directions

KIT Karlsruher Institut für Technologie

UNIKASSEL VERSITÄT

datenschutz cert

Trusted Cloud

Personenbezogene Daten:
Besonderer Schutz für Kinder und Jugendliche
- Datenschutzzertifizierung im Bildungssektor -

Forschungsprojekt DIRECTIONS

Data Protection Certification for Educational Information Systems

Berlin, den 21. Januar 2026

www.directions-cert.de

DLR-PT

OER-Strategie

Gefördert vom:

Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend

DIRECTIONS

- Ziel des Forschungsprojekts DIRECTIONS ist die Konzeptionierung, exemplarische Umsetzung und Erprobung einer nachhaltig anwendbaren Datenschutzzertifizierung für schulische Informationssysteme.
- Warum ? – siehe die Diskussionen zu Corona-Zeiten

Rechtlicher Rahmen für die Zertifizierung

- Rechtliche Vorgaben zur Zertifizierung: Art. 42, 43 DS-GVO + § 39 BDSG
- Zertifizierung als „Element“ / „Faktor“ zum Nachweis dafür, dass DS-GVO bei Verarbeitungsvorgängen von Verantwortlichen / Auftragsverarbeitern eingehalten wird
- Der Zertifizierungsgegenstand beschreibt das zu überprüfende datenschutzkritische Untersuchungsobjekt auf Basis der Zertifizierungskriterien

Was wird zertifiziert?

Ansicht 1: Produkte

ErwG 100 DS-GVO:

„Um die Transparenz zu erhöhen und die Einhaltung dieser Verordnung zu verbessern, sollte angeregt werden, dass Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen eingeführt werden, die den betroffenen Personen einen raschen Überblick über das **Datenschutzniveau einschlägiger Produkte und Dienstleistungen** ermöglichen."

Ansicht 2: Datenverarbeitungsvorgänge

Art. 42 Abs. 1 S. 1 DS-GVO:

„Die Mitgliedstaaten, die Aufsichtsbehörden, der Ausschuss und die Kommission fördern insbesondere auf Unionsebene die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dazu dienen, nachzuweisen, dass diese Verordnung **bei Verarbeitungsvorgängen** von Verantwortlichen oder Auftragsverarbeitern eingehalten wird."

Zertifizierungsgegenstand

✓ Teil des Projekts

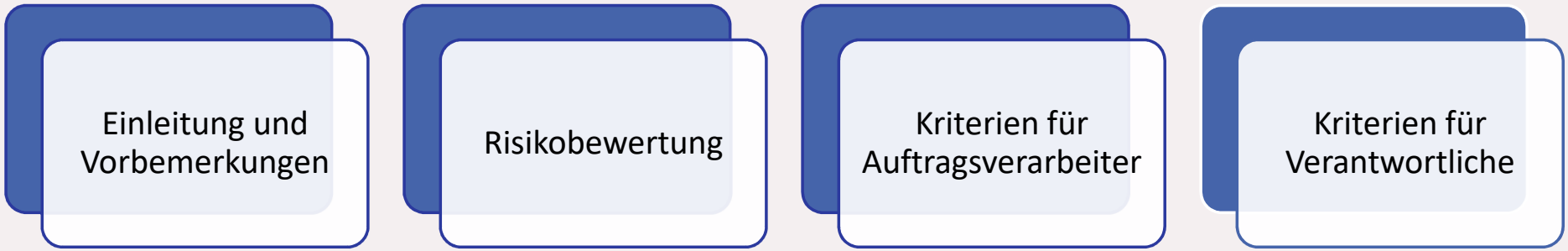
- ✓ Schutz der Daten von Schülern
- ✓ Ggf. indirekter Schutz der Daten von Lehrkräften (Lehrkräfte im digitalen Klassenzimmer)
- ✓ Use Cases der Schüler-zu-Schüler und Schüler-zu-Lehrkräfte Interaktion
- ✓ Zertifizierung nach den Kriterien der DS-GVO und Berücksichtigung weiter einschlägiger Regularien
- ✓ Auch im sog. Nachmittagsmarkt

✗ Nicht Teil des Projekts

- ❖ Zertifizierung von Schulen / Nutzern
- ❖ Schutz der Daten von Eltern
- ❖ Use Cases zur Interaktion von Lehrkräften untereinander
- ❖ Use Cases zur Interaktion von Lehrkräften mit Eltern
- ❖ Berücksichtigung von Anforderungen, die über die DSGVO hinaus gehen
- ❖ Eingesetzte Sub-Auftragsverarbeiter
- ❖ Beschaffungsprozesse durch die Länder
- ❖ Europäisierung / EU Ebene

