Regelwerk für die DIRECTIONS-Selbstverpflichtungserklärung von System-Anbietern

- Fassung 1.0 -

Stand 01.07.2024

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 (2024). Regelwerk für die DIRECTIONS-Selbstverpflichtungserklärung von System-Anbietern – Fassung 1.0. Online verfügbar: www.directions-cert.de

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

Das Forschungsprojekt DIRECTIONS basiert in Teilen 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

UNIKASSEL VERSITÄT

Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG)

Karlsruher Institut für Technologie (KIT)

CRITICAL INFORMATION INFRASTRUCTURES RESEARCHGROUP

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz neue Fassung (Geltung ab 25.5.18)
BMBF	Bundesministerium für Bildung und Forschung
DSGVO	EU-Datenschutz-Grundverordnung (Geltung ab 25.5.18)
Lit.	litera = Buchstabe
LMS	Lernmanagementsystem
TOM	technische und organisatorische Maßnahmen

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, sodass die grammatikalisch maskuline Form kontextbezogen jeweils als Neutrum zu lesen ist (z. B. ist bei der Bezeichnung *Datenschutzbeauftragter* die Funktionsbezeichnung als Neutrum zu lesen und meint nicht einen ausschließlich maskulinen Personenbezug).

1 Einleitung

Das Forschungsprojekt DIRECTIONS hat sich zum Ziel gesetzt, Instrumente zur Erhöhung des Datenschutzes im Bildungsmarkt und zur Schaffung von Transparenz zu entwickeln. Maßgeblich ist hierbei die Entwicklung einer Datenschutz-Zertifizierung gemäß Art. 42 DSGVO, welche die Konformität von Datenverarbeitungsvorgängen zur Datenschutz-Grundverordnung (DSGVO) bestätigt. Die Entwicklung und anschließende Bewilligung von Zertifizierungsverfahren ist jedoch aufwendig und benötigt Zeit. Aus diesem Grund hat das DIRECTIONS-Projekt als Übergangsinstrument eine Selbstverpflichtungserklärung von System-Anbietern entwickelt.

Die DIRECTIONS-Selbstverpflichtungserklärung ist gemäß ISO/IEC 17050-1:2010 eine Konformitätserklärung eines Anbieters, d. h. eine Bestätigung durch eine erste Stelle. Die DIRECTIONS-Selbstverpflichtungserklärung wird durch den System-Anbieter durchgeführt, welcher die erste Stelle ist und für das Erfüllen der DIRECTIONS-Kriterien verantwortlich ist. Der System-Anbieter stellt die Erklärung aus, um anzuzeigen, dass seine Datenverarbeitungsvorgänge innerhalb seines schulischen Informationssystems zu den festgelegten DIRECTIONS-Kriterien konform sind. Die Grundlage der Erklärung müssen Ergebnisse einer angemessenen Bewertung in Bezug auf die Erfüllung aller Kriterien sein (s. ISO/IEC 17050-1:2010, Nr. 5). Der System-Anbieter ist für die Abgabe, Aufrechterhaltung, Erweiterung, Einschränkung, Aussetzung und Widerruf der Erklärung und für die Konformität des Gegenstandes mit den Kriterien verantwortlich (s. ISO/IEC 17050-1:2010, Nr. 5). Eine Selbstverpflichtungserklärung darf für sich allein oder in Verbindung mit anderen Konformitätsbewertungsverfahren angewendet werden (s. ISO/IEC 17050-1:2010, Nr. 4). Zudem bestätigt der System-Anbieter, dieses Regelwerk für Selbstverpflichtungserklärungen einzuhalten.

Maßgeblich für die Abgabe der Selbstverpflichtungserklärung ist dieses Regelwerk. Es beschreibt die spezifischen Anforderungen, Regeln sowie Verfahren, die zur Abgabe der Selbstverpflichtungserklärung verwendet werden müssen. Dazu zählen die von den System-Anbietern zu erfüllende Grundsätze und weitere Anforderungen an den System-Anbieter zur Durchführung der Bewertung. Das DIRECTIONS-Regelwerk wird durch das Kompetenznetzwerk Trusted Cloud e.V. als Eigner von DIRECTIONS verwaltet und weiterentwickelt. Es wird interessierten System-Anbietern zu nicht-diskriminierenden Bedingungen zur Verfügung gestellt, um eine breite Anwendung von Selbstverpflichtungserklärungen sicherzustellen.

Das Regelwerk gliedert sich in vier wesentliche Kapitel. In Kapitel 2 wird der Zweck der Selbstverpflichtungserklärung festgelegt und zentrale Begriffe definiert. Kapitel 3 regelt die Grundsätze, um unter anderem Vertrauen in die Selbstverpflichtungserklärung zu schaffen. Kapitel 4 legt Anforderungen an den System-Anbieter fest. Kapitel 5 beschreibt Anforderungen an den Bewertungsprozess und die Abgabe der Erklärung.

2 Begrifflichkeiten

2.1 Gegenstand der Selbstverpflichtungserklärung

Gegenstand der Selbstverpflichtungserklärung sind Datenverarbeitungsvorgänge von personenbezogenen Daten in schulischen Informationssystemen.

2.2 Schulische Informationssysteme

Informationssysteme sind soziotechnische Systeme, in denen Technologie zur Verarbeitung von Informationen eingesetzt wird, zum Beispiel zur Unterstützung der Entscheidungsfindung, Koordination, Kontrolle, Analyse und Visualisierung.[1] Wenn Informationssysteme im Bereich der schulischen Bildung zum Einsatz kommen, werden sie als schulische Informationssysteme bezeichnet. Der Bereich der schulischen Bildung umfasst sowohl den Einsatz in der Schule selbst („Vormittagsmarkt“) als auch den privaten Einsatz („Nachmittagsmarkt“ zum Selbststudium etc.).

Schulische Informationssysteme können in Anlehnung an das didaktische Dreieck aus Lernenden, Lehrenden und Inhalten nach fünf Komponenten charakterisiert werden: Inhaltskomponente, Werkzeugkomponente, Beurteilungskomponente, Aufgabenkomponente, und Kommunikationskomponente.[2] Eine Übersicht über mögliche Funktionen für die Komponenten ist in Anhang A aufgeführt. Bei schulischen Informationssystemen kann außerdem zwischen vier Arten unterschieden werden: Lernmanagementsystem, Infrastruktursysteme, Content-Plattform und Lernanwendung. Hierbei handelt es sich um eine typisierende Unterscheidung, d. h. die Arten überlappen teilweise.

- **Lernmanagementsystem (LMS):** Ein LMS dient der Bereitstellung von Lerninhalten und der Organisation bestimmter Lernprozesse. Diese Lernprozesse können Aufgaben- und Beurteilungskomponenten enthalten. Darüber hinaus zeichnen sich LMS häufig durch Funktionen zur Benutzer- und Kursverwaltung (Werkzeugkomponenten) sowie durch Kommunikationskomponenten für den Austausch zwischen Lernende und Lehrenden aus, bspw. Diskussionsforen oder Chats. LMS können webbasiert bereitgestellt werden.[3]

- **Infrastruktursysteme:** Infrastruktursysteme unterstützen die schulische Bildung durch Werkzeugkomponenten und Kommunikationskomponenten. Werkzeugkomponenten ermöglichen die individuelle oder kollektive Verarbeitung von Dokumenten, z. B. auf virtuellen Whiteboards oder durch Dateimanagement-Systeme. Kommunikationskomponenten dienen dem Austausch zwischen Lernenden und Lehrenden, z. B. durch Videokonferenzen, und ermöglichen so ein ‚digitales Klassenzimmer‘.

- **Content-Plattform:** Eine Content-Plattform ermöglicht für Lernende und Lehrende den Umgang mit multimedialen Lerninhalten. Lehrende können Content-Plattformen beispielsweise nutzen, um Lerninhalt zu erstellen, zu bearbeiten, zu teilen, zu erwerben oder bereitzustellen. Content-Plattformen stellen daher in der Regel Inhaltskomponenten und unterstützenden Werkzeugkomponenten bereit.

- **Lernanwendung:** Lernanwendungen ermöglichen Lernenden eigenverantwortliches und interessengeleitetes Lernen durch Aufgaben, Übungen und Lernspiele. Darüber hinaus werden diese Aufgaben meist mit Erklär-Material oder Lernreisen ergänzt. Während Lernanwendungen somit in erster Linie Aufgabenkomponenten- und Inhaltkomponenten beinhalten, können auch

[1] *Laudon/Laudon* 2022, 46.
[2] *Petko,* in Petko 2010, 15–18.
[3] *Totschnig/Willems/Meinel,* Proceedings of the 5th International Conference on Computer Supported Education 2013, 597.

> Beurteilungskomponenten und weitere Werkzeuge enthalten sein. Bereitgestellt werden Lernanwendungen vor allem mit Hilfe mobiler Endgeräte wie Smartphones oder Tablets.[4]

Die Beschreibung dieser Anwendungstypen ist nicht abschließend und kann teilweise Überschneidungen enthalten. So enthalten beispielsweise LMS häufig auch Funktionen, die ähnlich oder gleich denen der Infrastruktursysteme und Content-Plattformen sind.

2.3 System-Anbieter als Datenverarbeiter

System-Anbieter von schulischen Informationssystemen können eine Selbstverpflichtungserklärung zum Datenschutz basierend auf dem DIRECTIONS-Kriterienkatalog abgeben. Der DIRECTIONS-Kriterienkatalog beschreibt die datenschutzrechtlichen Anforderungen an die Verarbeitung von personenbezogenen Daten auf der Seite des System-Anbieters für ein System. Die datenschutzrechtlichen Anforderungen an den System-Kunden oder -Nutzer werden nicht adressiert.

Aussteller der DIRECTIONS-Selbstverpflichtungserklärung sind somit die **System-Anbieter von schulischen Informationssystemen**, die Verarbeitungsvorgänge von personenbezogenen Daten durchführen und dabei entweder als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO und/oder als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO (ggf. in gemeinsamer Verantwortlichkeit mit dem System-Kunden, dann mit den Folgen des Art. 26 DSGVO) auftreten.

Der System-Anbieter ist Auftragsverarbeiter i.S.v. Art. 4 Nr. 8 DSGVO, wenn er die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet. Als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO gilt er, wenn er allein oder gemeinsam mit anderen (dann sind die Anforderungen des Art. 26 DSGVO zu berücksichtigen) über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der System-Kunde wird regelmäßig als datenschutzrechtlich Verantwortlicher auftreten. Der System-Anbieter muss sich seiner Rolle(n) bewusst sein, um die entsprechenden Kriterien des DIRECTIONS-Katalogs auszuwählen.

Weitere Informationen zum Begriff des System-Anbieter sind im DIRECTIONS-Kriterienkatalog (Kapitel A.3) zu finden.

2.4 (Sub-) Auftragsverarbeiter

Regelmäßig werden schulische Informationssysteme nicht in ihrer Gesamtheit höchstpersönlich vom System-Anbieter erbracht, sondern es werden (Sub-)Auftragsverarbeiter für die Leistungserbringung eingesetzt. Einzelne Abschnitte oder Teile eines Datenverarbeitungsvorgangs werden dann an diese delegiert und von ihnen erbracht. Die Genehmigung des System-Kunden zum Einsatz von (Sub-)Auftragsverarbeitern vorausgesetzt (dies ist nach Art. 28 Abs. 2 DSGVO erforderlich), können auf diese Weise mehrstufige (Sub-)Auftragsverhältnisse entstehen.

