Auftragsdatenverarbeitung und Datenschutz

Verarbeitung personenbezogener Daten im Auftrag nach § 7 des Landesdatenschutzgesetzes (LDSG) an Schulen

Bedient sich eine Schule einer Auftragsdatenverarbeitung, dann ist eine ganze Reihe von vor allem datenschutzrechtlichen Aspekten zu berücksichtigen. Im vorliegenden Artikel werden diese erläutert und Hintergründe dargestellt.

Dipl.-Phys. Thomas J. Eckert

Einleitung

Durch zunehmend komplexer werdende Anwendungen auf der einen, aber durch den steigenden Kostendruck auf der anderen Seite, können oder wollen immer mehr Schulen die gesamte EDV oder Teile davon nicht mehr selbst betreiben. Hinzu kommen Angebote wie z.B. von BelWue zur Nutzung von Moodle oder verschiedene andere web-basierte Services, teilweise als Cloud-Computing. In der Konsequenz wird also die EDV oder zumindest ein Teil davon nicht durch die Schule selbst, sondern von einem Dritten als Dienstleister betrieben.

Bedient sich nun eine Schule einer solchen Auftragsdatenverarbeitung, dann ist eine ganze Reihe von vor allem datenschutzrechtlichen Aspekten zu berücksichtigen.

Das Kultusministerium hat zudem – als Hilfestellung – eine Vertragsvorlage für eine Auftragsdatenverarbeitung geschaffen, die von Schulen genutzt werden kann. Der vorliegende Artikel soll auch bei der Nutzung dieser Vorlage helfen.

Der Artikel beleuchtet die Auftragsdatenverarbeitung alleine aus datenschutzrechtlicher Sicht. Selbstverständlich müssen neben datenschutzrechtlichen Aspekten noch weitere Rahmenbedingungen wie z.B. Fragen zur Gewährleistung, zum Gerichtsstand aber auch Vergütungsfragen berücksichtigt werden. Dies könnte beispielsweise durch die Verwendung der vom Kooperationsausschuss Datenverarbeitung Bund/Länder/Kommunaler Bereich (KoopA-ADV) erarbeiteten »Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT)« geschehen.

Was ist eine Auftragsdatenverarbeitung?

Aus datenschutzrechtlicher Sicht spricht man von einer Verarbeitung personenbezogener Daten im Auftrag oder kurz Auftragsdatenverarbeitung, wenn die eigentliche Verarbeitung personenbezogener Daten durch andere Personen oder Stellen außerhalb der Schule, also durch einen Dienstleister erfolgt. Dieser Dienstleister ist dann Auftragnehmer der Schule. Dabei spielt es keine Rolle, ob die Daten lediglich gespeichert oder auf eine andere Weise verarbeitet, also z.B. erhoben, verändert oder übermittelt werden. Als andere Stellen können auch öffentliche Einrichtungen zählen, so auch der Schulträger, der in vielen Fällen die EDV von Schulen betreut oder gar in seinem eigenen Rechenzentrum betreibt. Es kann auch dann eine Auftragsdatenverarbeitung vorliegen, wenn die Verwendung einer Anwendung für eine Schule verpflichtend vorgeschrieben ist, wie z.B. ASD-BW oder die Kompetenzanalyse Profil AC.

Übrigens gelten auch Wartungstätigkeiten oder damit vergleichbare Hilfstätigkeiten, also beispielsweise die Wartung der Serverhardware oder die Administration des Betriebssystems dann als Auftragsdatenverarbeitung, wenn dies durch Personal eines externen Dienstleisters außerhalb der Schule durchgeführt wird.

Was bedeutet das in der Praxis?