Bedeutung und Aufbau des Kriterienkatalogs

- Wesentlicher Faktor für System-Anbieter, um die Vereinbarkeit ihrer Datenverarbeitungsvorgänge insbesondere mit der DS-GVO nachzuweisen
- Aufbau des Dokuments zum Kriterienkatalog:



Bedeutung und Aufbau des Kriterienkatalogs

Wesentlicher Faktor für System-Anbieter, um die Vereinbarkeit ihrer Datenverarbeitungsvorgänge insbesondere mit der DS-GVO nachzuweisen
Aufbau des Dokuments zum Kriterienkatalog:

Kriterienkatalog mit einzelnen Kapiteln
Kapitel D Kriterien für Systemanbieter als Auftragsverarbeiter

Fokus auf Anforderungen der DS-GVO

&

Berücksichtigung Spezifika der Bundesländer

1. Rechtsverbindliche Vereinbarung über die Auftragsverarbeitung
2. Pflichten des System-Anbieters
3. Subauftragsverarbeitung
4. Datenverarbeitung außerhalb der EU und des EWR
5. Ergänzende Anforderungen an spezifische Arten von schulischen Informationssystemen
6. Werbe- und Cookieverbot
7. Anforderungen an die Systemgestaltung

Spezifische Regelungen SchulG

Nr. 5.5 – Löschung und Aufbewahrung (Art. 28 Abs. 1 und 3 UAbs. 2 i.V.m Art. 29 DS-GVO)

- (1) Der Prozess i.S.v. Nr. 5.1 Abs. 2 muss insbesondere sicherstellen, dass die Mitarbeitenden erkennen können, wenn die Verarbeitung offensichtlich gegen Löschungs- und/oder Aufbewahrungspflichten der Schulen, Schul-behörden und Schulträger, gegen Berichtigungspflichten und gegen Pflichten auf Gewährung von Einsicht verstößt.
- (2) Ist der System-Anbieter der Auffassung, dass eine Weisung des System-Kunden sowie die darauf beruhende Verarbeitung mit Blick auf Löschungs-, Aufbewahrungs-, Berichtigungs- und Einsichtspflichten rechts-widrig ist, informiert er den System-Kunden nach Nr. 5.1 und dokumentiert dies.

Erläuterung

- Den Schulen, Schulbehörden und Schulträgern als Verantwortliche und System-Kunden werden durch die für den Bereich der Schule relevanten landesgesetzlichen Regelungen verschiedene Pflichten auferlegt. Hierzu gehören die Einhaltung von Lösch- und Aufbewahrungspflichten, Berichtigungspflichten sowie die Erfüllung gesetzlicher Pflichten zur Gewährung von Einsichtnahmen. Zur Erfüllung dieser Pflichten ist der System-Kunde auf die Mitwirkung des System-Anbieters als Auftragsverarbeiter angewiesen, da der System-Anbieter häufig einen besseren Einblick in die relevanten Verarbeitungsvorgänge sowie Zugriff auf die ggf. benötigten technischen Einrichtungen hat. Daher muss sich der System-Anbieter in der rechtsverbindlichen Vereinbarung über die Auftragsverarbeitung dazu verpflichten, bei der Erfüllung dieser Pflichten mitzuwirken. Diese Mitwirkungspflichten des System-Anbieters ändern indes nichts an der Pflicht des System-Kunden, die genannten Pflichten einzuhalten. Eine Pflichtendelegation vom System-Kunden auf den System-Anbieter findet nicht statt. Der System-Anbieter hat den System-Kunden aber nach Kräften bei der Wahrnehmung der Pflichten zu unterstützen. …..

Landesgesetzliche Regelungen

- Vorgaben zur Löschung, Aufbewahrung, Berichtigung und Einsichtnahme finden sich insbesondere in den folgenden in landesrechtlichen Vorschriften (Stand: Juni 2025). Soweit in einzelnen Ländern keine spezifischen schuldatenschutzrechtlichen Vorschriften bestehen, gelten die allgemeinen datenschutzrechtlichen Vor-schriften (insbesondere die DS-GVO und die ergänzenden allgemeinen Landesdatenschutzgesetze).
- Baden-Württemberg: § 115 Abs. 3a SchulG BW; Ziffer 1.5, Ziffer 2.5.3. VwV-Datenschutz an öffentlichen Schulen BW (Löschung und Löschfristen); Ziffer 2.6. VwV-Datenschutz an öffentlichen Schulen BW (Einsichtnahme in Prüfungsarbeiten); Ziffer 3.2 VwV-Datenschutz an öffentlichen Schulen BW (Löschung von Daten von Lehrkräften).
- Bayern: § 40 BaySchO (Aufbewahrungsfristen); § 41 BaySchO (Einsichtnahme); Art. 85a Abs. 4, Art. 113a Abs. 4, Art. 113b Abs. 4 Satz 2, Art. 113c Abs. 3 Satz 9 BayEUG (Löschung).
- …….

