

DIRECTIONS-Zertifizierungsgegenstand

Executive Summary

Der Zertifizierungsgegenstand beschreibt das im Rahmen von DIRECTIONS zu überprüfende datenschutzkritische Untersuchungsobjekt auf Basis der Zertifizierungskriterien des DIRECTIONS-Kriterienkatalogs.

Für das DIRECTIONS-Zertifizierungsverfahren ist zusammenfassend festzuhalten, dass Datenverarbeitungsvorgänge in schulischen Informationssystemen den Zertifizierungsgegenstand bilden. Schulische Informationssysteme finden sich am Markt in sehr unterschiedlicher Form, sodass die konkrete Vorgangsreihe im Einzelfall zu bestimmen ist. Der konkrete Zertifizierungsgegenstand des DIRECTIONS-Zertifizierungsverfahrens muss diese Vielfalt erfassen, aber eine hinreichende Konkretisierungsstufe gegenüber den Vorgaben in Art. 42 DSGVO erreichen.

Bei der Bestimmung des Zertifizierungsgegenstands sind drei Komponenten wichtig, die System-Anbieter als Adressaten des DIRECTIONS-Zertifizierungsverfahrens beachten müssen: 1. personenbezogene Daten (sachlicher Anwendungsbereich der DSGVO), 2. technische Systeme (Infrastruktur, Hardware und Software, die genutzt werden, um personenbezogene Daten zu verarbeiten) und 3. Prozesse und Verfahren, die mit Verarbeitungsvorgängen in Verbindung stehen. Somit besteht ein Datenverarbeitungsvorgang in der Regel sowohl aus technischen und automatisierten als auch aus nicht-technischen organisatorischen Komponenten, die personenbezogene Daten zu einem bestimmten Zweck verarbeiten und deren Datenschutzmaßnahmen in Datenschutzkonzepten erfasst und zu Datenschutzmanagementsystemen zusammengefasst sind.

Im DIRECTIONS-Zertifizierungsverfahren können die Datenverarbeitungsvorgänge betrachtet werden, die der System-Anbieter als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) im Rahmen der Auftragsverarbeitung gemäß Art. 28 DSGVO durchführt 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) durchführt. Weiterhin müssen Datenverarbeitungsvorgänge bei einer Auftragsverarbeitung betrachtet werden, die der System-Anbieter als Verantwortlicher vornimmt, um den Vertrag mit dem System-Kunden über die Bereitstellung des schulischen Informationssystems schließen (bspw. Verarbeitung von Zahlungsdaten) und durchführen zu können sowie um rechtliche Pflichten zu erfüllen.

Durch die Festlegung des DIRECTIONS Zertifizierungsgegenstands werden die folgenden Ziele verfolgt: Schutz der Daten von Schülern, ggf. indirekter Schutz der Daten von Lehrkräften (Lehrkräfte im digitalen Klassenzimmer) und weiteren Person (z. B. Erziehungsberechtigte), Herausarbeitung von Use Cases der Schüler-zu-Schüler und Schüler-zu-Lehrkräfte Interaktion sowie Zertifizierung nach den Kriterien der DSGVO und Berücksichtigung weiterer einschlägiger Regularien. Nicht angestrebt wird die Zertifizierung von Schulen als System-Kunden und ihren Nutzern, die Herausarbeitung von Use Cases zur Interaktion von Lehrkräften untereinander, Use Cases zur Interaktion von Lehrkräften mit Erziehungsberechtigten, die Zertifizierung eingesetzter Subauftragsverarbeiter, der Beschaffungsprozess der schulischen Informationssysteme durch die Länder sowie die Europäisierung der Zertifizierung.

Ausführliche Informationen sind in der Langfassung des Zertifizierungsgegenstandes einzusehen (www.directions-cert.de).