eduSeal

Begleitdokument

Erläuterungen zum Zertifizierungsverfahren für System-Anbieter

Stand 01.03.2026

eduSeal

Weitere Begleitdokumente

- Zertifizierungsgegenstand
- Kriterienkatalog
- Risikobewertungskonzept
- Erläuterungen und Umsetzungshinweise

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).

directions

Gefördert vom:

Bundesministerium
für Bildung, Familie, Senioren,
Frauen und Jugend

Autoren

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

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

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

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

Inhaltsverzeichnis

Abkürzungsverzeichnis

DS-GVO	Datenschutz-Grundverordnung (letzte berücksichtigte Änderung: 04.03.2021)
DSK	Datenschutzkonferenz
EDSA	Europäischer Datenschutzausschuss
TOM	technische und organisatorische Maßnahme

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. Einleitung

Das Zertifizierungsverfahren umfasst die sequenziellen Prozessstufen Antrag, Evaluierung, Bewertung, Entscheidung und Bestätigung. Im Anschluss werden fortlaufende Überwachungstätigkeiten durchgeführt:

- Der Antrag steht vor dem eigentlichen Zertifizierungsprozess. Hierbei reicht der antragstellende System-Anbieter alle erforderlichen Informationen im Rahmen des Zertifizierungsantrages, inklusive der Darstellung und Abgrenzung des Zertifizierungsgegenstands, ein. Die Zertifizierungsstelle bewertet den Antrag.
- Die Evaluierung umfasst im Sinne des funktionalen Ansatzes Tätigkeiten zur Auswahl (u.a. Festlegung des Zertifizierungsgegenstandes, Wahl von Stichproben) und Ermittlung (u.a. Durchführung von Prüfungen) sowie zur Übernahme bestehender Zertifikate.
- Durch eine Bewertung verifizieren die Entscheider der Zertifizierungsstelle, ob die Auswahl-, Ermittlungs- und Übernahmetätigkeiten und deren Ergebnisse hinsichtlich der Erfüllung der festgelegten Zertifizierungskriterien durch die Verarbeitungsvorgänge geeignet, angemessen und wirksam sind.
- Die Entscheider fällen im Anschluss eine Entscheidung über die Erteilung der Zertifizierung, auf Grundlage der Evaluierung und der Bewertung.
- Bei der Bestätigung erteilt die Zertifizierungsstelle die Konformitätszeichen (insb. Gütesiegel und Zertifikat) als Nachweis, dass die Erfüllung festgelegter Anforderungen nachgewiesen wurde und stellt die Zertifizierungsdokumentation bereit.
- Eine Überwachung umfasst systematische, sich wiederholende Konformitätsbewertungstätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit einer Konformitätsaussage.

Damit die Zertifizierungsstelle ein ordnungsgemäßes Zertifizierungsverfahren durchführen kann, muss der System-Anbieter bei der Vorbereitung auf die Zertifizierung folgende drei Schritte beachten und umsetzen:

1) Festlegung und Beschreibung der zu zertifizierenden Verarbeitungsvorgänge (d.h. den Zertifizierungsgegenstand),
2) Festlegung der Nichtanwendbarkeit von Kriterien und
3) Durchführung einer Selbstbewertung und Abgabe einer Stellungnahme zur Erfüllung der Zertifizierungskriterien.

B. Festlegung und Beschreibung der zu zertifizierenden Verarbeitungsvorgänge

Der System-Anbieter legt den zu zertifizierenden Verarbeitungsvorgang bzw. das Bündel von Verarbeitungsvorgängen eigenständig fest. Dabei sind die Angaben zum Zertifizierungsgegenstand im Kriterienkatalog sowie dem Begleitdokument zum Zertifizierungsgegenstand zu beachten. Insbesondere werden keine Systeme, sondern Verarbeitungsvorgänge zertifiziert.