Nr. 12 – Werbe- und Cookieregelungen
(Art. 25 Abs. 2, Art. 5 Abs. 1 lit. b DS-GVO sowie Art. 95 DS-GVO)

- Kriterium
- (1) Personenbezogene Daten von Schülerinnen und Schülern sowie sonstigen System-Nutzern dürfen zu Zwecken der Werbung oder zu anderen kommerziellen Zwecken nur auf Grundlage einer dokumentierten ausdrücklichen Einwilligung verwendet werden.
- (2) Die Speicherung von Informationen auf Endgeräten der System-Nutzer oder der Zugriff auf Informationen, die bereits in den Endgeräten gespeichert sind, ist nur zulässig, wenn die Speicherung oder der Zugriff unbedingt erforderlich ist, um das schulische Informationssystem betreiben zu können, oder eine dokumentierte ausdrückliche Einwilligung des Endnut-zers vorliegt. Der System-Anbieter hat durch TOM sicherzustellen, dass ei-ne Speicherung nicht erforderlicher Informationen auf dem Endgerät des System-Nutzers unterbleibt.

Kriterienkatalog mit einzelnen Kapiteln
Kapitel E Systemanbieter als Verantwortlicher

Fokus auf Anforderungen der DS-GVO

Berücksichtigung Spezifika der Bundesländer

1. Datenschutzgrundsätze, Rechtsgrundlage und Verantwortlichkeit
2. Pflichten des System-Anbieters
3. Auftragsverarbeitung
4. Datenverarbeitung außerhalb der EU und des EWR
5. Ergänzende Anforderungen an spezifische Arten von schulischen Informationssystemen
6. Werbe- und Cookieregelungen
7. Anforderungen an die Systemgestaltung

Aktueller Stand: Selbstverpflichtungserklärung (SVE)

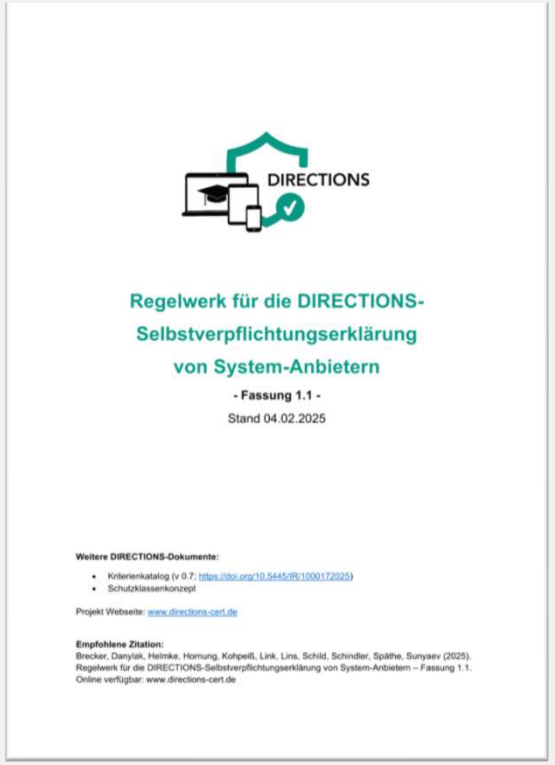
1. Ausbaustufe von DIRECTIONS

Selbstverpflichtungserklärung

- Übergangsinstrument bis zur Zertifizierung
- System-Anbieter stellt Erklärung aus, dass er konform zu den DIRECTIONS-Kriterien ist
- Regelwerk entwickelt, basierend auf ISO/IEC 17050
- Erfordert eigene Bewertung durch Anbieter
- Unterstützung bei der eigenen Bewertung durch externe Prüfstellen möglich

Erprobung des Kriterienkatalogs

- Ausgewählte System-Anbieter prüfen sich selbst anhand des Katalogs
- Hilfestellung für System-Anbieter im Rahmen der Erprobung
- Anschließend stellt System-Anbieter die Erklärung aus, insofern die Kriterien eingehalten werden
- Lessons Learned für den Kriterienkatalog