Weitere Informationen zur Reichweite der Selbstverpflichtungserklärung sind im DIRECTIONS-Kriterienkatalog (Kapitel A.3) zu finden.

2.5 System-Nutzer / System-Kunden

System-Nutzer sind natürliche Personen, deren personenbezogene Daten im schulischen Informationssystem verarbeitet werden, daher vorrangig Schüler, aber auch Lehrkräfte, Mitarbeitende an Schulen und Erziehungsberechtigte. Oftmals spricht man auch von End-Kunden in diesem Zusammenhang.

System-Kunden sind Vertragspartner des System-Anbieters und können eine natürliche oder juristische Person sein. Im Vormittagsmarkt handelt es sich um Schulen, Schulträger, Schulbehörden oder ggfs.

[4] *OeAD* 2022.

Lehrkräfte, im Nachmittagsmarkt vorwiegend um Erziehungsberechtigte oder (volljährige) Schüler. System-Kunden entscheiden über die Verwendung eines schulischen Informationssystems und können die Verantwortlichen der Datenverarbeitungsvorgänge sein.

Weitere Informationen zum Begriff des System-Kunden und -Nutzers sind im DIRECTIONS-Kriterienkatalog (Kapitel A.3) zu finden.

2.6 Konformitätsbewertungsstellen

Die DIRECTIONS-Selbstverpflichtungserklärung wird vom System-Anbieter ausgestellt. Die Grundlage der Erklärung müssen Ergebnisse einer angemessenen Bewertung in Bezug auf die Erfüllung der DIRECTIONS-Kriterien sein (s. ISO/IEC 17050-1:2010, Nr. 5). Diese Bewertung wird vorranging vom System-Anbieter selbst durchgeführt.

Er kann zusätzlich Unterstützung, z.B. durch eine dritte Stelle (z. B. Prüf- oder Kalibrierlaboratorien, Inspektionsstellen, Zertifizierungsstellen), zur Erlangung der Ergebnisse heranziehen (s. ISO/IEC 17050-1:2010, Nr. 5). Diese unterstützenden Stellen werden im Rahmen dieses Regelwerks als Konformitätsbewertungsstellen bezeichnetet. Sie stellen jedoch keine Konformitätsaussage aus, sondern unterstützen lediglich dem System-Anbieter bei seiner eigenen Bewertung in Bezug auf die Einhaltung der DIRECTIONS-Kriterien.

2.7 Interessierte Parteien

Interessierte Parteien stellen Unternehmen, Privatpersonen, Behörden etc. dar, welche Interesse an der Mitgestaltung oder Mitwirkung von DIRECTIONS haben und/oder die Selbstverpflichtungserklärung im Markt wahrnehmen. Interessierte Parteien können insbesondere sein: System-Nutzer und -Kunden von schulischen Informationssystemen, Datenschutz-Aufsichtsbehörden, Teilnehmer im Markt, oder Konformitätsbewertungsstellen.

2.8 Kriterien der Selbstverpflichtungserklärung

Kriterien der Selbstverpflichtungserklärung sind die in dem DIRECTIONS-Kriterienkatalog festgelegten datenschutzrechtlichen Anforderungen, die durch den System-Anbieter gemäß seiner Selbstverpflichtungserklärung als umgesetzt gelten.

2.9 Anforderungen an die Selbstverpflichtungserklärung

Anforderungen an die Selbstverpflichtungserklärung werden im Rahmen dieses Regelwerk beschrieben und legen u.a. fest, was ein System-Anbieter bei der Erklärung beachten muss, auf welchen Ergebnissen die Erklärung beruhen sollte, und welche Inhalte in der Erklärung enthalten sein müssen. Dabei stützen sich die Anforderungen dieses Regelwerks auf die ISO/IEC 17050-1:2010 und ISO/IEC 17050-2:2004.

2.10 Eigner

Der Eigner von DIRECTIONS ist das Kompetenznetzwerk Trusted Cloud e.V. Er ist für die Entwicklung und Aufrechterhaltung dieses Regelwerks verantwortlich. Der Eigner übernimmt die volle Verantwortung für die Ziele, den Inhalt und die Vollständigkeit dieses Regelwerks. Der Eigner pflegt dieses Regelwerk und gibt bei Bedarf Anleitung für System-Anbieter. Dazu werden folgende Aktivitäten ausgeführt:

(1) Durchführung von Änderungen an den festgelegten Kriterien und Anforderungen der Selbstverpflichtungserklärung;
(2) Durchführung von Änderungen an diesem Regelwerk;
(3) Beobachtung von

(a) Änderungen der rechtlichen Rahmenbedingungen, die sich durch Gesetzesnovellierungen, den Erlass delegierter Rechtsakte der Europäischen Kommission, Entscheidungen des Europäischen Datenschutzausschusses und Gerichtsentscheidungen ergeben;
(b) Fortentwicklungen des Stands der Technik;
(c) Änderungen von Anforderungen und Empfehlungen von den Datenschutz-Aufsichtsbehörden und des Datenschutzausschusses mit Relevanz für den Kriterienkatalog und das Regelwerk;
(d) Rechtsakten und anderen Vorgaben von dem Datenschutzausschuss oder den Datenschutz-Aufsichtsbehörden.

(4) Informieren der System-Anbieter bei relevanten bzw. wesentlichen Änderungen;
(5) Koordination von Kooperationen mit Interessengruppen zur Pflege und Weiterentwicklung des Regelwerks und des Kriterienkatalogs;
(6) Beratende Aktivitäten bei allen Fragen der Marktansprache.

Der Eigner stellt sicher, dass Informationen über dieses Regelwerk der Öffentlichkeit zugänglich gemacht werden, um Transparenz, Verständnis und Akzeptanz sicherzustellen. Hierzu werden folgende Maßnahmen durchgeführt:

(1) Veröffentlichung des DIRECTIONS-Kriterienkatalogs mit freiem Zugang für alle Interessengruppen auf einem Internetportal, und
(2) Veröffentlichung dieses Regelwerks mit freiem Zugang für alle Interessengruppen auf einem Internetportal.

3 Grundsätze der Selbstverpflichtungserklärung

3.1 Vertrauen, Zuverlässigkeit und Kompetenz

§ 3.1.1 Vermittlung von Vertrauen

(1) Übergeordnetes Ziel der Selbstverpflichtungserklärung ist es, allen Beteiligten im Markt das Vertrauen zu vermitteln, dass ein System-Anbieter technisch-organisatorische Maßnahmen (TOM) betreibt, um den Datenschutz bei seinen Datenverarbeitungsvorgängen in schulischen Informationssystemen einzuhalten.

(2) Die Selbstverpflichtungserklärung soll insbesondere ein Übergangsinstrument zur Erhöhung des Datenschutzes im Bildungsmarkt sein, bis bewilligte Zertifizierungsverfahren nach Art. 42 DSGVO (oder Verhaltensregeln nach Art. 40 DSGVO) verfügbar sind.

(3) Die Selbstverpflichtungserklärung ermöglicht es System-Anbietern gegenüber dem Markt zu signalisieren, dass ihre Datenverarbeitungsvorgänge den DIRECTIONS-Kriterienkatalog einhalten.

(4) Das Vertrauen in die Selbstverpflichtung soll verstärkt werden, indem

(a) die Erklärung auf Ergebnissen einer angemessenen Bewertung beruht (s. ISO/IEC 17050-1:2010, Nr. 5),

(b) der System-Anbieter eine unterstützende Dokumentation über die Bewertung und deren Ergebnisse dem Markt zur Verfügung stellt (s. ISO/IEC 17050-2:2004, Nr. 1), und

(c) der System-Anbieter bestätigt, die Anforderungen für Selbstverpflichtungserklärungen von diesem Regelwerk einhält.

§ 3.1.2 Ehrlichkeit und Zuverlässigkeit

(1) Um Vertrauen in die Selbstverpflichtungserklärung zu schaffen, muss der System-Anbieter wahrheitsgetreue und zuverlässige Aussagen abgeben.

(2) Dies bedeutet insbesondere, dass der System-Anbieter

(a) sich verpflichtet wahrheitsgemäße Aussagen über die Einhaltung der DIRECTIONS-Kriterien zu machen,

(b) eine Bewertung selbst durchführt oder durch geeignete Konformitätsbewertungsstellen durchführen lässt, auf der die Selbstverpflichtungserklärung basiert (s. ISO/IEC 17050-1:2010, Nr. 5), und

(c) interne Prozesse zur Aufrechterhaltung, Erweiterung, Einschränkung, Aussetzung und Widerruf der Erklärung etabliert, fortlaufend umsetzt, und deren Effektivität überwacht (s. ISO/IEC 17050-1:2010, Nr. 5).

(3) Der System-Anbieter darf keinen kommerziellen, finanziellen oder sonstigen Druck zulassen, der die Ehrlichkeit oder Zuverlässigkeit der Erklärung gefährdet.

(4) Risiken für die Ehrlichkeit und Zuverlässigkeit können entstehen durch:[5]

(a) Übermäßiger Eigennutz (z. B. Angst des System-Anbieters davor arbeitslos zu werden);

(b) Übermäßige Vertrautheit auf eigene Prozesse, anstatt eine ordnungsgemäße Bewertung der DIRECTIONS-Kriterien durchzuführen;

(c) Einschüchterung (z. B. kann der System-Anbieter durch einen Dritten abgeschreckt werden, ehrlich zu handeln);

(d) Wettbewerb (z. B. zwischen den System-Anbietern am Markt).

[5] Angelehnt an ISO/IEC 17065:2012 Tz. A.2.2.

§ 3.1.3 Kompetenz

(1) Für die Bewertung der DIRECTIONS-Kriterien ist Kompetenz des Personals des System-Anbieters erforderlich.
(2) Der System-Anbieter stellt sicher, dass sein Personal die notwendige Kompetenz zur Durchführung von Bewertungen aufweist, oder bezieht geeignete Konformitätsbewertungsstellen zur Unterstützung ein.

3.2 Vertraulichkeit und Offenheit

§ 3.2.1 Vertraulichkeit und Offenheit

(1) Der System-Anbieter stellt sicher, dass Informationen, auf denen die Selbstverpflichtungserklärung basiert, vertraulich behandelt werden (bspw. Dokumentation und Ergebnisse der Bewertung). So dürfen z.B. keine Informationen über angewendete TOMs bekannt werden, die zu einem Datenschutzrisiko führen könnten.
(2) Der System-Anbieter stellt sicher, dass einbezogene Konformitätsbewertungsstellen die Tätigkeiten vertraulich durchführen.
(3) Gleichzeitig muss der System-Anbieter für den öffentlichen Zugang und die Offenlegung sachgemäßer und rechtzeitiger Informationen über die Selbstverpflichtungserklärung sorgen, um Vertrauen in die Integrität und Glaubwürdigkeit der Selbstverpflichtungserklärung zu erzeugen (s. ISO/IEC 17050-2:2004, Nr. 1, 5).

