Der Digitalpakt Schule
Eine datenschutzrechtliche Herausforderung

Dr. Eric Heitzer[1]

Übersicht

---

* Der Autor ist zertifizierter Datenschutzbeauftragter und in dieser Funktion für rund 30 Unternehmen in Europa tätig. Von 1998-2010 verantwortete er in der Geschäftsleitung namhafter Telekommunikationsunternehmen die Bereiche Regulatory Affairs und Public Policy.

Executive Summary

- Die Umsetzung eines individuellen Netzwerkkonzeptes und ein professionelles Management des Netzwerks sind unabdingbare Voraussetzung für die gewünschte Digitalisierung in den Schulen.

- Die Administration des Netzwerks ist sicherheitsrelevant und zugleich ein Teil der gesetzlich vorgeschriebenen technischen und organisatorischen Maßnahmen, die den Schutz personenbezogener Daten von Schülern, Lehrern und allen anderen Nutzern bezwecken. Die Vergabe an professionelle Dienstleister stellt eine legitime und effiziente Lösung für die Mehrzahl der Schulen dar.

- Cloud-Lösungen sind als Variante der Dienstevergabe zulässig, wenn sie im Rahmen einer Auftragsverarbeitung nach den Regeln des europäischen Datenschutzrechts realisiert werden.

- Anbieter in den USA erfüllen diese Voraussetzungen trotz bilateraler Zusicherungen und/oder Unterwerfung unter den sogenannten Privacy-Shield nicht, weil die dortige Gesetzgebung einen unkontrollierbaren Zugriff amerikanischer Behörden auf die personenbezogenen Daten aller Nutzer ermöglicht und so in einem unauflösbaren Widerspruch zu den europäischen Regelungen steht.

- Ein kompetenter Cloud-Anbieter mit Sitz und Rechenzentrum in der EU gewährleistet demgegenüber die Einhaltung des datenschutzrechtlichen Schutzniveaus, so wie es gesetzlich Pflicht ist. Nur so kann vor einer missbräuchlichen Nutzung der Daten maximaler Schutz erlangt werden.

Vorwort

Welchen Einfluss nimmt Schule auf die Entwicklung von Kindern? Was ist das Ergebnis von meist 12 oder 13 Jahren schulischer Ausbildung? Und warum spielt Datenschutz in diesem Zusammenhang eine große Rolle?

Die Antworten auf diese Fragen müssen individuell ganz unterschiedlich ausfallen; gemein ist ihnen aber das Umfeld: Kinder wachsen in der Schule zu Erwachsenen heran und beginnen, aktiv am gesellschaftlichen Leben Teil zu nehmen. Im positiven Sinne prägend ist es, wenn sie dabei die Erfahrung machen, dass Gedanken, Meinungen und Gefühle möglichst offen und ohne Angst vor Abwertung oder Bestrafung geäußert werden können. In der Psychologie ist für eine solche Umgebung der Begriff des geschützten Raums geprägt worden.

Diese - positiv - prägende Erfahrung ist aber nur möglich, wenn Aussagen, Inhalte und die gesamte Kommunikation nicht unkontrolliert den geschützten Raum verlassen, in falsche Hände geraten und von Dritten - etwa zu bloßstellenden, diffamierenden oder auch werblichen Zwecken - missbraucht werden.

Damit ist das Tor zum Datenschutzrecht durchschritten: Manifestierte Äußerungen - etwa in Chats, E-Mails oder anderen Dokumenten - sind geschützt und zwar in Papier wie in digitaler Form. Richtig verstanden dient dies dem Recht des Einzelnen auf informationelle Selbstbestimmung, so wie es das Bundesverfassungsgericht bereits 1983 herausgearbeitet hat[2] und wie es seit Inkrafttreten der europäischen Regelungen am 25. Mai 2018[3] in den Fokus öffentlichen Interesses gerückt ist.

Unstrittig gelten die dortigen Regelungen nicht nur für Unternehmen, sondern auch für Einrichtungen der öffentlichen Hand. Ein besonderes Augenmerk gilt dabei den Schulen, für die die Digitalisierung im Einklang mit den datenschutzrechtlichen Bestimmungen zu einer großen Aufgabe geworden ist.