Für die Schule ist es ganz wichtig zu wissen, dass mit einer solchen Beauftragung die datenschutzrechtliche Verantwortung nach wie vor bei der Schule selbst bleibt: die Schule ist also – trotz Auftragsdatenverarbeitung – verantwortliche Stelle. Damit ist sie dafür verantwortlich, gegenüber den Betroffenen eine eventuell gewünschte Auskunft darüber zu erteilen, welche personenbezogenen Daten verarbeitet werden. Ferner bleibt die Schule dafür verantwortlich, dass die Datenverarbeitung rechtmäßig, also rechtlich zulässig erfolgt, insbesondere im Hinblick auf die verarbeiteten Daten. Dies ist schon deswegen wichtig, weil manches von Dienstleistern angebotene Software-Produkt die Verarbeitung von mehr Daten zulässt, als von Gesetzes wegen erlaubt. So ist eine Schulverwaltungssoftware mitunter in der Lage, Passbilder von Schülern zur elektronischen Schülerakte zu nehmen, was jedoch unzulässig ist, weil dies für die Erfüllung des Erziehungs- und Bildungsauftrages der Schule nicht erforderlich ist. Auch liegt es in der Verantwortung der Schule, sicherzustellen, dass die Daten entsprechend den Vorschriften rechtzeitig gelöscht werden. Zudem

bleibt die Verantwortung zum Führen eines Verfahrensverzeichnisses weiterhin bei der Schule.

Die Schule trägt ferner die Verantwortung für die zu treffenden technischen und organisatorischen Maßnahmen; auch für die Maßnahmen, die beim Dienstleister getroffen werden. Genau dies zeigt sich jedoch in der Praxis als größte Schwierigkeit, denn oft ist der Schule gar nicht bekannt, welche konkreten Maßnahmen ein Dienstleister treffen muss, zumal an Schulen die datenschutzrechtliche und technische Kompetenz dafür meist nicht vorhanden ist. Doch so schwierig ist es nicht, die zu treffenden Maßnahmen festzulegen. Denn professionelle Dienstleister haben in der Regel bereits von sich aus ein ganzes Bündel von Maßnahmen getroffen: angefangen bei der Zutrittssicherung des Rechenzentrums bis hin zu diversen Protokollierungen und Datensicherungen. Diese Maßnahmen müssen somit schlicht nur detailliert aufgelistet werden. Zudem sollte man seinen Dienstleister möglichst dazu verpflichten, für die geplante Auftragsdatenverarbeitung ein konkretes, anwendungsspezifisches Datenschutz- und Sicherheitskonzept zu erstellen. Entsprechende Hinweise sind in den vom Kultusministerium zur Verfügung gestellten Vorlagen bereits eingearbeitet.

Sorgfaltspflicht bei der Auswahl des Dienstleisters

Bevor eine Datenverarbeitung überhaupt beginnen kann, muss die Schule sich den potenziellen Auftragnehmer genau anschauen. Ist dieser – aus fachlichen Gründen – überhaupt dazu fähig, die Datenverarbeitung so durchzuführen, wie es die Schule sich vorstellt? Ist der Auftragnehmer überhaupt in der Lage, Datenschutzmaßnahmen zu treffen? Ist dem Dienstleister der Datenschutz überhaupt ein Begriff?

Um das herauszufinden, sollte man sich mit dem potenziellen Auftraggeber einmal zusammensetzen und sich die Datenschutzmaßnahmen erläutern lassen. Wo befinden sich seine Server? Wie sind diese gesichert? Was wird protokolliert? Usw. Verfügt der Dienstleister über ein Datenschutz- und Sicherheitskonzept? Handelt es sich um ein Rechenzentrum, dann sollte der Dienstleister über eine Übersicht der nach § 9 Abs. 3 LDSG getroffenen technischen und organisatorischen Maßnahmen verfügen. Hat der Dienstleister eine Referenzliste? Arbeitet er schon für andere Schulen? Dann könnte man sich bei diesen anderen Kunden über den Dienstleister erkundigen

Darüber hinaus kann es hilfreich sein, wenn der Dienstleister eine Zertifizierung, etwa nach dem Grundschutz des Bundesamtes für die Sicherheit in der Informationstechnik (BSI-Grundschutz) vorweisen kann. Dabei ist in jedem Fall darauf zu achten, dass auch das Grundschutz-Modul »Datenschutz« vom Zertifikat mit umfasst wird.