Der System-Anbieter legt der Zertifizierungsstelle dar, was Gegenstand der Zertifizierung und somit zu prüfen ist. Hierzu muss der System-Anbieter eine Dokumentation erstellen, welche eine detaillierte Beschreibung des Zertifizierungsgegenstands enthält (vgl. auch Art. 42 Abs. 6 DS-GVO). Dabei sind mindestens die folgenden Angaben zu machen:[1]

a) die Benennung und detaillierte (Funktions-)Beschreibung der Verarbeitungsvorgänge innerhalb eines schulischen Informationssystems, die zu zertifizieren sind, sowie die detaillierte Beschreibung aller Bestandteile der relevanten Verarbeitungsvorgänge, sodass eine abgeschlossene Verfahrensstruktur gewährleistet wird;

b) die Benennung der Zwecke, die mit den Verarbeitungsvorgängen abgedeckt werden, und die Erläuterung, weshalb diese Verarbeitungsvorgänge zur Erreichung der Zwecke erforderlich sind;

c) die Benennung eventueller Empfänger bzw. Kategorien von Empfängern in den Verarbeitungsvorgängen[2];

d) die Beschreibung, welche Daten im Zusammenhang mit dem Zertifizierungsgegenstand verarbeitet werden, und

   i. welche Daten davon besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO sind;

   ii. welche Daten sich auf strafrechtliche Verurteilungen und Straftaten nach Art. 10 DS-GVO beziehen;

   iii. welche Daten sich auf Minderjährige im Sinne der DS-GVO beziehen;

e) Informationen bezüglich aller Verarbeitungsvorgänge, in denen (Sub-)Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO eingebunden sind. Hierbei müssen die von ihnen übernommenen Zuständigkeiten und damit verbundenen Aufgaben benannt werden;

f) Informationen bezüglich aller Verarbeitungsvorgänge, in denen eine gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO gegeben ist;

g) eine auch in Hinblick auf die Verantwortlichkeit qualifizierte Darstellung des gesamten nach Phasen geordneten Verarbeitungsprozesses sowie des jeweiligen Akteurs- und Rollenmodells (Akteure, Rollen, Beziehungen) für jede Verarbeitungsphase. Hierbei ist insbesondere die Darstellung der Schnittstellen und Übergänge zu anderen Systemen und Organisationen zu beachten. Die qualifizierte Darstellung des Verarbeitungsvorgangs kann entweder durch eine grafische Darstellung (z. B. anhand standardisierter Darstellungsformen wie Business Process Modeling oder Unified Modelling Language) oder in textlicher

[1] DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, S. 4 ff.
[2] Art. 4 Nr. 9 DS-GVO definiert einen Empfänger als „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht“. Empfänger könnten bspw. Auftragsverarbeiter, Werbepartner oder andere System-Anbieter sein.

Form erfolgen. Datenflussdiagramme oder Netzpläne können ebenfalls hilfreich zur Darstellung sein;

h) Angabe, ob eine Übermittlung personenbezogener Daten

   i. außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums oder

   ii. an internationale Organisationen erfolgt.

   Dabei muss beachtet werden, dass es in der Praxis häufig zu derartigen Drittlandtransfers bei der Übermittlung von Daten im Rahmen von Wartung, Pflege und Supports kommt. Zu prüfen sind auch Weiterübermittlungen durch (Sub-)Auftragsverarbeiter;

i) Darstellung der eingesetzten Technik, IT-Landschaft und organisatorische Prozesse zur Durchführung der Verarbeitungsvorgänge, dazu zählen insbesondere relevante IT-Systeme, und das Zusammenspiel zwischen Technik und organisatorischen Prozessen. Systeme, die nicht relevant für die Verarbeitungsvorgänge sind, sollten explizit benannt und ausgeschlossen werden (z. B. Systeme für das eigene Unternehmen oder Sever, welche nicht für die Datenverarbeitung relevant sind);

j) falls die Datenverarbeitungsvorgänge an verschiedenen Standorten durchgeführt werden, so muss der System-Anbieter alle Standorte benennen und entsprechende Informationen zu den Standorten bereitstellen (darunter u.a. eine Beschreibung der Tätigkeiten an den Standorten, rechtliche und vertraglichen Regelungen für jeden Standort, die Schnittstellen zwischen den verschiedenen Standorten).

