eine bestimmte Lernanwendung nutzt). Automatisierte Bewertungen (z. B. von gelösten Aufgaben) und Profilbildungen können, wenn sie z. B. auf einer nicht repräsentativen oder unvollständigen Datenlage beruhen oder sachfremde Erwägungen berücksichtigen, zu Diskriminierungen führen und ggf. die Schulkarriere bzw. das schulische Fortkommen der Schülerinnen und Schüler negativ beeinflussen. Soweit derartige Verarbeitungsvorgänge intransparent sind, können sie die eine effektive Kontrolle behindern und die Rechtsausübung erschweren.

Dies betrifft z. B.:

- 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) und so z. B. Rückschlüsse auf das Privatleben zulässt.

- Daten über Fehl- bzw. Anwesenheitszeiten von Schülerinnen und Schülern oder Lehrkräften (z. B. Einträge über unentschuldigtes Fehlen von Schülerinnen oder Schülern im Unterricht, Krankmeldungen), wenn diese Daten zur Verhaltens- und Leistungskontrolle mit rechtlichen Konsequenzen (z. B. Ordnungsmaßnahmen, Abmahnungen, Überprüfung der Dienstfähigkeit beim Amtsarzt) genutzt werden können, sowie Daten, die Aufschluss über den zeitlichen Umfang der Nutzung eines schulischen Informationssystems geben (z. B. Zeitstempel bzgl. Ein- und Ausloggen, Dauer der Nutzung, Standortdaten, genutzte Programme). Es kommt aber auf den Einzelfall an. Soweit z. B. beim Zugriff auf das schulische

Informationssystem Protokolldaten erstellt werden (z. B. Zeitstempel), deren Zweck ausschließlich in der Sicherstellung des funktionierenden Betriebs (einschließlich ausreichender Supportmöglichkeiten) durch den System-Anbieter liegt und auf die auch nur der System-Anbieter nur zu diesem Zweck Zugriff hat, ist es meist unwahrscheinlich, dass sich die beschriebenen Schäden realisieren.

- Die Erfassung personenbezogener Daten von Schülerinnen und Schülern, um Lernfortschritte zu messen und/oder zukünftige Leistungen einzuschätzen (z. B. bzgl. Empfehlung für Gymnasium), sowie adaptive Lernsysteme, bei denen nicht ohne Weiteres nachvollziehbar ist, wie Lernpräferenzen oder Lernfortschritte ermittelt wurden.[13] Dabei macht es hinsichtlich möglicher Schäden allerdings einen Unterschied, ob die Erfassung bloß punktuell erfolgt (z. B. punktuelle Erfassung des Lernstandes eines Schülers, etwa durch einen Englisch-Vokabeltrainer im Rahmen einer Übungseinheit, der erkennt, dass unregelmäßige Verben nicht beherrscht werden und deshalb vorschlägt, unregelmäßige Verben verstärkt zu üben), oder ob sie längerfristig und systematisch durchgeführt wird (z. B. über mehrere Übungseinheiten oder Schuljahre hinweg). Letzteres kann eher zu Schäden führen, da mit dem Umfang der Erfassung auch die Aussagekraft der Daten steigt.
- Die Sammlung und Interpretation verschiedener Daten von Schülerinnen und Schülern, die für die Bewertung der schulischen Leistungen (insbesondere Notengebung) herangezogen werden sollen.
- Beurteilung von Prüfungsleistungen, Prüfungsergebnisse sowie Zeugnisse.
- Persönlichkeitsprofile, d.h. Zusammenstellungen von Informationen über eine Person, die eine Beurteilung wichtiger Aspekte der Persönlichkeit der Person erlauben. Hierzu zählen u.a. Bewegungs-, Beziehungs-, Interessen- oder Kaufverhaltensprofile sowie Nutzungsprofile, die einen Rückschluss auf die Art und Weise der Nutzung des schulischen Informationssystems zulassen.
- Die automatisierte Auswertung des Nutzungsverhaltens mittels KI zur Personalisierung des schulischen Informationssystems (KI als Blackbox), die z. B. zu Diskriminierungen (z. B. unpassende Lernvorschläge) führen kann.