§ 3.2.2 Abgrenzung der Verantwortlichkeiten

(1) Verantwortlich für die Erfüllung der DIRECTIONS-Kriterien ist der System-Anbieter.
(2) Der System-Anbieter ist ferner verantwortlich für die Abgabe, Aufrechterhaltung, Erweiterung, Einschränkung, Aussetzung und Widerruf der Erklärung.
(3) Werden Tätigkeiten von beauftragten Konformitätsbewertungsstellen durchgeführt, ist der System-Anbieter dafür verantwortlich, dass alle in diesem Regelwerk enthaltenen Anforderungen von den Konformitätsbewertungsstellen erfüllt und eingehalten werden.
(4) Der System-Anbieter ist für die ordnungsgemäße und ehrliche Selbstverpflichtungserklärung gemäß dem Kriterienkatalog verantwortlich, nicht beauftragte Konformitätsbewertungsstellen.
(5) Der System-Anbieter trägt die Verantwortung dafür, eine angemessene Bewertung anhand der DIRECTIONS-Kriterien durchgeführt zu haben, um eine Entscheidung zur Abgabe einer Selbstverpflichtungserklärung treffen zu können.

§ 3.2.3 Offenheit für Beschwerden

(1) Der System-Anbieter ist offen für Beschwerden von interessierten Parteien, insbesondere System-Kunden.
(2) Falls diese Beschwerden für begründet befunden werden, sollten die interessierten Parteien darauf vertrauen können, dass der System-Anbieter die Beschwerden zweckmäßig behandelt und dass angemessene Anstrengungen durch den System-Anbieter zu ihrer Klärung unternommen werden. Das Vertrauen in die Selbstverpflichtungserklärung wird erhöht, wenn Beschwerden vom System-Anbieter bearbeitet werden.

4 Anforderungen an den System-Anbieter

4.1 Grundlegende Anforderungen

§ 4.1.1 Rechtliche Verantwortung

(1) Der System-Anbieter muss eine juristische Person, ein festgelegter Teil einer juristischen Person oder eine natürliche Person sein, sodass der System-Anbieter für seine Selbstverpflichtungserklärung rechtlich verantwortlich gemacht werden kann (angelehnt an ISO/IEC 17065:2012 Tz. 4.1.1).

§ 4.1.2 Bereitstellung von Informationen für die Öffentlichkeit

(1) Der System-Anbieter muss (durch Publikationen, elektronische Medien oder andere Mittel) auf Anfrage Informationen über (oder Verweis auf) das Regelwerk und den Kriterienkatalog bereitstellen.

(2) Auf Anfrage muss der System-Anbieter zeitnah interessierten Parteien Informationen zur Erläuterung der Bedeutung der Selbstverpflichtungserklärung geben und mitteilen können, ob diese weiterhin gültig ist. Auf Fragen oder Bedenken interessierter Parteien hinsichtlich der Selbstverpflichtungserklärung muss der System-Anbieter zeitnah und gezielt antworten.

(3) Der System-Anbieter muss etwaige Rückfragen zur Klärung von Unklarheiten über den Gegenstand der Selbstverpflichtungserklärung beantworten.

(4) Der System-Anbieter muss eine Kontaktstelle für interessierte Parteien bereitstellen, um Beschwerden gegenüber der Selbstverpflichtungserklärung zu ermöglichen.

§ 4.1.3 Umgang mit Beschwerden und Einsprüchen

(1) Der System-Anbieter muss über ein Verfahren verfügen, um Beschwerden entgegenzunehmen, zu evaluieren sowie Entscheidungen über diese zu treffen (angelehnt an EDPB Annex 1 Tz. 7.13, 9.3.3, DSK Tz. 8.11.2).

(2) Der System-Anbieter sollte ein leicht auffindbares und bedienbares Kontaktformular oder gleichwertige Alternativen auf seiner Webseite zur Abgabe von Beschwerden einrichten.

§ 4.1.4 Anforderungen an das Personalmanagement des System-Anbieters

(1) Der System-Anbieter muss eine ausreichende Anzahl an Personal beschäftigen oder Zugang zu externem Personal haben, um den personellen Bedarf für die Bewertung und alle weiteren Prozesse für die Abgabe und das Management der Selbstverpflichtungserklärung abzudecken.

§ 4.1.5 Anforderungen an personelle Kompetenzen

(1) Das Personal des System-Anbieters muss die notwendige Fachkompetenz und Erfahrung in technischer und juristischer Hinsicht aufweisen, um eine Bewertung durchführen zu können.

(2) Es ist empfehlenswert, dass das Personal über Ressourcen mit Kenntnissen in folgenden Bereichen verfügt, um eine Bewertung vertrauenswürdig, effektiv und effizient durchführen zu können:

   (a) Kenntnisse im Datenschutzrecht (DSGVO/BDSG/einschlägige Landesdatenschutz- und Schulgesetze);
   (b) Kenntnisse im Telekommunikationsrecht sowie dem Recht der Dienste der Informationsgesellschaft bzw. der ePrivacy-Verordnung;
   (c) Kenntnisse über technische Grundlagen von Datenverarbeitungsvorgängen von schulischen Informationssystemen, darunter insbesondere auch TOM zur Sicherstellung des Datenschutzes;
   (d) Kenntnisse zu diesem Regelwerk und den Kriterienkatalog von DIRECTIONS.

(3) Zur Erfüllung der Grundsätze muss das Personal ferner die erforderliche persönliche Eignung und Zuverlässigkeit zur Durchführung der Bewertung aufweisen.

(4) Der System-Anbieter sollte ein Verfahren für das Management der Kompetenzen des Personals festlegen, einführen und aufrechterhalten (angelehnt an EDPB Annex 1 Tz. 9.2, DSK Tz. 8.10). Dazu zählt insbesondere auch, dass die Kenntnisse des Personals auf aktuellem Stand gehalten werden sollten (s. DSK Tz. 6.1.2.1). Die fortlaufende Schulung des Personals nimmt somit eine besondere Stellung zur Aufrechterhaltung der Kompetenz ein (s. DSK Tz. 8.10).

§ 4.1.6 Einbindung von externen Ressourcen, insb. Konformitätsbewertungsstellen

(1) Der System-Anbieter kann externe Ressourcen, insbesondere ausgegliederte, unabhängige und fachlich kompetenten Konformitätsbewertungsstellen, zur Unterstützung oder Durchführung der Bewertungstätigkeiten einbinden.

(2) Der System-Anbieter soll Bewertungstätigkeiten nur an Konformitätsbewertungsstellen ausgliedern, welche die in diesem Regelwerk beschriebenen Anforderungen einhalten.

§ 4.1.7 Management von Dokumentationen

(1) Der System-Anbieter muss Dokumentationen aufbewahren, um nachzuweisen, dass alle Anforderungen an die Selbstverpflichtungserklärung wirksam erfüllt worden sind.

(2) Aufzeichnungen müssen mindestens für den laufenden und den vorangegangenen Zyklus aufbewahrt werden.
Bei einer Gültigkeitsdauer von zwei Jahren beträgt die Aufbewahrungsdauer also mindestens vier Jahre zu Beginn eines neuen Zyklus und maximal zwei Jahre bei Beendigung des aktuellen Zyklus.

4.2 Anforderungen an das Management von Veränderungen

§ 4.2.1 Management von Veränderungen an Datenverarbeitungsvorgängen

(1) Der System-Anbieter verpflichtet sich während der gesamten Gültigkeitsdauer der Selbstverpflichtungserklärung, Veränderungen an den Datenverarbeitungsvorgängen zu überwachen und die Selbstverpflichtungserklärung unverzüglich anzupassen, falls die Änderungen die Aussagen der Selbstverpflichtung betreffen (s. ISO/IEC 17050-1:2010, Nr. 10.2). Beispiele für Veränderungen sind:

   (a) Veränderung bei dem rechtlichen, wirtschaftlichen oder organisatorischen Status oder bei der Eigentümerschaft und Änderungen der tatsächlichen oder rechtlichen Verhältnisse (s. DSK Tz. 4.1.2.2);
   (b) Veränderung bei Organisation und Management (z. B. Änderungen von Schlüsselpositionen, Entscheidungsprozessen oder technischem Personal);
   (c) wesentliche Änderungen an Software oder Hardware, welche zur Erbringung der Datenverarbeitungsvorgänge erforderlich sind;
   (d) wesentliche Änderungen hinsichtlich der Verarbeitung personenbezogener Daten;
   (e) Änderungen an Rechenzentren (bspw. Standortwechsel);
   (f) Änderungen bei der Einbindung von Subauftragsverarbeitern mit Relevanz für den Datenverarbeitungsvorgang.

(2) Der System-Anbieter ist bei Hinweisen über solche Änderungen, die Einfluss auf die Selbstverpflichtungserklärung haben könnten, verpflichtet, den Sachverhalt innerhalb von 8 Wochen zu ermitteln und geeignete Maßnahmen zu ergreifen (angelehnt an DSK Tz. 4.1.2.2). Der System-Anbieter hat darüber hinaus zu definieren, wie sichergestellt wird, dass in vergleichbaren Fällen vergleichbare Maßnahmen ergriffen werden. Geeignete Maßnahmen sind:

   (a) Der System-Anbieter kann feststellen, dass eine Zwischenbewertung zur Aufrechterhaltung der Selbstverpflichtungserklärung erforderlich ist.

(b) Der System-Anbieter kann eine Einschränkung der Schutzklasse, die Aussetzung oder den Widerruf der Selbstverpflichtungserklärung durchführen.

§ 4.2.2 Management von Änderungen an rechtlichen Rahmenbedingungen

(1) Der Eigner von DIRECTIONS (s. Kapitel 2.10) muss geeignete Maßnahmen ergreifen und fortlaufend durchführen, um Änderungen der rechtlichen Rahmenbedingungen, die die Selbstverpflichtungserklärung betreffen, zeitnah zu erkennen (s. ISO/IEC 17050-1:2010, Nr. 10.2). Beispiele für Veränderungen sind (s. DSK Tz. 7.10, EDPB Annex 1 Tz. 7.10):

(a) Gesetzesnovellierungen;
(b) Erlass delegierter Rechtsakte der Europäischen Kommission;
(c) Entscheidungen des Europäischen Datenschutzausschusses;
(d) Gerichtsentscheidungen;
(e) Fortentwicklungen des Stands der Technik.

(2) Der Eigner muss dem System-Anbieter Änderungen der rechtlichen Rahmenbedingungen, die ihn bzw. die Selbstverpflichtungserklärung betreffen, zeitnah mitteilen (angelehnt an DSK Tz. 7.10).

(3) Der System-Anbieter ist bei Hinweisen über solche Änderungen, die Einfluss auf die Aussage der Selbstverpflichtungserklärung haben könnten, verpflichtet, den Sachverhalt zu ermitteln und geeignete Maßnahmen zu ergreifen (angelehnt an DSK Tz. 4.1.2.2). Geeignete Maßnahmen sind:

(a) Der System-Anbieter kann feststellen, dass eine Zwischenbewertung zur Aufrechterhaltung der Selbstverpflichtungserklärung erforderlich ist.
(b) Der System-Anbieter kann eine Einschränkung der Schutzklasse, die Aussetzung oder den Widerruf durchführen.

(4) Stellt der System-Anbieter Änderungen an rechtlichen Rahmenbedingungen fest, informiert er den Eigner entsprechend.