Anbieter, die Server außerhalb der EU betreiben, US-amerikanische Unternehmen oder Cloud-Computing Anbieter, die nicht transparent machen, in welchen Ländern und auf welchen Servern eine Datenverarbeitung erfolgt, kommen als Dienstleister überhaupt nicht infrage.

Form und Inhalt des Vertrages mit dem Auftragnehmer

Generell gilt, dass die Beauftragung immer schriftlich zu erfolgen hat. Um es vorweg zu nehmen: Dienstleister, bei denen es nur möglich ist, in vorgefertigte, bspw. im Internet bereitgestellte AGBs oder Nutzungsbedingungen einzuwilligen, erfüllen die rechtlichen Anforderungen des LDSG in der Regel nicht. Falls mit solchen Anbietern keine andere vertragliche Vereinbarung (z.B. entsprechend der Vorlage des KM) abgeschlossen werden kann, ist eine Beauftragung nicht zulässig.

Der genaue Inhalt des Auftrages ergibt sich aus § 7 LDSG.

- Zunächst sind Gegenstand und der Umfang der Datenverarbeitung darzustellen: Welche personenbezogenen Daten sollen überhaupt verarbeitet werden? Bei einer Darstellung dieser Daten muss auch an »technische Daten«, wie etwa Protokoll- oder log-Dateien gedacht werden, die z.B. bei der Nutzung von Internetportalen entstehen. Auf welcher Software, also mittels welcher Computerprogramme, erfolgt die Verarbeitung? Was wird mit den Daten durchgeführt, wie werden diese Daten verarbeitet? Werden diese lediglich beim Dienstleister gespeichert? Finden Übermittlungen oder Veröffentlichungen statt?
- Als nächstes müssen im Auftrag die notwendigen und zu treffenden technischen und organisatorischen Maßnahmen vollständig aufgeführt werden. Es genügt dabei nicht, lediglich in allgemeiner Form darzustellen, dass beispielsweise eine Transportkontrolle realisiert wird. Es muss vielmehr zu allen der in § 9 Abs. 3, Nr. 1 bis 11 LDSG genannten Kontrollen detailliert, konkret und nachvollziehbar erläutert werden, auf welche Weise, also durch welche Maßnahme diese realisiert wird. In unserem Beispiel könnte also aufgeführt sein, dass zur Transportkontrolle die übertragenen Daten mittels des Verschlüsselungsprogramms TrueCrypt per Verschlüsselungsalgorithmus AES-256 verschlüsselt sind. Das vom Auftragnehmer erstellte Datenschutz- und Sicherheitskonzept ist dem Auftrag als Anlage beizufügen, um dieses zum Vertragsbestandteil zu machen.

- Der Auftrag muss ferner Ausführungen darüber enthalten, ob und unter welchen Bedingungen der Auftragnehmer Unterauftragsverhältnisse begründen kann. Dabei geht es darum, festzulegen, inwieweit der Auftragnehmer seinerseits weitere Dienstleister, also weitere Unternehmen, Stellen oder Personen außerhalb seiner eigenen Einrichtung zur Leistungserbringung hinzuziehen kann. Empfehlenswert ist es, zu regeln, dass der Auftragnehmer erst nach vorheriger schriftlicher Zustimmung durch die Schule Unterauftragsverhältnisse begründen kann.
- Im Auftrag muss aufgeführt sein, dass die Schule die Befugnis besitzt, dem Auftragnehmer hinsichtlich der Verarbeitung personenbezogener Daten Weisungen zu erteilen. Dies ist schon deshalb wichtig, um bei der Verarbeitung eventuell auftretenden Fehlern wirksam begegnen zu können.
- Zudem muss der Auftragnehmer dazu verpflichtet werden, dass technische und funktionale Änderungen der Verarbeitung erst nach vorheriger Zustimmung der Schule erfolgen dürfen. Nur dann kann die Schule ihrer Pflicht als verantwortliche Stelle nachkommen.
- Die Schule sollte sich ggf. zusammen mit einer von der Schule beauftragten Stelle das Recht sichern, die Betriebsstätten des Dienstleisters zu besuchen, um sich dort selbst ein Bild zu verschaffen, ob und inwieweit der Dienstleister die vertraglichen Vereinbarungen und datenschutzrechtlichen Vorschriften einhält (Kontrollbefugnis). Auf welcher Weise Sie dieser Kontrolle nachgehen können, wird weiter unten noch detailliert dargestellt.
- Darüber hinaus sollte der Dienstleister dazu verpflichtet werden, dass er seinerseits seine Mitarbeiter auf das Datengeheimnis nach § 6 LDSG verpflichtet.