Die Studie beschreibt die rechtliche und tatsächliche Ausgangssituation und zeigt hiervon ausgehend Lösungswege auf, mit welchen die Schulen das Potenzial der Digitalisierung effizient und zugleich datenschutzkonform erschließen können.

---

[2] BVerfGE 65, 1 (Volkszählungsurteil vom 15.12.1983)

[3] VO 2016/679 des europäische Parlaments, Datenschutzgrundverordnung (DSGVO), abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=LEGISSUM:310401_2&from=DE

1. Schulen und Digitalisierung - Eine Bestandsaufnahme

Lesen, Schreiben, Rechnen, die Fähigkeit, Inhalte zu verstehen und Probleme zu lösen - dies sind seit jeher die zentralen Bildungsinhalte an Grund- und weiterführenden Schulen. Auf dem Weg dorthin stehen heute moderne Technologien bereit, die eine kompetente Nutzung erfordern. Diese Nutzung will erlernt werden, denn Studien zufolge führt die bei den Schülern vorhandene digitale Affinität alleine nicht zu einer Verbesserung oder Entwicklung digitaler Kompetenz. Erforderlich ist vielmehr das Erlernen von Informationsmanagement-Fähigkeiten auf einem abstrakten Niveau[4]. Das ist eine anspruchsvolle Aufgabe, denn der Gaming-Industrie ist es in den vergangenen Jahren gelungen, Schülern eine konkrete digitale Problemlösungskompetenz zu vermitteln. Tatsächlich bezieht sich diese Kompetenz aber fast ausschließlich auf virtuelle Spielumgebungen und hat mit den Anforderungen des wahren Lebens und spezifisch des Berufslebens oft nur wenig gemeinsam.

Auch Lehrer stellt die Digitalisierung vor große Herausforderungen: In seinem Buch Digitalisierung für Nachzügler beschreibt Christoph Schmidt diese wie folgt:

> *„Solange ich nicht weiß, wie ich mit ganz neuen Herausforderungen umgehen soll, reagiere ich verständlicherweise mit Zurückhaltung und Skepsis. Erst recht, wenn ich durch Schule und Erziehung nie darauf vorbereitet wurde. Wenn ich die nötigen Fähigkeiten nicht entwickeln konnte, und wenn mein Umfeld voll von verunsicherten Menschen steckt. Dann liegt „Blockieren" nahe"*[5].

Dieses Dilemma zwischen vermeintlich vorhandener Kompetenz auf Schüler- und unzureichender Lehrbefähigung auf Lehrerseite löst der Gesetzgeber mit einem klaren verfassungsrechtlichen Auftrag in Art. 7 GG, den die Länder in den Schulgesetzen in inhaltlich ähnlicher Weise umsetzen. Beispielhaft sei auf Art. 2 BayEuG verwiesen. Hiernach haben Schulen insbesondere die Aufgabe,

> *„Kenntnisse und Fertigkeiten zu vermitteln und Fähigkeiten zu entwickeln, (und) zu selbständigem Urteil und eigenverantwortlichem Handeln zu befähigen, und*
>
> *„auf Arbeitswelt und Beruf vorzubereiten, in der Berufswahl zu unterstützen".*

Schulen sind daher nicht nur gesetzlich verpflichtet, sondern geradezu prädestiniert, den Schülern eine kompetente Nutzung von Informationen und Daten ebenso zu vermitteln wie ein Verständnis für digitale Infrastrukturen und einen intelligenten Umgang mit Endgeräten. All dies dient auch dem Zweck, die Schüler auf eine weitgehend bereits digitalisierte Arbeitswelt vorzubereiten.

Um diesem Ziel gerecht zu werden, müssen die meisten Schulen allerdings noch nennenswert Aufholarbeit leisten: Einer repräsentativen Studie der BITKOM aus dem Jahre 2015 zufolge hapert es in vielen Schulen noch an der technischen Ausstattung: So sei die Anzahl der Endgeräte

---

[4] Veronica Rodriguez Rochette, 29.4.2019 in: www.digitalexpert.ch

[5] Christoph Schmitt, Digitalisierung für Nachzügler: Einsichten eines digitalen Immigranten, Kindle Version, Positionen 257 ff.

unzureichend, die installierte Technik funktioniere nicht einwandfrei, weil Geräte und Software häufig veraltet seien, und während Whiteboards immerhin an jeder zweiten Schule vorhanden seien, fehle es meist an Tablets oder E-Book-Readern.