Zur Erstellung der Dokumentation wird auf folgende Hilfestellungen hingewiesen:

- Begleitdokument Zertifizierungsgegenstand
- EDSA, Leitlinien 1/2018, Ziffer 5.2., inkl. Beispiele zur Beschreibung des Gegenstands
- DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Nr. 2.1.1 und 2.1.2

Der System-Anbieter legt in der Regel die Dokumentationen zur Festlegung und Beschreibung des Zertifizierungsgegenstands der Zertifizierungsstelle vor. Es wird empfohlen, dass die Dokumentation durch die Geschäftsleitung und den Datenschutzbeauftragten des System-Anbieters validiert und freigegeben wird.

C. Festlegung der Nichtanwendbarkeit von Kriterien

In der Regel werden nicht alle Kriterien des Kriterienkatalogs für jeden Zertifizierungsgegenstand anwendbar sein. Verarbeitungsvorgänge sowie implementierte TOM unterscheiden sich von Verarbeitungsvorgang zu Verarbeitungsvorgang bzw. von System-Anbieter zu System-Anbieter. Der System-Anbieter muss daher für den Zertifizierungsgegenstand festlegen, ob einzelne Zertifizierungskriterien nicht anwendbar sind. Dabei ist es wichtig, dass sich die Bewertung der Nichtanwendbarkeit auf die Spezifika des konkreten Zertifizierungsgegenstandes (d.h. der zu zertifizierenden Verarbeitungsvorgänge in einem schulischen Informationssystem) bezieht und bei vergleichbaren Zertifizierungsverfahren und Sachverhalten die gleiche Entscheidung hinsichtlich der Nichtanwendbarkeit getroffen wird, um eine mögliche Willkür bei der Bewertung zu unterbinden. Eine pauschale oder generalisierte Festlegung der Nichtanwendbarkeit von Kriterien ist nicht möglich. Aus diesem Grund regelt das eduSeal-Konformitätsbewertungsprogramm als maßgebliche

Verfahrensordnung für die Zertifizierung die Voraussetzungen und das Verfahren zur Feststellung und Beurteilung der Nichtanwendbarkeit von Kriterien.

Der System-Anbieter muss eine dokumentierte Prüfung durchführen, um festzustellen, welche Zertifizierungskriterien abhängig vom jeweiligen, spezifischen Zertifizierungsgegenstand anwendbar sind. Der System-Anbieter dokumentiert die Einschätzung der Nichtanwendbarkeit von Zertifizierungskriterien nachvollziehbar. Dies bedeutet, dass mindestens für jedes nichtanwendbare Kriterium eine hinreichende Begründung für die Nichtanwendbarkeit angegeben werden muss.

Der System-Anbieter stellt die Dokumentation zur Nichtanwendbarkeit der Zertifizierungsstelle zur Verfügung. Die Zertifizierungsstelle prüft anschließend die Begründungen des System-Anbieters. Dabei stellt die Zertifizierungsstelle sicher, dass die Nichtanwendbarkeit begründet und bei ähnlichen schulischen Informationssystemen vergleichbar gehandhabt wird. Kriterien, die als nicht anwendbar deklariert wurden, werden im Rahmen der Zertifizierung nicht überprüft. Alle nicht anwendbaren Kriterien werden im Zertifikat kenntlich gemacht, um die Transparenz im Markt und insbesondere für System-Kunden zu erhöhen. Bestehen Zweifel an der Nichtanwendbarkeit eines Kriteriums durch die Zertifizierungsstelle, wirkt der System-Anbieter auf die Auflösung von Unklarheiten hin. Hierzu stellt der System-Anbieter unter anderem weitere Dokumente und Erläuterungen bereit.