§ 4.2.3 Management von Änderungen an dem Kriterienkatalog und dem Regelwerk

(1) Der Eigner von DIRECTIONS (s. Kapitel 2.10) kann Änderungen an dem Kriterienkatalog und diesem Regelwerk durchführen (bspw. aufgrund von Änderungen an den rechtlichen Rahmenbedingungen). Der Eigner informiert daraufhin den System-Anbieter.

(2) Wenn dieses Regelwerk neue oder überarbeitete Anforderungen an die Erklärung einführt, verpflichtet sich der System-Anbieter zur raschen Umsetzung dieser Anforderungen (s. ISO/IEC 17050-1:2010, Nr. 10.2). In der Regel ist eine rasche Umsetzung innerhalb eines Monats durchzuführen. Ausnahmen können mit dem Eigner im Einzelfall abgestimmt werden.

(3) Der System-Anbieter muss geeignete Prozesse etablieren, um auf Änderungen des Kriterienkatalogs und des Regelwerks zu reagieren (s. ISO/IEC 17050-1:2010, Nr. 10.2). Hierzu zählen unter anderem folgende Maßnahmen:

(a) Ein System-Anbieter leitet Maßnahmen ein, um Änderungen an den Anforderungen der Erklärung zeitnah umzusetzen (i.d.R. innerhalb eines Monats);
(b) Der System-Anbieter ist verpflichtet, bei Änderungen am Kriterienkatalog, die Einfluss auf die Aussage der Selbstverpflichtungserklärung haben könnten, den Sachverhalt für jeden Datenverarbeitungsvorgang zu ermitteln und geeignete Maßnahmen zu ergreifen. Geeignete Maßnahmen sind:
    (i) Der System-Anbieter kann feststellen, dass eine Zwischenbewertung zur Aufrechterhaltung der Selbstverpflichtungserklärung erforderlich ist.
    (ii) Der System-Anbieter kann eine Einschränkung der Schutzklasse, die Aussetzung oder den Widerruf durchführen.

4.3 Anforderungen zur Nutzung der DIRECTIONS-Selbstverpflichtungserklärung

§ 4.3.1 Abschluss einer Vereinbarung mit dem Eigner

(1) Der Eigner stellt dieses Regelwerk zu nicht-diskriminierenden Bedingungen interessierten System-Anbietern zur Verfügung.
(2) Zur Nutzung des Regelwerks, des Kriterienkatalogs sowie weiterer Dokumente von DIRECTIONS für die Abgabe der Selbstverpflichtungserklärung schließt der System-Anbieter eine Nutzungsvereinbarung mit dem Eigner.
(3) Der Eigner legt die Bedingungen für die Nutzung der DIRECTIONS-Selbstverpflichtungserklärung selbst in einer separaten Vereinbarung fest.

§ 4.3.2 Eintrag in einem Register für Selbstverpflichtungserklärungen

(1) Der Eigner führt ein öffentlich einsehbares Register mit Selbstverpflichtungserklärungen, um eine Rückverfolgung durch interessierte Parteien zu ermöglichen (angelehnt an ISO/IEC 17050-2:2004, Nr. 4.1).
(2) Für jede Selbstverpflichtungserklärung müssen mindestens folgende Informationen im Register hinterlegt sein:

   (a) die eindeutige Bezeichnung des Gegenstands der Selbstverpflichtung (s. Kapitel 2.1);
   (b) die eindeutige Bezeichnung des System-Anbieters, inkl. Name und Anschrift des System-Anbieters;
   (c) die maßgebliche Fassung des DIRECTIONS-Kriterienkatalogs;
   (d) die maßgebliche Fassung des Regelwerks;
   (e) die Gültigkeitsdauer der Selbstverpflichtungserklärung, inkl. Datum der Erklärung und Ende der Selbstverpflichtungserklärung;
   (f) die Aussage, wonach der System-Anbieter eine Selbstverpflichtung basierend auf einer Bewertung abgegeben hat;
   (g) Verweis auf die unterstützende Dokumentation zur Bewertung (s. § 5.3.3);
   (h) Ansprechstellen für Beschwerden.

(3) Der System-Anbieter erklärt sich einverstanden, die obigen Informationen dem Eigner bereitzustellen und öffentlichkeitswirksam im Register gelistet zu werden.

§ 4.3.3 Werbung mit der Selbstverpflichtungserklärung

(1) Der System-Anbieter darf mit der Selbstverpflichtungserklärung auf Webseiten, (gedruckten) Publikationen, Dokumenten und sonstigen Werbematerialien werben, insofern keine Missverständnisse, Unklarheiten und Irreführungen erzeugt werden und alle Anforderungen dieses Regelwerks eingehalten werden (angelehnt an ISO/IEC 17030:2009 Tz. 5.6).
(2) Insbesondere darf durch die Werbung am Markt nicht der Eindruck entstehen, dass es sich bei der Selbstverpflichtungserklärung um eine Konformitätsbewertung durch eine zweite oder dritte Stelle handelt. Wenn irgendein Kennzeichen auf Webseiten, Dokumenten, o.ä. angebracht wurde, um das Vorhandensein einer Selbstverpflichtungserklärung anzuzeigen, muss solche Kennzeichnung so gestaltet sein, dass keine Verwechslungen mit irgendwelchen Zertifizierungszeichen möglich ist (s. ISO/IEC 17050-1:2010, Nr. 9). Solche Kennzeichnung muss auf die Selbstverpflichtungserklärung rückverfolgbar sein. Bei der Selbstverpflichtungserklärung handelt es sich um ein Übergangsinstrument zur Erhöhung des Datenschutzes im Bildungsmarkt, bis bewilligte Zertifizierungsverfahren nach Art. 42 DSGVO (oder Verhaltensregeln nach Art. 40 DSGVO) verfügbar sind.

§ 4.3.4 Werbung mit und Verweis auf dieses Regelwerk

(1) System-Anbieter müssen auf dieses Regelwerk und den Kriterienkatalog verweisen, insofern keine Missverständnisse, Unklarheiten und Irreführungen erzeugt werden.

(2) Die maßgebliche Fassung des Regelwerks und des Kriterienkatalogs sind anzugeben.

5 Anforderungen an den Bewertungsprozess und die Abgabe der Erklärung

Die Grundlage der Selbstverpflichtungserklärung müssen Ergebnisse einer angemessenen Bewertung sein (s. ISO/IEC 17050-1:2010, Nr. 5). Insgesamt werden die sequenziellen Prozessstufen Auswahl (**Nr. 5.1**), Bewertung (**Nr. 5.2**), Entscheidung und Abgabe der Erklärung (**Nr. 5.3**) durchlaufen. Im Anschluss werden fortlaufende Überwachungstätigkeiten (**Nr. 5.4**) durchgeführt.

Nr. 5.1 Im Rahmen der **Auswahl** finden planende und vorbereitende Tätigkeiten statt, um für die nachfolgende Bewertung alle erforderlichen Informationen und Eingangsgrößen sammeln oder bereitstellen zu können, inklusive der Darstellung und Abgrenzung des Gegenstands der Selbstverpflichtung (s. ISO/IEC 17000:2020 Tz. A.2).

Nr. 5.2 Bei der **Bewertung** untersucht der System-Anbieter, ob und wie er die Kriterien des DIRECTIONS-Kriterienkatalogs umsetzt.

Nr. 5.3 Der System-Anbieter fällt im Anschluss eine **Entscheidung** über die Abgabe der Selbstverpflichtungserklärung, auf Grundlage der Bewertung über die Erfüllung der Kriterien (s. ISO/IEC 17000:2020 Tz. 7.2) und gibt anschließend die **Erklärung ab**.

Nr. 5.4 Eine **Überwachung** umfasst sich wiederholende Tätigkeiten als Grundlage zur Aufrechterhaltung der Gültigkeit der Selbstverpflichtungserklärung (s. ISO/IEC 17000:2020 Tz. A.5).

5.1 Auswahl

§ 5.1.1 Beschreibung und Festlegung des Gegenstands der Selbstverpflichtungserklärung

(1) Die Beschreibung des Gegenstands ist zentraler Bestandteil des Bewertungsberichts (s. § 5.2.9) und der zusätzlichen Dokumentation zur Selbstverpflichtungserklärung (s. § 5.3.3).

(2) Gegenstand der Selbstverpflichtungserklärung sind Datenverarbeitungsvorgänge von personenbezogenen Daten in schulischen Informationssystemen (s. Kapitel 2.1).

(3) Der System-Anbieter legt den Gegenstand selbst fest und dokumentiert dies.

(4) Der System-Anbieter stellt auf Anfrage der Öffentlichkeit ausreichend Informationen über den Gegenstand der Selbstverpflichtungserklärung zur Verfügung. Ziel der Offenlegung ist die Schaffung von Transparenz bezüglich des konkreten Gegenstands, da schulische Informationssysteme komplex sind.

(5) Die vom System-Anbieter bereitgestellte Dokumentation enthält mindestens eine detaillierte Beschreibung des Gegenstands, dazu zählen

   (a) die Benennung und detaillierte (Funktions-)Beschreibung des Datenverarbeitungsvorgangs oder der Datenverarbeitungsvorgänge innerhalb eines entsprechenden schulischen Informationssystems, auf das sich die Selbstverpflichtungserklärung bezieht;
   (b) detaillierte Beschreibung aller Bestandteile der relevanten Datenverarbeitungsvorgänge, sodass eine abgeschlossene Verfahrensstruktur gewährleistet wird;
   (c) Dokumentation von Verantwortlichkeiten des System-Anbieters im Datenverarbeitungsvorgang;
   (d) Ggf. Benennung und Informationen zu Standorten bei denen Datenverarbeitungsvorgänge durchgeführt werden (s. IAF MD 1:2018 Tz. 7.1.1);
   (e) Informationen bezüglich aller ausgegliederten Vorgänge, die von dem System-Anbieter im Rahmen des Datenverarbeitungsvorgangs genutzt werden und welche die Selbstverpflichtung beeinflussen. Dabei müssen insbesondere Subauftragsverarbeiter und die von ihnen übernommenen Zuständigkeiten und damit verbundenen Aufgaben benannt werden (s. DSK Tz. 7.2).

(6) Der System-Anbieter kann das Begleitdokument ‚DIRECTIONS-Zertifizierungsgegenstand' zur Unterstützung bei der Festlegung des Gegenstandes heranziehen.

§ 5.1.2 Auswahl der Schutzklasse

(1) Der System-Anbieter legt die Schutzklasse fest, welche seine Datenverarbeitungsvorgänge erfüllen. Zur Festlegung sei auf den DIRECTIONS-Kriterienkatalog Kapitel B. hingewiesen.
(2) Der System-Anbieter muss etwaige Rückfragen zur Klärung von Unklarheiten über die gewählte Schutzklasse beantworten.

§ 5.1.3 Etablierung von Prozessen

(1) Der System-Anbieter muss Prozesse etablieren, die sicherstellen, dass die in der Erklärung angegebenen Kriterien an den Gegenstand fortdauernd erfüllt werden (s. ISO/IEC 17050-1:2010, Nr. 10).
(2) Der System-Anbieter muss ferner Prozesse zur Erweiterung, Einschränkung, Aussetzung und Widerruf der Erklärung etablieren, fortlaufend umsetzen, und deren Effektivität überwachen (s. ISO/IEC 17050-1:2010, Nr. 5).