2.5 Kommerzielle Zwecke

Die Verarbeitung personenbezogener Daten von Schülerinnen und Schülern, Lehrkräften, anderem pädagogischen Personal sowie Erziehungsberechtigten zu kommerziellen Zwecken, etwa zum Schalten personalisierter Werbung in Folge von Profiling (ggf. auch nach Weitergabe an Dritte), kann bei den Betroffenen zu finanziellen Verlusten und wirtschaftlichen Nachteilen führen, wenn z. B. Minderjährige zu Kaufentscheidungen verführt werden, die nicht in ihrem Interesse sind. Die Auswertung von Daten zu kommerziellen Zwecken[14] kann zudem die Privatsphäre beeinträchtigen, wenn hierdurch z. B. Vorlieben einer Person ermittelt werden.

2.6 Besondere Kategorien personenbezogener Daten und Daten zu anderweitig „verpönten“ Merkmalen

Werden besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO bzw. Daten zu „verpönten“ Merkmale i.S.v. Art. 21 GRCh (z. B. Zugehörigkeit zu einer nationalen Minderheit) und Art. 3 Abs. 3 GG verarbeitet, kann dies – insbesondere bei (unbefugter) Offenlegung gegenüber Dritten – zu Diskriminierungen (z. B. Diskriminierungen von Schülerinnen und Schülern durch andere Schülerinnen und Schülern oder Dritte) und gesellschaftlichen Nachteilen sowie Verletzungen der Privatsphäre (z. B. bei Offenlegung von Gesundheitsdaten) führen.

Zu den besonderen Kategorien personenbezogener Daten zählen:

- Daten über die ethnische Herkunft von Schülerinnen und Schülern, Lehrkräften, Erziehungsberechtigten oder anderen Personen (z. B. Angaben zum äußeren Erscheinungsbild,

[13] Insoweit kann auch von Learning Analytics gesprochen werden. Zum Begriff s. Johnson/Adams/Dummins, NMC Horizon Report 2012, S. 26.
[14] Inwieweit die Verfolgung kommerzieller Zwecke im Schulkontext zulässig ist, ist eine andere Frage. Im Vormittagsmarkt wird eine Verarbeitung personenbezogener Daten von Schülerinnen und Schülern zu kommerziellen Zwecken regelmäßig unzulässig sein.

insbesondere Augenfarbe und -form, Haartyp oder Hautfarbe). Hierzu zählt nicht die Staatsangehörigkeit. Insoweit drohen z. B. rassistische Diskriminierungen.

- Daten über politische Meinungen oder die Gewerkschaftszugehörigkeit von Schülerinnen und Schülern, Lehrkräften, Erziehungsberechtigten oder anderen Personen (z. B. Informationen über politische Orientierungen der Schülerinnen und Schüler, die sich aus Unterrichtsbeiträgen wie z. B. Aufsätzen oder Freitextaufgaben zu politischen Themen ergeben). Insoweit drohen z. B. Diskriminierungen oder auch Rufschädigungen wegen als abseitig empfundener politischer Auffassungen, was sich auch in gesellschaftlichen Nachteilen äußern kann.

- Daten über religiöse oder weltanschauliche Überzeugungen von Schülerinnen und Schülern, Lehrkräften oder Erziehungsberechtigten (z. B. Informationen über religiöse oder weltanschauliche Überzeugungen, die sich aus Unterrichtsbeiträgen wie z. B. Aufsätzen oder Freitextaufgaben zu religiösen oder weltanschaulichen Themen ergeben; ebenso 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. Insoweit drohen z. B. Diskriminierungen wegen bestimmter religiöser Auffassungen.