Grundsätzlich ist ein Kriterium nicht anwendbar, wenn die spezifischen Verarbeitungsvorgänge des System-Anbieters nicht in den Anwendungsbereich des Kriteriums fallen. Dies ist der Fall, wenn der System-Anbieter bestimmte Verarbeitungsvorgänge nicht vornimmt bzw. sein System bestimmte Funktionalitäten nicht aufweist, die Voraussetzung dafür sind, dass ein Kriterium anwendbar ist.

Für den System-Anbieter als Auftragsverarbeiter kann dies insbesondere die folgenden Kriterien betreffen, die ggf. nicht anwendbar sind:

- Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Nr. 2.1), wenn das Gesetz einen Datenschutzbeauftragten nicht vorschreibt (Nr. 2.1 Abs. 1-4) und der System-Anbieter aus diesem Grund nicht über einen solchen verfügt.
- Subauftragsverhältnis (Nr. 13), wenn der System-Anbieter keine Subauftragsverarbeiter einschaltet.
- Datenübermittlung an Drittstaaten und internationale Organisationen (Nr. 14):
    - Wenn der System-Anbieter keine personenbezogenen Daten an Drittstaaten oder internationale Organisationen übermittelt, ist Nr. 14.1 nicht anwendbar. Das Vorliegen einer solchen Übermittlung darf nicht vorschnell ausgeschlossen werden, da es z. B. im Rahmen von Wartung, Pflege und Support häufig zu Drittlandübermittlungen kommt.
    - Wenn der System-Anbieter in der EU oder dem EWR niedergelassen ist, ist Nr. 14.2 nicht anwendbar.
- Videokonferenzsysteme und andere digitale Kommunikationssysteme (Nr. 15), wenn der System-Anbieter keine Videokonferenzsysteme oder andere digitale Kommunikationssysteme anbietet.
- Identitätsmanagement (Nr. 16), wenn der System-Anbieter kein Identitätsmanagement anbietet.

- Digitale Klassenbücher (Nr. 17), wenn der System-Anbieter kein digitales Klassenbuch anbietet.

Für den System-Anbieter als Verantwortlichen kann dies insbesondere die folgenden Kriterien betreffen, die ggf. nicht anwendbar sind:

- Gemeinsame Verantwortlichkeit (Nr. 3), wenn der System-Anbieter nicht mit einem anderen Verantwortlichen gemeinsam Verantwortlicher ist.
- Benennung, Stellung und Aufgaben eines Datenschutzbeauftragten (Nr. 4.1), wenn das Gesetz einen Datenschutzbeauftragten nicht vorschreibt (s. Nr. 4.1 Abs. 1-4) und der System-Anbieter aus diesem Grund nicht über einen solchen verfügt.
- Auftragsverarbeiter des System-Anbieters (Nr. 8), wenn der System-Anbieter keine Auftragsverarbeiter einschaltet.
- Datenübermittlung an Drittstaaten und internationale Organisationen (Nr. 9):
    - Wenn der System-Anbieter keine personenbezogenen Daten an Drittstaaten oder internationale Organisationen übermittelt, ist Nr. 9.1 nicht anwendbar. Das Vorliegen einer solchen Übermittlung darf nicht vorschnell ausgeschlossen werden, da es z. B. im Rahmen von Wartung, Pflege und Support häufig zu Drittlandübermittlungen kommt.
    - Wenn der System-Anbieter in der EU oder dem EWR niedergelassen ist, ist Nr. 9.2 nicht anwendbar.
- Videokonferenzsysteme und andere digitale Kommunikationssysteme (Nr. 10), wenn der System-Anbieter keine Videokonferenzsysteme oder andere digitale Kommunikationssysteme anbietet.