DIRECTIONS

Regelwerk für die DIRECTIONS-Selbstverpflichtungserklärung von System-Anbietern

- Fassung 1.1 -

Stand 04.02.2025

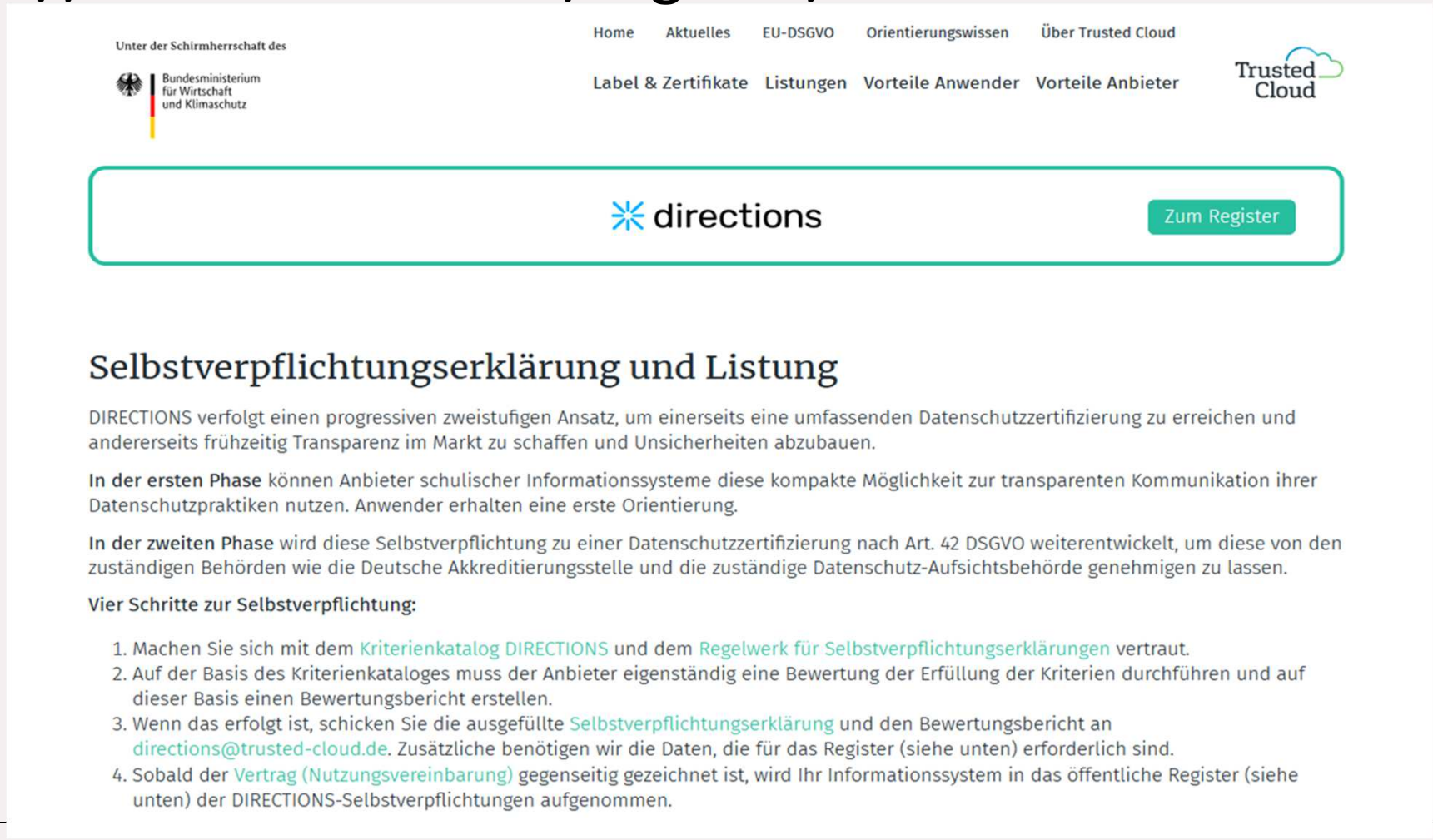
Weitere DIRECTIONS-Dokumente:

- Kriterienkatalog (v 0.7; https://doi.org/10.5445/IR/1000172025)
- Schutzklassenkonzept