- Nicht veränderbare Personendaten, die lebenslang als Anker für Profilbildungen dienen können wie genetische Daten i.S.v. Art. 4 Nr. 13 DS-GVO oder biometrische Daten i.S.v. Art. 4 Nr. 14 DS-GVO. Die Verarbeitung von Lichtbildern fällt als solche grundsätzlich nicht unter den Begriff der biometrischen Daten (EG 51 Satz 3 DS-GVO). Insbesondere biometrische Daten können, wenn sie in unbefugte Hände geraten, z. B. für einen Identitätsdiebstahl genutzt werden.

- Gesundheitsdaten i.S.v. Art. 4 Nr. 15 DS-GVO, also Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen. Insoweit drohen bei Bekanntwerden z. B. Diskriminierungen (und ggf. auch Rufschädigungen) wegen bestimmter Krankheiten, gesellschaftliche Nachteile (z. B. Stigmatisierungen bei bestimmten Krankheiten wie etwa HIV) sowie Nachteile für das schulische Fortkommen (z. B. bei psychischen oder chronischen Erkrankungen). Denkbar sind aber auch körperliche oder psychische Schäden, etwa wenn Gesundheitsdaten unrichtig sind oder fehlen und dies zur Nichtberücksichtigung gesundheitlicher Einschränkungen im Schulalltag führt.

- Daten zum Sexualleben oder zur sexuellen Orientierung von Schülerinnen und Schülern, Lehrkräften, Erziehungsberechtigten oder anderer Personen. Insoweit drohen bei Bekanntwerden z. B. Diskriminierungen wegen bestimmter sexueller Orientierungen, die nicht einer vermeintlichen Norm entsprechen.

Es kann auch die Verarbeitung von personenbezogenen Daten, die keine besonderen Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO sind, zu einer Diskriminierung führen, wie bspw. die Verarbeitung von Daten, die den sozialen Hintergrund erkennen lassen (z. B. eine Anschrift, die die Herkunft aus einem sozial schwachen Stadtteil erkennen lässt, oder Angaben zum Bezug von Sozialleistungen).

2.7 Daten zum Privat- oder Familienleben

Verarbeitungsvorgänge, die Einblicke in das Privat- und Familienleben sowie die Wohnung gewähren, können die besonders geschützte Privatsphäre (Art. 7 GRCh) beeinträchtigten bzw. verletzen. Werden Informationen aus der Privatsphäre bekannt, kann dies ggf. zudem zu Diskriminierungen, Rufschädigungen und (sonstigen) gesellschaftlichen Nachteilen führen.

Dies betrifft z. B.:

- Videofunktionen, die Vorgänge in einer Wohnung für andere Personen sichtbar machen können.

- Audiofunktionen, die Vorgänge in einer Wohnung für andere Personen hörbar machen können.

- Allgemein personenbezogene Daten, die Privates offenlegen können (z. B. Informationen zu zwischenmenschlichen Beziehungen oder Einblick in das häusliche Umfeld), sowie insbesondere auch besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO, etwa bzgl. religiöser Auffassungen (s. hierzu auch B.2.6.).

2.8 Geheimhaltungspflichtige Daten

Bei Verarbeitungsvorgängen, die Geheimhaltungspflichten außerhalb der DS-GVO betreffen, z. B. das Fernmeldegeheimnis oder das Berufsgeheimnis, kann der Bruch dieser Geheimnisse z. B. zu Beeinträchtigungen der Privatsphäre oder zu wirtschaftlichen Nachteilen führen. Auch kann der Bruch des Geheimnisses selbst als Schaden verstanden werden.

Dies betrifft z. B.:

- Kommunikationsinhalte und Verkehrsdaten (z. B. E-Mail, Brief, Telefonat), die durch das Fernmeldegeheimnis i.S.v. § 3 TDDDG 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 (z. B. bei Psychologen oder Ärzten).