Sehr uneinheitlich sei auch der Zustand der vorhandenen Infrastruktur und ihrer Pflege: Teilweise seien Netzwerke vorhanden, die vielfach von technikaffinen Lehrern gepflegt werden. Einer Studie des Meinungsforschungsinstituts FORSA aus dem Jahr 2019 zufolge, bei welcher 1.232 Schulleitungen allgemeinbildender Schulen befragt wurden, setzen 59 % der Schulen zur Pflege zusätzliches IT-Fachpersonal ein und an 4 % der Schulen kommen externe Dienstleister zum Einsatz. Zugang zu schnellem Internet und WLAN gibt es allerdings nur in jeder dritten Schule in allen Klassen und Fachräumen. Bei Gymnasien beläuft sich der Anteil auf immerhin 45 %.[6]

Im Hinblick auf die Digitalkompetenz der Lehrer gaben 72 % der befragten Lehrer an, sich privat fortzubilden; 65 % der Lehrkräfte nahmen an dienstlichen Fort- und Weiterbildungen teil und 58 % bildeten sich im Dialog mit Kollegen fort.

Die Ausgangssituation an Schulen ist mithin uneinheitlich und insgesamt ausbaufähig. Dies betrifft die vorhandenen IT-Strukturen ebenso wie deren Nutzung durch die Beteiligten.

2. Rechtliche Grundlagen

2.1 Die Verwaltungsvereinbarung Digitalpakt Schule vom Mai 2019

Vor dem Hintergrund der oben skizzierten Ausgangslage hat die Bundesrepublik Deutschland auf Grundlage von Art. 104 c GG mit den Bundesländern im Mai 2019 eine auf fünf Jahre befristete Vereinbarung getroffen, welche Finanzhilfen des Bundes an die Länder in Höhe von 5 Milliarden € für Digitalisierungsmaßnahmen an Schulen vorsieht. Voraussetzung zur Erlangung der Förderung ist die Übernahme eines investiven Eigenanteils durch die Bundesländer in Höhe von mindestens 10 %. Das Gesamtvolumen des Digitalpaktes Schule beläuft sich somit auf 5,5 Milliarden € - wenn die entsprechenden Anträge gestellt und bewilligt werden.

2.2 Umsetzungsmaßnahmen der Länder

Voraussetzung für die Erlangung der Finanzhilfen sind entsprechende Umsetzungsmaßnahmen der Länder, etwa in Form von Richtlinien, in denen insbesondere das Antragsverfahren ausgestaltet werden muss. Stand heute (Oktober 2019) sind alle Bundesländer tätig geworden und haben in unterschiedlicher Form das Antragsverfahren geregelt[7]. Als einziges Bundesland hat Hessen die auf das Land entfallenden Bundesmittel i. H. v. 372 Mio. € auf knapp 500 Mio. € aufgestockt.

---

[6] https://www.vbe.de/presse/pressedienste-2019/schneckentempo-digitalisierung-an-schulen-kommt-zu-langsam-voran, vgl. auch: Bericht des MERKUR vom 7.5.2019

[7] Baden-Württemberg: 15.8.2019

3. Die datenschutzrechtliche Problematik

Die förderfähigen Maßnahmen betreffen ganz besonders die Infrastruktur und hier die Errichtung und den Betrieb eines Netzwerks, welches sodann Voraussetzung für die Nutzung von Lernplattformen sowie den Betrieb digitaler Arbeitsgeräte ist, beides Maßnahmen, welche ebenfalls - separat - gefördert werden. Dies ergibt sich aus § 3 Digitalpakt i. V. m. den insoweit übereinstimmenden Richtlinien und Bestimmungen der Länder. Dem liegt offensichtlich der Wunsch - zumindest die Option - zugrunde, dass die Schulen grundsätzlich eigene Infrastrukturen etablieren, über die hierauf laufenden Dienste selber entscheiden und dieses Netz - wenn auch nicht zwingend vollständig - selbst administrieren. Netzbetrieb und Nutzung durch Schüler, Lehrer und vielleicht noch weitere Beteiligte, etwa Eltern, sind ohne die Verarbeitung einer Vielzahl personenbezogener Daten nicht vorstellbar. Damit ist der Anwendungsbereich des Datenschutzrechts eröffnet.