Vorlage für eine Beauftragung

Weil die rechtliche Situation sehr kompliziert ist und umfangreiche Details zu berücksichtigen sind, hat das Kultusministerium, wie schon angeführt, einen Vertragsentwurf geschaffen, der allen Schulen zur Verfügung steht.

→ Praxis-Tipp:

Die Vorlage für eine Beauftragung finden Sie im Intranet der Kultusverwaltung und unter www.it.kultus-bw.de, sowie auf dem Lehrerfortbildungsserver lehrerfortbildung-bw.de. Dort finden Sie auch Erläuterungen sowie Ausfüllhinweise für den Vertragsentwurf.

Kontrolle durch die verantwortliche Stelle

Die Schule als verantwortliche Stelle muss sich im Verlaufe der Verarbeitung hin und wieder davon überzeugen, dass sich der Auftragnehmer tatsächlich an die vertraglichen Vereinbarungen hält. Dies kann beispielweise dadurch geschehen, dass der behördliche Datenschutzbeauftragte, sofern ein solcher bestellt ist, sich vor Ort selbst ein Bild davon verschafft, inwieweit der Dienstleister den Vertrag einhält. Der Datenschutzbeauftragte kann sich beispielsweise erläutern und konkret zeigen lassen, wie die vereinbarten technischen und organisatorischen Maßnahmen konkret umgesetzt sind. So könnte man sich die baulichen (Sicherheits-)Einrichtungen des Rechenzentrums erläutern lassen, ferner kann man sich, um ein weiteres Beispiel anzuführen, Eingabeprotokollierungen der EDV-Systeme zeigen lassen. Eine solche Überprüfung durch die Schule könnte auch dadurch geschehen, dass mehrere Schulen, die denselben Auftragnehmer haben, kooperieren: Die Schulen könnten gemeinsam eine kundige Person, z.B. von einer der Schulen bestimmen, die dann eine solche Begehung durchführt. Ferner könnte auch eine vom Auftragnehmer veranlasste, regelmäßig aktualisierte datenschutzrechtliche Zertifizierung (BSI-Grundschutz incl. Modul Datenschutz) durch einen zugelassenen Dienstleister quasi als »Kontrollersatz« erfolgen.

Fazit

An vielen Schulen erfolgt bereits jetzt eine Verarbeitung personenbezogener Daten im Auftrag durch einen Dritten. Zukünftig wird die Zahl der Auftragsdatenverarbeitungen wohl noch weiter zunehmen. Durch eine Auftragsdatenverarbeitung bleibt die Schule nach wie vor die datenschutzrechtlich verantwortliche Stelle. Lediglich die Datenverarbeitung an sich erfolgt durch einen Dritten. Dabei müssen eine Menge von zum Teil anspruchsvollen rechtlichen Aspekten berücksichtigt werden. Durch die richtige Verwendung der vom Kultusministerium bereitgestellten Vertragsvorlage kommt die Schule ihrer gesetzlichen Pflicht nach und erreicht Rechtssicherheit. Das Kultusministerium hat hierfür zur Arbeitserleichterung auch eine Ausfüllhilfe zur Verfügung gestellt. ■

Dipl.-Phys.
Thomas J. Eckert
Kultusministerium
Baden-Württemberg