C. Risikobewertung

Nach der Identifikation möglicher Schäden (s. B.) sind die Risiken der Verarbeitungsvorgänge im Rahmen einer objektiven Bewertung anhand von Schwere und Eintrittswahrscheinlichkeit der möglichen Schäden zu bestimmen (s. EG 76 DS-GVO).[15]

In bestimmten Fällen sind dabei grundlegende Wertungen des Gesetzgebers zu berücksichtigen. Diese können dazu führen, dass für bestimmte Verarbeitungsvorgänge von vornherein von einem hohen – zumindest aber nicht geringen – Risiko auszugehen ist. Dabei sind Korrekturen dieser Wertungen möglich, wenn etwa die Eintrittswahrscheinlichkeit möglicher Schäden gering ist.

1. Von der DS-GVO vorgegebene Risikoeinstufungen

1.1 Daten Minderjähriger

Werden personenbezogene Daten von Minderjährigen bzw. Kindern verarbeitet, was bei schulischen Informationssystemen der Regelfall sein wird, ist zu berücksichtigen, dass Kindern nach der DS-GVO besonders zu schützen sind (vgl. EG 38, 58 Satz 4 DS-GVO, Art. 6 Abs. 1 UAbs. 1 lit. f., Art. 8, Art. 12 Abs. 1 Satz 1 DS-GVO). Mögliche Schäden – seien es Rufschädigungen, wirtschaftliche Nachteile oder Diskriminierungen – können somit besonders schützenswerte Personen betreffen, was von vorherein für eine gewisse Schwere möglicher Schäden und damit für ein mindestens mittleres Risiko derartiger Verarbeitungsvorgänge spricht.[16]

1.2 Besondere Kategorien personenbezogener Daten

Die DS-GVO sieht bei besonderen Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO von vornherein eine gesteigerte Schutzbedürftigkeit vor, „da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und Grundfreiheiten auftreten können“ (EG 51 S. 1 DS-GVO). Bei Verarbeitung derartiger Daten können schwere Schäden entstehen (zu den einzelnen Kategorien und möglichen Schäden s. B.2.6), sodass grundsätzlich von einem hohen Risiko auszugehen ist.[17] Dies gilt – nicht nur, aber insbesondere –, wenn eine umfangreiche Verarbeitung dieser Daten stattfindet (s. die Wertung in Art. 35 Abs. 3 lit. b DS-GVO).

[15] DSK, Kurzpapier Nr. 18, S. 4 f.
[16] S.a. DSK, Kurzpapier Nr. 18, S. 5 und Art.-29-Gruppe, WP 248 Rev. 01, S. 12, die Kinder zu den schutzbedürftigen Personengruppen zählen.
[17] S.a. DSK, Kurzpapier Nr. 18, S. 5 zur gesteigerten Schutzbedürftigkeit derartiger Daten; Art.-29-Gruppe, WP 248 Rev. 01, S. 11.

Indes muss die Verarbeitung besonderer Kategorien personenbezogener Daten – je nach Einzelfall – nicht zwingend mit einem hohen Risiko verbunden sein. Dies gilt insbesondere für Verarbeitungssituationen, in denen die Daten regelmäßig keine konkrete Diskriminierungseignung aufweisen und auch sonst keine gesellschaftlichen Nachteile zu erwarten sind, sodass mögliche Schäden tendenziell nicht als schwerwiegend anzusehen sind. Dies betrifft z. B.:

- Daten, die einen Rückschluss auf Erkrankungen der betroffenen Person zulassen (Gesundheitsdaten, Art. 9 Abs. 1 i.V.m. Art. 4 Nr. 15 DS-GVO), deren Bekanntwerden der betroffenen Person aber regelmäßig nicht unangenehm ist und auch nicht zu Diskriminierungen oder gesellschaftlichen Nachteilen (z. B. einer Stigmatisierung) der betroffenen Person führen. 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).

- Daten, die sich nur auf die Teilnahme oder Nichtteilnahme an Religionsunterricht oder vergleichbarem Weltanschauungsunterricht (z. B. Ethikunterricht) beziehen (Daten über religiöse oder weltanschauliche Überzeugungen i.S.v. Art. 9 Abs. 1 DS-GVO), ohne aber konkrete Aussagen über religiöse oder weltanschauliche Überzeugungen zu ermöglichen.