5.2 Bewertung durch den System-Anbieter

§ 5.2.1 Selbstverpflichtungserklärung basierend auf eine Bewertung

(1) Die Grundlage der Erklärung müssen Ergebnisse einer angemessenen Bewertung sein (s. ISO/IEC 17050-1:2010, Nr. 5).
(2) Im Rahmen der Bewertung gibt der System-Anbieter eine detaillierte Stellungnahme zur Umsetzung für jedes einzelne Kriterium des DIRECTIONS-Kriterienkatalogs ab (s. hierzu auch § 5.2.9 und § 5.3.3).
(3) Diese Bewertung wird vorranging vom System-Anbieter selbst durchgeführt. Er kann zusätzlich Unterstützung durch Konformitätsbewertungsstellen zur Erlangung der Ergebnisse heranziehen (s. ISO/IEC 17050-1:2010, Nr. 5). Hierzu zählen gemäß Kapitel 2.6 insbesondere dritte Stellen (z.B. Prüf- oder Kalibrierlaboratorien, Inspektionsstellen, Zertifizierungsstellen).

§ 5.2.2 Planung der Bewertung

(1) Der System-Anbieter sollte vor der Durchführung der Bewertung einen Plan anfertigen, welcher Angaben zum zeitlichen Ablauf sowie das verantwortliche Personal umfasst. Dadurch wird sichergestellt, dass eine vertrauenswürdige Bewertung durchgeführt werden kann.

§ 5.2.3 Umfang der Bewertung

(1) Die Bewertung erfolgt auf Grundlage der abgegrenzten Beschreibung des Gegenstands der Selbstverpflichtung. Die Bewertung muss für den gesamten Gegenstand, inklusive aller technischen und organisatorischen Vorgänge oder Vorgangsreihen, die anwendbaren Kriterien des Kriterienkatalogs in der maßgeblichen Fassung umfassen.
(2) Gegenstand der Bewertung ist auch das Zusammenwirken der Datenverarbeitungsvorgänge oder deren Bestandteile mit anderen Bestandteilen, Datenverarbeitungsvorgängen oder Diensten. Hierzu zählt insbesondere auch die Betrachtung möglicher Schnittstellen zu Subauftragsverarbeitern.
(3) Im Rahmen der Bewertung werden durch den System-Anbieter unterschiedliche, sozio-technische Bestandteile seines schulischen Informationssystems begutachtet. Dabei setzt sich ein schulisches Informationssystem aus einem oder mehreren Datenverarbeitungsvorgängen zusammen. Einem Datenverarbeitungsvorgang können wiederrum Objekte und Entitäten zugeordnet werden, darunter Vereinbarungen (4), Prozesse (5), Anbietereigenschaften (6), Systemeigenschaften (7), Infrastrukturkomponenten (8), Softwarekomponenten (9), die Entwicklungsumgebung (10), Mitarbeiter des System-Anbieters (11), und (12) das (Datenschutz-)Managementsystem.
(4) Bei rechtsverbindlichen Vereinbarungen werden die Eigenschaften und Inhalte von Verträgen oder Vereinbarungen mit System-Kunden oder Subauftragsverarbeitern bewertet.

(5) Ein Prozess oder eine entsprechende und realitätsnahe Prozessdokumentation kann bewertet werden.
(6) Eine Bewertung von Anbietereigenschaften umfasst die Begutachtung von Eigenschaften und Ausprägungen des System-Anbieters, bspw. die zugrundeliegende Organisationsstruktur.
(7) Zu den Systemeigenschaften gehören insbesondere Features und -Funktionen des schulischen Informationssystems, die für den System-Kunden unmittelbar sichtbar sind und bewertet werden müssen.
(8) Eine Bewertung kann Infrastrukturkomponenten umfassen, also physische Objekte, wie bspw. Hardware-Komponenten oder die Rechenzentrumsinfrastruktur.
(9) Die Bewertung von Softwarekomponenten umfasst virtuelle Objekte, bspw. Quellcode sowie die Zusammenstellung und Interaktionen der einzelnen Komponenten der Datenverarbeitungsvorgänge.
(10) Die Bewertung der Entwicklungsumgebung umfasst eingesetzte Entwicklungsmethoden, sichere und vom Produktivsystem getrennte Test- und Entwicklungsumgebung, und Abnahmetests.
(11) Die Bewertung von Mitarbeitern kann notwendig sein, um bspw. deren fachliche oder persönliche Eignung sicherzustellen.
(12) Die Bewertung des (Datenschutz-)Managementsystems ist notwendig, um zu erkennen, ob der System-Anbieter für das Management der relevanten Aspekte seiner Tätigkeiten, Produkte und Dienstleistungen ein System umgesetzt hat, das im Einklang mit der Politik der Organisation und den Kriterien der Selbstverpflichtung steht.

§ 5.2.4 Durchführung der Bewertung

(1) Im Rahmen der Bewertung muss der System-Anbieter **dezidiert für jedes anwendbare Kriterium prüfen**, wie er das Kriterium umsetzt. Die Bewertung sollte dabei differenziert für die Unterpunkte des jeweiligen Kriteriums durchgeführt werden (bspw. Bewertung des Kriteriums Nr. 2.2 (2)).
(2) In Situationen, in denen der System-Anbieter einen Datenverarbeitungsvorgang an mehreren (eigenen) Standorten durchführt, sind solche Standorte in die Bewertung einzubeziehen.
(3) Die Ausführung von einzelnen Bewertungsmethoden ist zu protokollieren.
(4) Der System-Anbieter kann im Rahmen der Bewertung bestehende Zertifikate, Testate, Gütesiegel oder andere Konformitätszeichen und -nachweise als Nachweis zur Erfüllung von einzelnen Kriterien benennen.
(5) Der System-Anbieter kann externe Ressourcen, insbesondere ausgegliederte, unabhängige und fachlich kompetenten Konformitätsbewertungsstellen zur Unterstützung oder Durchführung der Bewertungstätigkeiten einbinden.

§ 5.2.5 Bewertungsmethoden

(1) Die Bewertung sollte durch angemessene Formen von Konformitätsbewertungstätigkeiten (z. B. Prüfen, Auditieren, Messung, Inspektion oder Prüfung von Personen) durchgeführt werden (s. ISO/IEC 17050-1:2010, Nr. 5).
(2) Wo zutreffend, sollten Internationale Normen, Leitfäden und andere normative Dokumente zu solchen Konformitätsbewertungstätigkeiten zu Rate gezogen werden (s. ISO/IEC 17050-1:2010, Nr. 5).
(3) Folgende Konformitätsbewertungstätigkeiten werden empfohlen: eine Prüfung von Dokumentationen (4), und Durchführung von Inspektionen (5), Prüfungen (6), und (interne) Audits (7), und/oder Entwicklungs- und Designprüfungen (8).
(4) Dokumentprüfung (im Sinne der ISO/IEC 17020). Mit der Dokumentprüfung bewertet der System-Anbieter die Einhaltung der Kriterien anhand bestehender Konzepte, Berichte, (technischer) Logs, Testate oder andere Dokumentationen. Insbesondere führt der System-Anbieter eine Rechtsanalyse durch (bspw. der rechtsverbindlichen Vereinbarungen), um sicherzugehen, dass die geltenden rechtlichen Kriterien erfüllt werden. Zudem kann ein System-Anbieter

im Rahmen einer Dokumentprüfung auch Personenzertifikate (im Sinne der ISO/IEC 17024) zum Kompetenznachweis für das Personal bzw. einer natürlichen Person (bspw. des Datenschutzbeauftragten) und zur Gewährleistung eines angemessenen Datenschutzniveaus bewerten.

(5) Inspektion (im Sinne der ISO/IEC 17020). In Bezug auf die DIRECTIONS-Kriterien wird mittels einer (rechtlichen) Inspektion vom System-Anbieter insbesondere die Einhaltung von geeigneten TOM gem. Art. 32 Abs. 1 lit. a) bis d) DSGVO bewertet. Bei der Inspektion können bspw. Datenverarbeitungsvorgänge im Rahmen einer Systemnutzung durchgeführt werden, um die Funktionsweise und die Ergebnisse der Vorgänge beurteilen zu können. Ein System-Anbieter vergleicht hierbei die zu erwartenden Ergebnisse gemäß der vorliegenden Dokumentation mit den tatsächlichen Ergebnissen, welche durch eine Systemnutzung erbracht werden. Er erhält somit keinen Einblick in die internen Verarbeitungsschritte der Verarbeitungsvorgänge (‚Black-Box-Test'). Daneben kann ein Vorgang oder eine Vorgangsreihe auch angestoßen und die tatsächliche Ausführung überwacht (‚monitoring') oder Logs der Vorgangsausführung überprüft werden (‚White-Box-Test').

(6) Prüfung (im Sinne der ISO/IEC 17025). Eine Prüfung umfasst Tests oder Messungen durch den System-Anbieter zur Untersuchung des Datenverarbeitungsvorgangs. So kann eine Assetprüfung durchgeführt werden, indem bei der Prüfung ein Asset (z.B. Hardware oder Softwarecode und ggf. die dazugehörige Dokumentation) untersucht wird. Ein System-Anbieter kann zur Prüfung und Überwachung des Vorgangs (‚monitoring') geeignete (ggf. extern bereitgestellte) Testierungs- und Auditierungsprodukte und -dienstleistungen nutzen (s. ISO/IEC 17025:2017 Tz. 6.6). In Bezug auf die DIRECTIONS-Kriterien wird mittels einer (rechtlichen) Prüfung insbesondere die Einhaltung von geeigneten TOM gem. Art. 32 Abs. 1 lit. a) bis d) DSGVO bewertet. Bspw. kann mittels Sicherheitstests die korrekte und starke Verschlüsselung von Daten festgestellt werden.

(7) Audit (im Sinne der ISO/IEC 17021-1). Ein (internes) Audit wird zum Zweck der Bewertung des (Datenschutz-)Managementsystems des System-Anbieters durchgeführt (s. ISO/IEC 17021-1:2015 Tz. 3.4). Im Rahmen des Audits können insbesondere Befragungen, Beobachtungen und Prüfungen durchgeführt werden, um Informationen über Wissen und Fertigkeiten zu ermitteln sowie festzustellen, ob Prozesse und das Managementsystem beim System-Anbieter gelebt werden. Die Befragung von Mitarbeitern oder anderen Personen, die mit der Erbringung der Datenverarbeitungsvorgänge befasst sind, kann zur Sachverhaltsermittlung einzelner Aspekte und zur Überprüfung der Richtigkeit der Dokumentation eingesetzt werden (s. ISO/IEC 17021-1:2015 Tz. B.4). Eine Person bei der Erfüllung einer Aufgabe zu beobachten, kann durch die damit dargelegte Anwendung von Wissen und Fertigkeiten zur Erzielung eines gewünschten Ergebnisses direkte Nachweise für die Kompetenz liefern (s. ISO/IEC 17021-1:2015 Tz. B.5). Schriftliche, mündliche und praktische Prüfungen können gute und gut dokumentierte Nachweise für vorhandenes Wissen und — je nach angewendeter Methodik — auch für Fertigkeiten liefern (s. ISO/IEC 17021-1:2015 Tz. B.6). Eine Vor-Ort-Prüfung umfasst die Inaugenscheinnahme der Verfahren und technischen Einrichtungen in den Räumlichkeiten des System-Anbieters. In Bezug auf die DIRECTIONS-Kriterien sollen insbesondere (rechtliche, interne) Audits durchgeführt werden, um eine korrekte Einrichtung, Aufrechterhaltung und Pflege eines Datenschutz-Managementsystems (im Sinne von Art. 24 und 25, 32, 33, 34 sowie 37 bis 39 DSGVO) zu bewerten.