Projekt Webseite: www.directions-cert.de

Empfohlene Zitation:
Brecker, Danylak, Helmke, Hornung, Kohpeiß, Link, Lins, Schild, Schindler, Späthe, Sunyaev (2025). Regelwerk für die DIRECTIONS-Selbstverpflichtungserklärung von System-Anbietern – Fassung 1.1. Online verfügbar: www.directions-cert.de

https://trusted-cloud.de/register/



Unter der Schirmherrschaft des
Bundesministerium für Wirtschaft und Klimaschutz

Home Aktuelles EU-DSGVO Orientierungswissen Über Trusted Cloud
Label & Zertifikate Listungen Vorteile Anwender Vorteile Anbieter

Trusted Cloud

directions Zum Register

Selbstverpflichtungserklärung und Listung

DIRECTIONS verfolgt einen progressiven zweistufigen Ansatz, um einerseits eine umfassenden Datenschutzzertifizierung zu erreichen und andererseits frühzeitig Transparenz im Markt zu schaffen und Unsicherheiten abzubauen.

In der ersten Phase können Anbieter schulischer Informationssysteme diese kompakte Möglichkeit zur transparenten Kommunikation ihrer Datenschutzpraktiken nutzen. Anwender erhalten eine erste Orientierung.

In der zweiten Phase wird diese Selbstverpflichtung zu einer Datenschutzzertifizierung nach Art. 42 DSGVO weiterentwickelt, um diese von den zuständigen Behörden wie die Deutsche Akkreditierungsstelle und die zuständige Datenschutz-Aufsichtsbehörde genehmigen zu lassen.

Vier Schritte zur Selbstverpflichtung:

1. Machen Sie sich mit dem Kriterienkatalog DIRECTIONS und dem Regelwerk für Selbstverpflichtungserklärungen vertraut.
2. Auf der Basis des Kriterienkataloges muss der Anbieter eigenständig eine Bewertung der Erfüllung der Kriterien durchführen und auf dieser Basis einen Bewertungsbericht erstellen.
3. Wenn das erfolgt ist, schicken Sie die ausgefüllte Selbstverpflichtungserklärung und den Bewertungsbericht an directions@trusted-cloud.de. Zusätzliche benötigen wir die Daten, die für das Register (siehe unten) erforderlich sind.
4. Sobald der Vertrag (Nutzungsvereinbarung) gegenseitig gezeichnet ist, wird Ihr Informationssystem in das öffentliche Register (siehe unten) der DIRECTIONS-Selbstverpflichtungen aufgenommen.

Ausblick

Ablauf des Genehmigungsprozesses

1 Entwicklung

Entwicklung Kriterien

- Rechtliche Anforderungen
- DSK-Vorgaben für Kriterien
- EDSA-Vorgaben

Entwicklung KBP

- DSGVO gibt Akkreditierungs-norm vor: ISO/IEC 17065
- DAkkS-Regeln
- DSK-Vorgaben
- EDSA-Vorgaben

2 Programmprüfung

Prüfverfahren DAkkS

- DAkkS prüft
- Ggf. Behebung Abweichungen
- DAkkS erteilt Bescheid

Prüfverfahren Aufsichts-behörden

- Aufsichtsbehörde prüft
- Ggf. Behebung Abweichungen
- Aufsichtsbehörde erteilt Bescheid
- Stellungnahme des EDSA

3 Akkreditierung und Zertifizierung

Akkreditierung Programm

- DAkkS erteilt formellen Bescheid über Akkreditierung des KBP

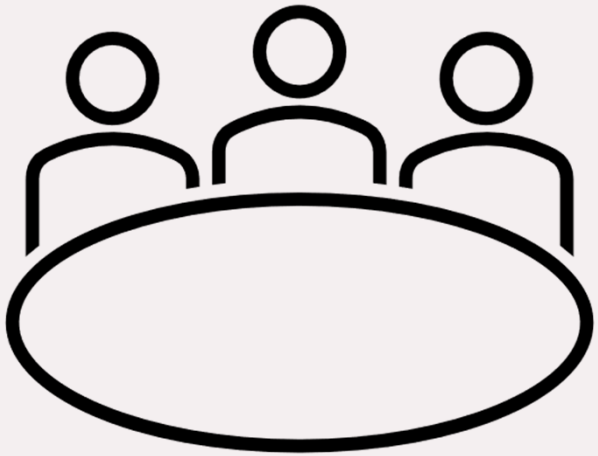
Akkreditierung Zertifizierungs-stellen

- Antrag Zert-stellen auf Akkreditierung nach dem KBP
- Prüfung DAkkS + Aufsichtsbehörde
- Witnessverfahren
- Akkreditierung von Zertstellen

Zertifizierungen

- Zertstellen können Zertifizierungen durchführen

Diskussion



Vielen Dank für Ihre Aufmerksamkeit!