- Daten, die eine Aussage über die bloße Mitwirkung in schulischen Vertretungsgremien treffen (ggf. Daten über Gewerkschaftszugehörigkeit oder politische Meinungen i.S.v. Art. 9 Abs. 1 DS-GVO), ohne aber konkrete Aussagen über politische Meinungen etc. zu ermöglichen.

- Daten, die lediglich eine Aussage über den Personenstand treffen (obwohl dies i.V.m. Angaben zum Geschlecht des Partners Daten über die sexuelle Orientierung i.S.v. Art. 9 Abs. 1 DS-GVO sein können)[18].

Bei Freifeldern (z. B. Felder, in denen Angaben zu einer Person oder Klasse eingetragen werden können) oder im Rahmen von Freitextaufgaben kann regelmäßig nicht ausgeschlossen werden, dass es zu einer Verarbeitung von Daten i.S.v. Art. 9 DS-GVO kommt. Dies kann z. B. der Fall sein, wenn ein Aufsatz über das schönste Ferienerlebnis geschrieben werden soll, wobei der Besuch bei den Großeltern in Namibia oder Argentinien geschildert wird (ethnische Herkunft), oder wenn in einer Freitextaufgabe abgefragt wird, ob man schon einmal an einer politischen Demonstration teilgenommen hat (politische Meinung). Dies sollte aber für sich gesehen nicht dazu führen, bei Systemen, die Freifelder oder Freitextaufgaben vorsehen, immer von einem hohen Risiko auszugehen. Zum einen sollte geprüft werden, wie wahrscheinlich es ist, dass tatsächlich derartige Informationen eingegeben werden (zu Wahrscheinlichkeit s.a. C.2.). Zum anderen kann z. B. die Pseudonymisierung der Daten, ihre zeitnahe Löschung sowie die Nichtverknüpfung mit anderen Informationen dafür sprechen, nicht von einem hohen Risiko auszugehen (s.a. C.2.4.).

1.3 Systematische und umfassende Bewertung persönlicher Aspekte

Aus Art. 35 Abs. 3 lit. a DS-GVO geht hervor, dass auch bei systematischen und umfassenden Bewertungen persönlicher Aspekte, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen, von einem hohen Risiko auszugehen ist.

2. Schwere und Eintrittswahrscheinlichkeit

2.1 Allgemeine Überlegungen

„Die Eintrittswahrscheinlichkeit eines Risikos beschreibt, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher weiteren Wahrscheinlichkeit es zu Folgeschäden kommen kann“.[19] Es ist also abzuschätzen, wie wahrscheinlich die Verarbeitung zu einem physischen, materiellen oder immateriellen Schaden führt. Da sich das Risikobewertungskonzept insbesondere auf die Gewährleistung der Datensicherheit bezieht, soll-

[18] S. EuGH, Urt. v. 1.8.2022 – C-184/20.
[19] S. DSK, Kurzpapier Nr. 18, S. 4.

ten zur Risikobewertung und somit zur Bewertung der Eintrittswahrscheinlichkeit etablierte Verfahren der Risikoeinstufung bei der IT-Sicherheit (bspw. BSI-Standard 200-3, ISO 31000, ISO/IEC 27005, NIST 800-30) und dem operativen Datenschutz (z. B. SDM oder DSK, Kurzpapier Nr. 18) herangezogen werden.

Eine geringe Eintrittswahrscheinlichkeit kann das Risiko senken. Dies gilt z. B. in den folgenden Fällen:

- Basierend auf der Einschätzung von Fachpersonal und seiner fundierten Erfahrung oder statistischen Bewertungsverfahren wurde festgestellt, dass die Eintrittswahrscheinlichkeit des Risikos gering ist, d.h., es tritt höchstens alle fünf Jahre ein.[20]
- Ein System-Anbieter kann durch (zusätzliche) TOM oder eine Kombination von TOM die Eintrittswahrscheinlichkeit des Risikos absenken. So könnte ein System-Anbieter z. B. Daten über politische Meinungen von Schülerinnen und Schülern verarbeiten. Führt er eine Pseudonymisierung durch, sodass eine Zuordnung der politischen Meinungen zu den individuellen Personen erschwert oder unmöglich gemacht wird, kann dies die Eintrittswahrscheinlichkeit von Schäden reduzieren.
- Die Eintrittswahrscheinlichkeit eines Risikos ist u.a. auch von der Motivation, der Expertise und den Mitteln eines potenziellen Angreifers abhängig. Eine Eintrittswahrscheinlichkeit könnte bspw. als geringfügig eingeschätzt werden, falls ein Angreifer einen erheblichen Aufwand betreiben müsste, um einen Schaden zu erzeugen, der in einem ungenügenden oder keinem Verhältnis zu den potenziellen Gewinnen durch einen erfolgreichen Angriff steht. Zu denken ist z. B. an eine Situation, in der ein Angreifer zwar Sicherheitslücken eines schulischen Informationssystems ausnutzen könnte, um Zugang zu personenbezogenen Daten zu erhalten, ein tatsächlicher Schaden aber nur eintreten würde, wenn der Angreifer bspw. Daten unter Aufwendung erheblicher Anstrengungen verketten kann. Wenn diese Aufwendung des Angreifers aber nicht im Verhältnis zu seinem Gewinn steht, spricht dies dafür, dass es eher unwahrscheinlich ist, dass ein Angreifer diese Maßnahmen umsetzen wird. Ein System-Anbieter kann daher durch die Anwendung von etablierten Bedrohungsanalysen (engl. Threat Modelling[21]) ebenfalls die Eintrittswahrscheinlichkeit von Schäden evaluieren.

Neben der Eintrittswahrscheinlichkeit muss immer auch die Schwere möglicher Schäden beurteilt werden, um über das Risiko zu entscheiden. Sowohl bzgl. Eintrittswahrscheinlichkeit als auch bzgl. Schwere sind Art, Umfang und Umstände der Verarbeitungsvorgänge zu berücksichtigen (EG 76 DS-GVO).

2.2 Art der Datenverarbeitung bzw. der verarbeiteten Daten

Bzgl. der Art der verarbeiteten Daten ist zu berücksichtigen, dass bestimmte Arten von Daten vom Gesetzgeber als besonders schutzbedürftig angesehen werden. Dies betrifft in der DS-GVO die besonderen Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DS-GVO sowie die Daten von Kindern, auf die bereits unter C.1. eingegangen wurde.

Schwere (bzw. hohe) Schäden können aber auch bei Verarbeitung anderer Daten auftreten, etwa bei Daten, die sich auf „verpönte" Merkmale i.S.v. Art. 21 GRCh bzw. Art. 3 Abs. 3 GG beziehen und z. B. für Diskriminierungen genutzt werden können. Auch bei Daten, die die besonders geschützte Privat- oder Intimsphäre betreffen (Art. 7 GRCh), drohen schwere (bzw. hohe) Schäden, wenn z. B. private oder intime Sachverhalte gegen den Willen der betroffenen Person an die Öffentlichkeit gelangen. Dies ist ggf. anders zu beurteilen, wenn die betroffene Person die Daten selbst öffentlich zugänglich gemacht hat.[22]

2.3 Umfang der Datenverarbeitung

Zur Bestimmung des Umfangs der Datenverarbeitung können u.a. die Zahl der betroffenen Personen (konkrete Anzahl oder Anteil der relevanten Personengruppe), die verarbeitete Datenmenge (Quantität), die Bandbreite und Qualität der verarbeiteten Daten, die Dauer der Datenverarbeitung sowie das geografische Ausmaß der Datenverarbeitung berücksichtigt werden.[23]

[20] S. BSI-Standard 200-3, S. 26.
[21] Siehe hierzu auch etablierte Best-Practices wie z. B. STRIDE, DREAD, OCTAVE, oder PASTA.
[22] S. Art.-29-Gruppe, WP 248 Rev. 01, S. 11.
[23] Art.-29-Gruppe, WP 248 Rev. 01, S. 11.