(8) Entwicklungs- und Designprüfung (im Sinne der ISO/IEC 17020). Eine Entwicklungsprüfung umfasst die Bewertung von Entwicklungsmethoden und -verfahren sowie bei Bedarf eine Prüfung der Testsysteme und -umgebungen, welche bei der Entwicklung von Hard- und Software zur Erbringung der Datenverarbeitungsvorgänge eingesetzt werden. Bei der Designprüfung können unter anderem die gewählte Architektur, Datenbankdiagramme, Datenflussdiagramme, Designentscheidungen aber auch die Konfiguration des Systems zur Erbringung des Datenverarbeitungsvorgangs überprüft werden. Eine Entwicklungs- und Designprüfung sollte auch eine Rechtsanalyse umfassen, um sicherzugehen das die geltenden rechtlichen

Kriterien erfüllt werden. So kann eine rechtliche Entwicklungs- und Designprüfung insbesondere im Rahmen der Bewertung zur Erfüllung des Art. 25 DSGVO oder zur Überprüfung der Datenschutz-Folgenabschätzung erforderlich sein.

§ 5.2.6 Wahl von Stichproben bei der Bewertung

(1) Ein System-Anbieter kann eine Stichprobenentnahme durchführen, wenn es weder praktikabel noch kostengünstig ist, alle verfügbaren Informationen während einer Bewertung ganzheitlich zu prüfen. So können bspw. die Aufzeichnungen zu zahlreich sein, um eine Bewertung jedes einzelnen Elements der Grundgesamtheit zu rechtfertigen.

(2) Eine Stichprobenentnahme umfasst in der Regel folgende Schritte:

(a) Festlegen der Ziele und Gründe der Stichprobenentnahme;
(b) Festlegung der Grundgesamtheit, aus der Stichproben zu entnehmen sind;
(c) Auswahl einer Methode zur Stichprobenentnahme (bspw. entscheidungsbasierte oder statistische Stichprobenentnahme);
(d) Bestimmen der Größe der zu entnehmenden Stichprobe;
(e) Durchführen der Probenentnahmetätigkeit;
(f) Zusammenstellen, Beurteilen, Berichten und Dokumentieren der Ergebnisse.

(3) Die Stichprobe ist mindestens so umfassend zu wählen, dass eine repräsentative Stichprobe in Bezug auf die Grundgesamtheit gezogen werden kann.

(4) Es können die entscheidungsbasierte Stichprobenentnahme oder die statistische Stichprobenentnahme angewandt werden. Die entscheidungsbasierte Stichprobenentnahme stützt sich bei der Festlegung von Proben auf Kompetenz und Erfahrungen des Personals. Statistische Verfahren zur Stichprobenentnahme verwenden ein Probeauswahlverfahren, das auf Wahrscheinlichkeitstheorie beruht.

§ 5.2.7 Nichtanwendbarkeit von Kriterien

(1) Der DIRECTIONS-Kriterienkatalog regelt die Nichtanwendbarkeit von Kriterien (s. Kapitel A.4).

(2) Der System-Anbieter prüft, welche Kriterien des DIRECTIONS-Kriterienkatalogs abhängig vom jeweiligen Gegenstand der Selbstverpflichtung anwendbar sind. Die Einschätzung der Nichtanwendbarkeit von Kriterien der Selbstverpflichtung dokumentiert der System-Anbieter und teilt diese auf Rückfragen den interessierten Parteien mit. Die Dokumentation sollte dabei mindestens enthalten:

(a) eine Auflistung der Kriterien, die nicht anwendbar sind;
(b) eine ausführliche Begründung pro Kriterium, warum dieses für den konkreten Gegenstand der Selbstverpflichtung nicht anwendbar ist.

§ 5.2.8 Feststellung von Mängeln und Nichtkonformitäten

(1) Wurde bei der Bewertung festgestellt, dass ein oder mehrere Kriterien nicht erfüllt werden, muss der System-Anbieter Nachbesserungen in angemessener Frist durchführen und sein System so gestalten, dass alle Kriterien erfüllt sind, bevor die Selbstverpflichtungserklärung abgegeben werden darf.

(2) Im Rahmen der Nachbesserung muss der System-Anbieter dafür Sorge tragen, dass alle Mängel und Abweichungen zur Erfüllung der Kriterien abgestellt werden.

(3) Der System-Anbieter muss die durchgeführten Korrekturen und Korrekturmaßnahmen erneut bewerten, um festzustellen, ob sie annehmbar sind.

(4) Wurde bei der Bewertung der Korrekturen festgestellt, dass ein oder mehrere Kriterien weiterhin nicht erfüllt sind, prüft der System-Anbieter, ob eine weitere Nachbesserung in angemessener Frist sinnvoll erscheint oder keine Selbstverpflichtungserklärung abgegeben werden kann.

§ 5.2.9 Bewertungsbericht

(1) Der System-Anbieter erstellt auf der Grundlage der Bewertung einen Bericht, indem die Ergebnisse genau, klar, eindeutig und objektiv dokumentiert werden.
(2) Dieser Bewertungsbericht bildet die Grundlage für die Entscheidung zur Abgabe der Erklärung. Ferner bildet der Bewertungsbericht die Grundlage für die Erstellung der zusätzlichen Dokumentation zur Selbstverpflichtungserklärung (s. § 5.3.3).
(3) Der Bewertungsbericht enthält die Ergebnisse der Bewertung. Die Ergebnisse müssen umfassend und detailliert dokumentiert sein. Dies bedeutet insbesondere,

   (a) dass die Umsetzung **jedes einzelnen Kriteriums** hinreichend umfassend beschrieben und begründet ist, und
   (b) die Beschreibung hinreichend klar, plausibel und eindeutig hinsichtlich der Umsetzung ist.

(4) Um das Vertrauen in die Bewertung zu erhöhen, wird empfohlen, dass der System-Anbieter für jedes Kriterium die entsprechende Dokumentation (bspw. Prozessdokumentation, Logs, Intranet, Wiki etc.), Systeme, oder andere Nachweise referenziert und benennt.
(5) Der Bewertungsbericht enthält darüber hinaus mindestens folgende Angaben:

   (a) eindeutige Kennzeichnung, sodass alle Teile des Bewertungsberichts als Teil eines vollständigen Berichts erkannt werden sowie eine eindeutige Kennzeichnung des Endes;
   (b) eine (Referenz zur) detaillierten Beschreibung des Gegenstands der Selbstverpflichtung (s. § 5.1.1);
   (c) Beschreibung der nichtanwendbaren Kriterien sowie eine Begründung, warum diese nichtanwendbar sind (s. § 5.2.7);
   (d) Angaben zu durchgeführten Bewertungsmethoden;
   (e) Angaben zu dem Personal zur Durchführung der Bewertung und ggf. zur Einbindung von Konformitätsbewertungsstellen;
   (f) eine Darstellung des zeitlichen Ablaufs, darunter mindestens das Start- und Enddatum der Bewertung;
   (g) eine Darstellung von identifizierten Mängeln und Nichtkonformitäten, durchgeführten Abstellmaßnahmen sowie das Ergebnis der erneuten Bewertung dieser;
   (h) eine abschließende Bewertung mit der Empfehlung die Selbstverpflichtungserklärung abzugeben oder nicht abzugeben;
   (i) die Erklärung, dieses Regelwerk eingehalten zu haben;
   (j) das Ausstellungsdatum des Bewertungsberichts;
   (k) Unterschrift oder äquivalentes Zeichen der Gültigkeit, Name und Funktion des (der) dazu autorisierten Person(en), die verantwortlich für den Bewertungsbericht ist (sind).

(6) Wenn ein ausgestellter Bewertungsbericht geändert oder neu ausgestellt werden muss, müssen alle Änderungen von Informationen eindeutig gekennzeichnet werden und, wo erforderlich, muss der Grund für die Änderung im Bericht aufgenommen werden. Wenn es erforderlich ist, einen vollständigen neuen Bericht auszustellen, muss dieser Bericht eine eindeutige Bezeichnung haben und einen Verweis auf das Original enthalten, welches er ersetzt.
(7) Der Bewertungsbericht und alle referenzierten Dokumente müssen vor unbefugtem Zugriff geschützt und gegen Manipulation und Verlust gesichert sein.

5.3 Entscheidung über die Abgabe der Selbstverpflichtungserklärung

§ 5.3.1 Treffen einer Entscheidung

(1) Der System-Anbieter entscheidet auf Grundlage der Bewertung und des entsprechenden Bewertungsberichts über die Abgabe der Selbstverpflichtungserklärung.
(2) Die Selbstverpflichtungserklärung kann durch der System-Anbieter im festgelegten Umfang abgeben werden, wenn

(a) die Bewertung ergeben hat, dass der Gegenstand **alle** anwendbaren Kriterien einhält,
(b) der System-Anbieter versichert wahrheitsgemäße Aussagen über die Einhaltung der DIRECTIONS-Kriterien gemacht zu haben, und
(c) interne Prozesse zur Aufrechterhaltung, Erweiterung, Einschränkung, Aussetzung und Widerruf der Erklärung etabliert sind, und fortlaufend umgesetzt werden sowie deren Effektivität überwacht wird (s. ISO/IEC 17050-1:2010, Nr. 5).

(3) Der Zeitraum zwischen dem Abschluss der Bewertung und der Entscheidung über die Abgabe der Selbstverpflichtungserklärung darf nur in berechtigten Ausnahmefällen die Dauer von einem Monat überschreiten.

(4) Die Entscheidung über die Selbstverpflichtungserklärung muss durch leitende Führungskräfte des System-Anbieters oder eine direkt von ihnen beauftragte qualifizierte Person erfolgen.

§ 5.3.2 Inhalt der Selbstverpflichtungserklärung

(1) Der System-Anbieter muss sicherstellen, dass die Selbstverpflichtungserklärung ausreichende Informationen enthält, die interessierte Parteien als Empfänger der Erklärung in die Lage versetzt, den System-Anbieter als Aussteller der Erklärung, den Gegenstand der Erklärung und den angewendeten Kriterienkatalog erkennen zu können (s. ISO/IEC 17050-1:2010, Nr. 6.1).

(2) Die Selbstverpflichtungserklärung enthält mindestens die folgenden Angaben (s. ISO/IEC 17050-1:2010, Nr. 6.1):

(a) die eindeutige Bezeichnung der Erklärung („Selbstverpflichtungserklärung“);
(b) Ggf. eine graphische Illustration;[6]
(c) kurze Beschreibung des Datenverarbeitungsvorgang des schulischen Informationssystems und die Datenschutzrolle des System-Anbieters (beispielsweise „als Auftragsverarbeiter“);
(d) die Selbstverpflichtungsaussage („Hiermit verpflichten wir uns auf die fortlaufende Einhaltung der DIRECTIONS-Kriterien gemäß der Version [X.XX]“);
(e) die Gültigkeitsdauer der Selbstverpflichtungserklärung mit Angabe des Zeitraums (Abgabe, Laufzeit bis);
(f) den DIRECTIONS-Kriterienkatalog und das Regelwerk in ihren gültigen Fassungen;
(g) die festgelegte Schutzklasse 1 oder 2;
(h) Beschreibung der nichtanwendbaren Kriterien (s. § 5.2.7);
(i) ein Verweis auf die unterstützende Dokumentation (s. § 5.3.3 ; gemäß ISO/IEC 17050-2:2004);
(j) die Bestätigung, dass alle Angaben wahrheitsgemäß gemacht worden sind;
(k) den Namen (und ggf. die Kontaktadresse) der Person, welche die Erklärung ausstellt;
(l) den Hinweis, dass es sich hierbei nicht um ein Konformitätszeichen zweiter oder dritte Stelle handelt, sondern um eine Selbstverpflichtungserklärung des Anbieters als erste Stelle;
(m) den Ort und das Abgabedatum der Erklärung;
(n) Unterschrift oder äquivalentes Zeichen der Gültigkeit, Name und Funktion des (der) dazu autorisierten Person(en), die im Namen des System-Anbieters handelt (handeln).