Die Nichtanwendbarkeit ist stets zu begründen, wobei auf die Umstände der konkreten Verarbeitungsvorgänge bzw. des konkreten schulischen Informationssystems Bezug zu nehmen ist. Es ist ferner zu beachten, dass Änderungen bei den Verarbeitungsvorgängen oder den Funktionalitäten des schulischen Informationssystems dazu führen können, dass ehemals nicht anwendbare Kriterien aufgrund der Änderung anwendbar werden. Schaltet z. B. der System-Anbieter in der Rolle als Auftragsverarbeiter erstmals einen Subauftragsverarbeiter ein, müssen die Kriterien in zu Subauftragsverhältnissen eingehalten werden. Bei Änderungen am schulischen Informationssystem und/oder dessen Verarbeitungsvorgängen ist grundsätzlich die Zertifizierungsstelle zu informieren.[3] Diese prüft die Änderungen und führt anschließend geeignete Maßnahmen durch. Hierzu zählt auch die Anordnung einer Zwischenprüfung von weiteren Kriterien, welche aufgrund der Änderung nun anwendbar sind, sowie das Aussetzen der Zertifizierung.

[3] Weiterführende Regelungen und Vorgaben sind im Konformitätsbewertungsprogramm für die Zertifizierungsstelle enthalten. Der System-Anbieter schließt in der Regel eine Zertifizierungsvereinbarung mit der Zertifizierungsstelle, welche alle Rechte und Pflichten im Rahmen der Zertifizierung festhält. Darunter z. B. auch die Pflicht von System-Anbietern, wesentliche Änderungen der Zertifizierungsstelle mitzuteilen.

D. Durchführung einer Selbstbewertung und Abgabe einer Stellungnahme zur Erfüllung der Zertifizierungskriterien

Der System-Anbieter führt vor der Zertifizierung eine eigenständige Bewertung durch, bei der er feststellt, dass alle Kriterien dieses Kriterienkatalogs eingehalten werden. Werden Mängel oder Abweichungen festgestellt, werden diese vom System-Anbieter unverzüglich behoben.

Um sich bestens auf die Zertifizierung vorzubereiten, erstellt der System-Anbieter auf Grundlage der Selbstbewertung eine detaillierte Stellungnahme zur Erfüllung der Zertifizierungskriterien. Diese Stellungnahme sollte dediziert für jedes Zertifizierungskriterium korrekt und vollständig darstellen, wie der System-Anbieter das Kriterium umsetzt. Die Darstellung sollte dabei differenziert für die Unterpunkte des jeweiligen Kriteriums durchgeführt werden. Die Stellungnahme kann eine Referenzierung zu der entsprechenden Dokumentation (bspw. Prozessdokumentation, Logs, Intranet, Wiki etc.) oder Systeme enthalten. Falls eine Zertifizierungsstelle eine elektronische Vorlage zur Stellungnahme zur Unterstützung der System-Anbieter anbietet, sollte diese genutzt werden. Die Stellungnahme sollte dann der Zertifizierungsstelle vorgelegt werden.

Eine solche Selbstbewertung der Einhaltung der Kriterien durch den System-Anbieter vor der Durchführung eines Zertifizierungsverfahren ist zwingend erforderlich. Dadurch werden die Erfolgschancen für ein Zertifizierungsverfahren und dessen Wirtschaftlichkeit erhöht. Die Stellungnahme ist ein zentrales Dokument für das Zertifizierungsverfahren, welches die Zertifizierungsstelle zur Planung der Evaluierungstätigkeiten benötigt. Wichtig ist dabei zu beachten, dass eine Zertifizierungsstelle in der Regel keine Beratungsdienstleistungen für System-Anbieter durchführen kann, die ihre Unabhängigkeit oder Unparteilichkeit gefährden.

Referenzen

DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme	DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme. Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6), Version 3.0 (17.11.2025), https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2025/2025-DSK-Zertifizierungskriterien-Version_3.0.pdf.
EDSA, Leitlinien 1/2018	EDSA, Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679, 4.6.2019, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_de_0.pdf.

directions