Je umfangreicher die Datenverarbeitung ist, desto höher können mögliche Schäden ausfallen, da insbesondere mehr Personen in intensiver Weise betroffen sein können. Mit dem Umfang der Datenverarbeitung kann zudem die Wahrscheinlichkeit eines Schadenseintritts steigen, da es bei einer Vielzahl von Verarbeitungsvorgängen bzw. einer großen Menge an verarbeiteten Daten eher zu Fehlern, Vorfällen oder Angriffen kommen kann, die zu Schäden führen. Werden etwa in einem schulischen Informationssystem (z. B. einem Identitätsmanagementsystem) nahezu alle Schülerinnen und Schüler und/oder alle Lehrkräfte eines Bundeslandes erfasst, drohen bei einem Sicherheitsvorfallen all diesen Personen Schäden.

Erfolgt die Datenverarbeitung – und insbesondere auch die Speicherung der Daten – über einen langen Zeitraum, steigert dies regelmäßig nicht nur die verarbeitete Datenmenge, sondern führt auch dazu, dass die Daten für einen langen Zeitraum zur Auswertung sowie für sonstige Verarbeitungsvorgänge zur Verfügung stehen. Dies kann z. B. der Fall sein, wenn Daten von Schülerinnen und Schülern über mehrere Schuljahre hinweg erfasst und gespeichert werden und ihre Aussagekraft über die Jahre ansteigt (z. B. durch die Möglichkeit von Aggregation und Verkettung). Je länger die Datenverarbeitung anhält, desto wahrscheinlicher ist es, dass es währenddessen zu einem Schaden kommt. Steigt die Aussagekraft der Daten, kann dies die Schwere möglicher Schäden steigern und z. B. zu tiefgreifenden Beeinträchtigungen der Privatsphäre führen. Werden Daten hingegen nur kurzzeitig verarbeitet und sodann wieder gelöscht, kann dies die Wahrscheinlichkeit eines Schadenseintritts und die Schwere möglicher Schäden senken.

Werden Daten oder Datensätze aus unterschiedlichen Verarbeitungsvorgängen zusammengeführt oder miteinander abgeglichen (s.a. C.1.3. zur systematischen und umfassenden Bewertung), steigt die Aussagekraft der Daten, was wiederum mögliche Schäden vertiefen kann (z. B. weitreichendere Verletzungen der Privatsphäre). Dies spricht für ein hohes Risiko.[24]

2.4 (sonstige) Umstände der Datenverarbeitung

Es sind weitere Umstände denkbar, die die Risikobewertung beeinflussen können. Etwa kann es bei Verwendung neuen Technologien (z. B. Künstlicher Intelligenz) schwierig sein, die tatsächliche Eintrittswahrscheinlichkeit und Schwere möglicher Schäden (z. B. persönlicher oder gesellschaftlicher Schäden) verlässlich abzuschätzen, so dass – im Interesse eines effektiven Schutzes der Rechte und Freiheiten betroffener Personen – zunächst eher von einer hohen Eintrittswahrscheinlichkeit bzw. von hohen Schäden auszugehen ist. Dementsprechend kann die Verwendung neuer Technologien das Risiko der Verarbeitung erhöhen.[25] Eine Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO kann helfen, die Risiken neuer Technologien zu verstehen.[26]

Werden Daten von Personen verarbeitet, die sich in einem Abhängigkeitsverhältnis (zum System-Kunden) befinden, wie dies insbesondere bei Lehrkräften und anderen Mitarbeitenden einer Schule der Fall sein kann, spricht dies ebenfalls für eine erhöhte Schutzbedürftigkeit, die sich in einem erhöhten Risiko niederschlagen kann.[27]

Andererseits kann die Verarbeitung pseudonymisierter Daten das Risiko verringern, indem die Identifizierbarkeit betroffener Personen erschwert wird (etwa wenn ein Angreifer nicht über die zusätzlichen Informationen verfügt, die für eine Zuordnung der Daten zu einer spezifischen Person erforderlich sind, s. Art. 4 Nr. 5 DS-GVO). So können die Wahrscheinlichkeit und Schwere eines Schadens reduziert werden.