(3) Die Selbstverpflichtungserklärung kann weiter folgende optionale Angaben enthalten (s. ISO/IEC 17050-1:2010, Nr. 6.2):

[6] Wenn eine grafische Illustration oder ein anderweitiges Kennzeichen auf Webseiten, Dokumenten, o.ä. angebracht wurde, um das Vorhandensein einer Selbstverpflichtungserklärung anzuzeigen, muss solche Kennzeichnung so gestaltet sein, dass keine Verwechslungen mit Zertifizierungszeichen möglich ist (s. ISO/IEC 17050-1:2010, Nr. 9). Solche Kennzeichnung muss auf die Selbstverpflichtungserklärung rückverfolgbar sein (bspw. durch das Klicken auf das Zeichen).

(a) der Name und die Anschrift jeder beteiligten Konformitätsbewertungsstelle im Rahmen der Bewertung, z. B. Prüf- oder Kalibrierlaboratorien, Inspektionsstellen, Zertifizierungsstellen;
(b) der Bezug auf deren Konformitätsbewertungsbericht und das Ausstellungsdatum des Berichtes;
(c) zusätzliche Informationen über erhaltene Zertifikate, Testate, Gütesiegel oder andere Konformitätszeichen, welche verwiesen wurden.

(4) Wird die Selbstverpflichtungserklärung in elektronischen Medien (bspw. Webseite) angebracht, so ist dieses mit einem Link auf den Eintrag im Register des Eigners zu versehen (s. § 4.3.1), um die Rückverfolgbarkeit durch System-Kunden und interessierte Parteien zu ermöglichen.

§ 5.3.3 Zusätzliche Dokumentation zur Selbstverpflichtungserklärung

(1) Die Akzeptanz der Selbstverpflichtungserklärung kann verstärkt werden, indem die Angaben, auf die der System-Anbieter seine Erklärung gründet, als Dokument bereitgehalten und auf Wunsch den interessierten Parteien verfügbar gemacht wird (s. ISO/IEC 17050-2:2004). Neben der Verstärkung des Vertrauens in die Erklärung kann solche Art der Dokumentation die zutreffenden Behörden in ihrer Überwachungstätigkeit unterstützen.
(2) Die unterstützende Dokumentation muss auf eine Weise entwickelt, aufbewahrt, gelenkt und aufrechterhalten werden, die eine Rückverfolgbarkeit der Selbstverpflichtungserklärung gestattet (s. ISO/IEC 17050-2:2004, Nr. 4.1).
(3) Die unterstützende Dokumentation muss mindestens für den laufenden und den vorangegangenen Zyklus aufbewahrt werden (s. ISO/IEC 17050-2:2004, Nr. 4.3).
(4) Es wird empfohlen, den Bewertungsbericht (s. § 5.2.9) als unterstützende Dokumentation bereitzustellen. Sollte der Bewertungsbericht nicht bereitgestellt werden (bspw. zur Wahrung der Vertraulichkeit), muss die unterstützende Dokumentation mindestens folgende Informationen enthalten (s. ISO/IEC 17050-2:2004, Nr. 5.1):
   (a) Detaillierte Beschreibung des Gegenstandes der Erklärung (basierend auf § 5.1.1), inkl. der Schutzklasse;
   (b) Beschreibung der nichtanwendbaren Kriterien sowie eine kurze Begründung, warum diese nichtanwendbar sind (s. § 5.2.7);
   (c) Ergebnisse der Bewertung, darunter
      (i) Beschreibung der verwendeten Bewertungsmethoden,
      (ii) Umfassende Darstellung der Ergebnisse der Bewertung pro Kriterium, und
      (iii) Beurteilungen von Ergebnissen einschließlich möglicher Abweichungen und Einschränkungen.
   (d) Bezeichnung von eingeschalteten Konformitätsbewertungsstellen und Wesentliches über deren Qualifikation und technische Kompetenz;
   (e) Informationen über durchgeführte Überwachungstätigkeiten (s. Nr. 5.4).
(5) Jede Änderung in der unterstützenden Dokumentation, die sich auf die Gültigkeit der Erklärung auswirkt, muss dokumentiert werden (s. ISO/IEC 17050-2:2004, Nr. 5.3).

§ 5.3.4 Gültigkeitsdauer und Aufrechterhalten der Selbstverpflichtungserklärung

(1) Die Selbstverpflichtungserklärung wird für eine Gültigkeitsdauer von zwei Jahren abgegeben. Die Frist beginnt mit dem in der Erklärung ausgewiesenen Datum.
(2) Der System-Anbieter kann vor oder nach Ablauf der Gültigkeitsdauer die Aufrechterhaltung der Selbstverpflichtungserklärung sicherstellen, indem er den Gegenstand der Selbstverpflichtung erneut durch eine Bewertung beurteilt.
(3) Der System-Anbieter kann die erneute Selbstverpflichtungserklärung bei rechtzeitig abgeschlossener Bewertung auf das Datum unmittelbar nach Ablauf der Gültigkeitsdauer der vorangegangenen Erklärung ausstellen.

5.4 Überwachung

§ 5.4.1 Durchführung von regelmäßigen Überwachungstätigkeiten

(1) Die Datenverarbeitungsvorgänge bedürfen während der Gültigkeitsdauer der Selbstverpflichtungserklärung eine Überwachung von Änderungen gemäß Nr. 4.2 (s. ISO/IEC 17050-1:2010, Nr. 10).
(2) Insbesondere wenn dieses Regelwerk oder der Kriterienkatalog neue oder überarbeitete Kriterien oder Anforderungen einführt oder sonstige Änderungen unterliegen, die den System-Anbieter betreffen, muss der System-Anbieter sicherstellen, dass diese Änderungen umgesetzt werden.
(3) Die Überwachung der Änderungen kann ergeben, dass Zwischenbewertungen erforderlich sind, um sicherzustellen, dass die Selbstverpflichtungserklärung weiterhin gültig ist.
(4) Für die Durchführung der Zwischenbewertung gelten die Anforderungen unter Nr. 5.2 analog, insb. die Anwendung geeigneter Bewertungsmethoden.
(5) Es ist empfohlen, dass der System-Anbieter als Nachweis über die Durchführung der Zwischenbewertungen eine Dokumentation bereitstellt, bspw. die Ergebnisse einer erneuten oder aktualisierten Bewertung.

§ 5.4.2 Feststellung der Nichteinhaltung von Kriterien und Fehlen der Vorrausetzungen für die Selbstverpflichtungserklärung

(1) Wenn der System-Anbieter aufgrund der Überwachungstätigkeiten, von Mitteilungen eines Dritten oder aufgrund sonstiger Umstände Grund zur Annahme hat, dass die Voraussetzungen für die Erklärung nicht vorlagen oder nicht mehr vorliegen, ergreift er unverzüglich die erforderlichen Maßnahmen, um das Vorliegen der Voraussetzungen festzustellen (s. ISO/IEC 17050-1:2010, Nr. 10.1, 10.2):

   (a) Der System-Anbieter kann insbesondere feststellen, dass eine Zwischenbewertung zur Aufrechterhaltung der Selbstverpflichtungserklärung erforderlich ist;
   (b) Der System-Anbieter kann feststellen, dass die Bewertung vollständig zu erneuern ist;
   (c) Der System-Anbieter kann basierend auf der Bewertung Maßnahmen zur Behebung der Missstände durchführen.

(2) Stellt der System-Anbieter die Erforderlichkeit einer Zwischenbewertung fest, so sollte diese in einer angemessenen Frist durchgeführt werden (in der Regel ein Monat).
(3) Der System-Anbieter trifft aufgrund seiner Feststellungen die erforderlichen Maßnahmen. Hierzu gehören:

   (a) Der System-Anbieter kann die Selbstverpflichtungserklärung für einen festgelegten Zeitraum vorbehaltlich der Abstellmaßnahmen aussetzen (s. § 5.4.3);
   (b) Der System-Anbieter kann die Selbstverpflichtungserklärung einschränken (s. § 5.4.4).
   (c) Der System-Anbieter kann die Selbstverpflichtungserklärung widerrufen (s. § 5.4.5).

§ 5.4.3 Aussetzung der Selbstverpflichtungserklärung durch den System-Anbieter

(1) Eine Aussetzung bezeichnet ein vorübergehendes Außerkraftsetzen der Selbstverpflichtungserklärung (s. ISO/IEC 17000:2004 Tz. 6.2).
(2) Der System-Anbieter kann die Selbstverpflichtungserklärung für die Dauer einer Zwischenbewertung und die anschließende Umsetzung von Abstellmaßnahmen aussetzen.
(3) Die Aussetzung wird sofort wirksam.
(4) Wenn die Selbstverpflichtungserklärung ausgesetzt wird, muss der System-Anbieter Maßnahmen ergreifen, um alle erforderlichen Veränderungen an formellen Dokumenten, öffentlichen Informationen, usw. vorzunehmen, um sicherzustellen, dass sie keinen Hinweis darauf geben, dass die Selbstverpflichtungserklärung weiterhin gültig ist. Hierzu zählt insbesondere auch die Entfernung der Datenverarbeitungsvorgänge aus dem Register des Eigners.
(5) Der System-Anbieter stellt sicher, dass die Werbung mit der Selbstverpflichtungserklärung eingestellt wird und definierte Maßnahmen zur Abstellung der Mängel und Nichtkonformitäten umgesetzt werden.

(6) Wenn die Selbstverpflichtungserklärung nach der Aussetzung wieder in Kraft gesetzt wird, muss der System-Anbieter alle Änderungen an formalen Dokumenten, öffentlichen Informationen, usw. vornehmen, um sicherzustellen, dass die Selbstverpflichtungserklärung wieder gültig ist (s. ISO/IEC 17065:2012 Tz. 7.11.6). Der System-Anbieter darf dann auch die Werbung mit der Erklärung fortsetzen.
(7) Der System-Anbieter informiert seine System-Kunden über die Aussetzung.

§ 5.4.4 Erweiterung oder Einschränkung der Selbstverpflichtungserklärung durch den System-Anbieter

(1) Der System-Anbieter kann jederzeit die Erweiterung oder Einschränkung der Selbstverpflichtungserklärung durchführen. Die Erweiterung bezeichnet die Erhöhung der Schutzklasse. Die Einschränkung eine Reduzierung der Schutzklasse.
(2) Bei einer Erweiterung muss der System-Anbieter eine erneute Bewertung durchführen, in dem er prüft, dass er die Kriterien des DIRECTIONS-Kriterienkatalogs der höheren Schutzklasse umsetzt. Der System-Anbieter bewertet die Ergebnisse und entscheidet über die Abgabe einer Erklärung mit höherer Schutzklasse.
(3) Der System-Anbieter informiert seine System-Kunden über die Einschränkung oder Erweiterung.