Zu den Umständen, die das Risiko eines Schadenseintritts beeinflussen können, gehört auch die Zahl der Personen, die Zugriff auf personenbezogene Daten haben. Ist diese groß, kann dies die Wahrscheinlichkeit, dass es zu einem Schaden kommt, steigern, z. B. durch eine unbefugte Offenlegung.

D. Einordnung und Folgerung

Unter Berücksichtigung gesetzgeberischer Wertungen (C.1.) sowie der Eintrittswahrscheinlichkeit und der Schwere möglicher Schäden (C.2.) hat der System-Anbieter das Risiko für einzelne Verarbeitungsvorgänge zu bestimmen. Je nach Verarbeitungsvorgang kann das Risiko dabei unterschiedlich ausfallen.

[24] Art.-29-Gruppe, WP 248 Rev. 01, S. 12.
[25] S.a. Art. 35 Abs. 1 DS-GVO, der bzgl. eines hohen Risikos u.a. auf die „Verwendung neuer Technologien“ abstellt.
[26] Art.-29-Gruppe, WP 248 Rev. 01, S. 12.
[27] S. DSK, Kurzpapier Nr. 18, S. 5: Beschäftigte als schützenswerte Personengruppe.

Der System-Anbieter hat jeweils zu bestimmen, ob ein geringes, mittleres oder hohes Risiko vorliegt. Dies verlangt kein mathematisch-präzises Vorgehen und kann auch auf einer gleitenden Skala erfolgen. Das ermittelte Risiko ist Grundlage für die Implementierung risikoangemessener TOM. Es ist aber auch in anderen Bereichen, in denen ein Risiko zu ermitteln ist, relevant. Dies betrifft insbesondere

- die Melde und Benachrichtigungspflichten bei Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 und 34 DS-GVO, wobei es aber auf das Risiko der konkreten Verletzung ankommt,
- die Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO und
- den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art. 25 DS-GVO.

Allgemein gilt dabei: „Je höher das Risiko, desto umsichtiger muss die Verarbeitungstätigkeit gestaltet sein und desto wirksamer müssen die entsprechenden konkreten technischen und organisatorische Maßnahmen betrieben, kontrolliert und ggf. verbessert werden.“[28]

Das Risikobewertungskonzept ist nicht abschließend und schließt andere Methoden der Risikoermittlung nicht aus. Daher sind bei der Risikobewertung auch Erwägungen zulässig, die in dem Risikobewertungskonzept nicht aufgeführt werden, solange sie plausibel und nachvollziehbar sind.

[28] SDM, S. 50.

Referenzen

Art.-29-Gruppe, WP 248 Rev.01	Art.-29-Gruppe, WP 248 Rev. 01 Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, 4.10.2017, https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf.
BSI-Standard 200-3	BSI-Standard 200-3. Risikoanalyse auf der Basis von IT-Grundschutz, Version 1.0, Oktober 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2, Stand 13.10.2025.
DSK, Kurzpapier Nr. 18	DSK Kurzpapier 18: Risiko für die Rechte und Freiheiten natürlicher Personen, 26.4.2018, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.
ISO 31000	Risikomanagement - Leitlinien. Stand 2018
Johnson/Adams/Dummins, NMC Horizon Report 2012	Johnson/Adams/Dummins, NMC Horizon Report 2012: Higher Education Edition, https://www.mmkh.de/fileadmin/dokumente/publikationen/horizon_reports/2012HorizonReport_German_final.pdf.
SDM	Standard-Datenschutzmodell, Version 3.1, 14.5.2024, https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf.
Simitis/Hornung/Spiecker gen. Döhmann/*Bearbeiter*	Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht DSGVO/BDSG, 2. Auflage 2025.

directions