§ 5.4.5 Widerruf der Selbstverpflichtungserklärung durch den System-Anbieter

(1) Der Widerruf bezeichnet das Zurückziehen bzw. die eigenständige Rücknahme der Selbstverpflichtungserklärung (s. ISO/IEC 17000:2004 Tz. 6.3).
(2) Der System-Anbieter kann jederzeit die Selbstverpflichtungserklärung widerrufen.
(3) Die Selbstverpflichtungserklärung ist vom System-Anbieter zu widerrufen, wenn

(a) Der System-Anbieter feststellt, dass die Voraussetzungen für die Abgabe der Erklärung nicht vorlagen oder nicht mehr vorliegen;
(b) wenn eine Zwischenbewertung nicht oder nicht innerhalb der festgelegten und angemessenen Frist durchgeführt wird und der System-Anbieter dies zu vertreten hat;
(c) wenn der System-Anbieter in einer Weise schädigend auf den Bestand der Selbstverpflichtungserklärung wirkt, z.B. diskeditierend oder durch nicht zugelassene Werbung;
(d) wenn der System-Anbieter den Datenverarbeitungsvorgang nicht mehr am Markt anbietet.

(4) Wenn die Selbstverpflichtungserklärung widerrufen wird, muss der System-Anbieter Maßnahmen ergreifen, um alle erforderlichen Veränderungen an formellen Dokumenten, öffentlichen Informationen, usw. vorzunehmen, um sicherzustellen, dass sie keinen Hinweis darauf geben, dass die Selbstverpflichtungserklärung gültig ist. Hierzu zählt insbesondere die Entfernung des Datenverarbeitungsvorgangs aus dem Register des Eigners.
(5) Der System-Anbieter stellt die Werbung mit der Selbstverpflichtungserklärung ein.
(6) Der System-Anbieter informiert seine System-Kunden über den Widerruf.

§ 5.4.6 Aussetzung, Einschränkung und Widerruf der Selbstverpflichtungserklärung durch den Eigner

(1) Der Eigner führt keine eigenständige Überprüfung über die Einhaltung der Selbstverpflichtungserklärung durch. Insb. ist der Eigner **keine** Konformitätsbewertungsstelle und stellt daher auch **keine** Konformitätsaussagen aus.
(2) Der Eigner muss dennoch das Vertrauen des Marktes in und die Glaubwürdigkeit von DIRECTIONS sicherstellen und aufrechterhalten.
(3) Wenn der Eigner aufgrund von eigenen Feststellungen, Mitteilungen des System-Anbieters oder eines Dritten oder aufgrund sonstiger Umstände einen fundierten Grund zur Annahme hat, dass die Voraussetzungen für die Abgabe der Selbstverpflichtungserklärung nicht vorlagen oder nicht mehr vorliegen (s. auch § 5.3.1 und § 5.2.8), ergreift der Eigner erforderliche Maßnahmen, um die Vertrauenswürdigkeit und Glaubwürdigkeit von DIRECTIONS sicherzustellen.

(4) Der Eigner kann den System-Anbieter auffordern die Selbstverpflichtungserklärung auszusetzen, einzuschränken und zu widerrufen, insb. wenn

(a) die Voraussetzungen für die Abgabe der Erklärung nicht vorlagen oder nicht mehr vorliegen;
(b) keine Bewertung vom System-Anbieter durchgeführt worden ist (s. Kapitel 5.2);
(c) der System-Anbieter in einer Weise schädigend auf DIRECTIONS wirkt, z.B. diskreditierend oder durch nicht zugelassene Werbung;
(d) der System-Anbieter den Datenverarbeitungsvorgang nicht mehr am Markt anbietet;
(e) die für den System-Anbieter zuständige Datenschutz-Aufsichtsbehörde den Eigner auffordert, die Selbstverpflichtungserklärung aussetzen, einzuschränken oder zu widerrufen; oder
(f) der Eigner feststellt, dass der DIRECTIONS-Kriterienkatalog die gesetzlichen Vorgaben der Datenschutz-Grundverordnung und des BDSG oder die an deren Stelle tretenden gesetzlichen Bestimmungen nicht oder nicht mehr erfüllt. Dies gilt nicht, wenn der System-Anbieter unverzüglich eine erneute Bewertung nach einer neuen Version des DIRECTION-Kriterienkatalogs durchführt.

(5) Der Eigner hat dem System-Anbieter deutlich zu beschreiben, unter welchen Aspekten Zweifel an der Selbstverpflichtungserklärung bestehen oder welche anderen fundierten Gründe die Durchführung von Maßnahmen erfordern.
(6) Der Eigner gibt dem System-Anbieter vor seiner Entscheidung Gelegenheit zur Stellungnahme. Die Entscheidung des Eigners ist zu begründen und dem System-Anbieter in Textform zuzustellen.
(7) Die Aussetzung, die Einschränkung oder der Widerruf durch den Eigner wird spätestens drei Wochen nach Zustellung der Entscheidung über die Maßnahmen wirksam.
(8) Der System-Anbieter muss alle Maßnahmen unter § 5.4.3 im Falle einer Aussetzung, unter § 5.4.4 im Falle einer Einschränkung und unter § 5.4.5 bei einem Widerruf durchführen. Der Eigner kann insbesondere den System-Anbieter und seine Datenverarbeitungsvorgänge aus dem Register entfernen (s. § 4.3.2).
(9) Der System-Anbieter informiert seine System-Kunden über die durchgeführten Maßnahmen des Eigners.
(10) Es ist empfohlen, dass diese Anforderungen und Maßnahmen auch in der Vereinbarung zwischen dem Eigner und dem System-Anbieter festgeschrieben werden (s. § 4.3.1).

6 Literaturverzeichnis

DSK	Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO in Verbindung mit DIN EN ISO/IEC 17065. Version 1.4 (08.10.2020).
EDPB Annex 1	EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Annex 1. Version 3.0 Stand 04.06.2019
IAF MD 1:2018	Verbindliches IAF Dokument für die Auditierung und Zertifizierung von Managementsystemen in Organisationen mit mehreren Standorten (Deutsche Übersetzung des IAF Dokumentes „IAF MD 1:2018“); https://www.dakks.de/sites/default/files/dokumente/iaf_md_1-2018_auditierung_und_zertifizierung_von_managementsystemen_in_organisationen_mit_mehreren_standorten_uebersetzung_20181218_v1.0.pdf. Stand 29. Januar 2018
ISO/IEC 17000:2004	Begriffe und allgemeine Grundlagen. Stand 2004.
ISO/IEC 17021-1:2015	Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren – Teil 1: Anforderungen. Stand 2015
ISO/IEC 17024:2012	Konformitätsbewertung - Allgemeine Anforderungen an Stellen, die Personen zertifizieren. Stand 2012
ISO/IEC 17030:2009	Allgemeine Anforderungen an Konformitätszeichen einer dritten Seite. Stand 2009
ISO/IEC 17050-1:2010	Konformitätserklärung von Anbietern – Teil 1: Allgemeine Anforderungen. Stand 2010
ISO/IEC 17050-2:2004	Konformitätserklärung von Anbietern – Teil 2: Unterstützende Dokumentation. Stand 2004
ISO/IEC 17065:2012	Anforderungen an Stellen, die Produkte, Prozesse und Dienstleistungen zertifizieren. Stand 2012

7 Anhang A - Beispielhafte Funktionen von schulischen Informationssystemen

Die Funktionen in schulischen Informationssystemen können nach verschiedenen didaktischen Komponenten charakterisiert werden: Inhaltskomponente, Kommunikationskomponente, Aufgabenkomponente, Beurteilungskomponenten und Werkzeugkomponente.[7] Häufig sind diese Komponenten eng miteinander verzahnt, zum Beispiel Werkzeugfunktionen zum kollaborativen Arbeiten mit Kommunikationsfunktionen oder Aufgabenfunktionen mit Beurteilungsfunktionen. Die folgende beispielhafte Auflistung basiert auf aktuellen Angeboten am Markt und ist nicht abschließend.

Inhaltsfunktionen vermitteln die Lerninhalte. Dies kann insbesondere in schulischen Informationssystemen multimedial, interaktiv und adaptiv geschehen.

- Lernvideos und Audioinhalte
- Lernreisen
- Lerngeschichten
- Zusammenfassungen
- Weitere digitale Bildungsmedien

Kommunikationsfunktionen ermöglichen sowohl den synchronen und asynchronen Austausch zwischen Lehrenden und Lernenden als auch den Austausch Lernender untereinander. Zusätzlich können Kommunikationskomponenten auch für die Benachrichtigung z. B. der Erziehungsberechtigten verwendet werden.

- Audio und Video-Konferenzen
- Live-Feedback und Umfragen
- Messenger und Chatfunktionen
- Blogs, Foren und Gruppendiskussion
- Benachrichtigungen, Mitteilungen und Rundschreiben an Schüler und Erziehungsberechtigte
- Abwesenheiten melden
- Push-Erinnerungen

Aufgabenfunktionen ermöglichen die Bereitstellung und das Management von Aufgaben. Diese Aufgaben können verschiedene Grade der Interaktivität und Multimedialität haben (beispielsweise von digitalen Arbeitsblättern bis zu Lernspielen) und individuell oder in Gruppen bearbeitet werden.

- Aufgaben und Übungen planen, zuweisen und überprüfen
- Projekte und Gruppenaufgaben
- Lernspiele
- Vokabeltrainer
- Quizzes

Beurteilungsfunktionen ermöglichen – in schulischen Informationssystemen auch automatisiert - die Leistungsbeurteilung Lernender. Darüber hinaus können Beurteilungsfunktionen auch Rückmeldungen zu Leistungen und Lernfortschritt geben und individuelle Lernpläne enthalten.

- Prüfungen und Tests
- Ergebnisse, Feedback und Peer-Review
- Lernfortschritt verfolgen
- Notendurchschnitt
- Individuelle Lernpläne und Kompetenzraster

[7] *Bransford/Brown/Cocking* 2000, 133-136; *Kerres* 2009, 43–44; *Petko,* in Petko 2010, 15–18.

Werkzeugfunktionen ermöglichen die individuelle und kollaborative, kollektive Verarbeitung von Informationen und können für das Wissensmanagement werden. Außerdem können Werkzeugfunktionen die Vorbereitung und Anwendung anderer Komponenten durch administrative Funktionen unterstützen

- Digitale Tafeln und kollaborative Whiteboards
- Präsentationen durchführen und annotieren
- (Kollaborative) Dokumentbearbeitung
- Cloud-Speicher, Bibliotheken und Wikis
- Editoren für digitale Lerninhalte und Tools zur Einbindung externer Inhalte
- Kalender, Stundenpläne und Termin-Assistenten
- Klassen, Kurse und Gruppen anlegen und verwalten
- Rollen und Berechtigungen zuweisen und verwalten
- Berichte

8 Anhang B - Beispielhafte Selbstverpflichtungserklärung

Siehe ISO/IEC 17050-1:2010 Anhang A.