Im Kern will das durch die Datenschutzgrundverordnung (DSGVO) heute europäisch kodifizierte Datenschutzrecht die von einer Datenverarbeitung betroffenen Personen schützen. Es geht also darum, die personenbezogenen Daten all derer zu schützen, die das Datennetzwerk einer Schule nutzen oder deren Daten entweder nutzungsbezogen oder aus anderen Gründen dort verarbeitet werden[8].

4. Die Schule als Normadressat

Normadressat des Datenschutzrechts ist insofern die einzelne Schule. Diese ist Verantwortliche im Sinne von § 4 Nr. 7 der europäischen Datenschutzgrundverordnung (DSGVO) und nicht der Schulträger. Dies ergibt sich aus den insoweit übereinstimmenden landesrechtlichen Bestimmungen. Exemplarisch genannt seien die Bestimmungen in NRW: Hier regelt § 3 SchulG NRW, dass die

---

Bayern: 30.7.2019
Berlin: Pressemitteilung und Infobriefe liegen vor
Brandenburg: 31.7.2019
Bremen: 25.7.2019
Hamburg: 20.5.2019
Hessen: Programm liegt vor
Mecklenburg-Vorpommern: Erklärung Digitalpakt liegt vor
Niedersachsen: 8.8.2019
Nordrhein-Westfalen: 11.9.2019
Rheinland-Pfalz: 26.7.2019
Saarland: Handout liegt vor
Sachsen: 21.5.2019
Sachsen-Anhalt: Eckpunkte liegen vor
Schleswig- Holstein: Zeitplan liegt vor
Thüringen: 12.7.2019
Württemberg: 15.8.2019
Bayern: 30.7.2019
Berlin: Pressemitteilung und Infobriefe liegen vor

Schule in Bezug auf ihre inneren Angelegenheiten eigenverantwortlich handelt. Zu diesen inneren Angelegenheiten zählt auch die Verarbeitung personenbezogener Daten. Die ausführende Verordnung über die zur Verarbeitung zugelassenen Daten von Schülern und Eltern regelt in Folge dessen in § 1 Abs. 3 SchulG NRW:

> *„Für die Schule stellt die Schulleiterin oder der Schulleiter, […] durch technische oder organisatorische Maßnahmen sicher, dass der Schutz der verarbeiteten Daten gemäß § 10 DSG NRW gewährleistet ist und die Löschungsbestimmungen eingehalten werden."*

Damit ist das in der Praxis oft komplizierte und von Eingriffen des finanzierenden Schulträgers in die Autonomie der Schule nicht freie Verhältnis datenschutzrechtlich eindeutig geklärt: Die einzelne Schule ist allein für die Einhaltung der gesetzlichen Bestimmungen verantwortlich.

Dass Schule und Schulträger gleichwohl im Interesse einer effizienten Prozessgestaltung auch bei Fragen des Datenschutzes zusammenarbeiten müssen, ergibt sich aus der Ausgestaltung des Antragsverfahrens für die Fördermaßnahmen: Dieses sieht in § 3 Abs. II nämlich - neben den Bundesländern - den Schulträger als Antragsteller vor und nicht die einzelne Schule. Wenn aber der Schulträger Anträge stellt, so betreffen diese die datenschutzrechtlichen Belange der Schule. Ein Antrag etwa, welcher die Errichtung und Pflege einer komplexen IT-Infrastruktur betrifft und in datenschutzrechtlicher Hinsicht eine kompetente Betreuung durch eigenes Personal erfordert, darf nicht gestellt werden, wenn dieses Personal für die Schule nicht verfügbar ist. Abstimmung und Zusammenarbeit im Vorfeld der Antragstellung sind insoweit nicht nur Ausdruck von Effizienz, sondern geradezu rechtlich verpflichtend. Aus Sicht der Schule ergibt sich dies schlussendlich auch daraus, dass sie allein als Verantwortliche dafür geradesteht und haftet, dass die vom Schulträger für die Schule beantragten Maßnahmen datenschutzrechtlich einwandfrei umgesetzt werden können und beispielsweise ein implementiertes System auch in Übereinstimmung mit allen datenschutzrechtlichen Vorgaben von der Schule betrieben wird.

5. Spezifische datenschutzrechtliche Verpflichtungen für Schulen

Zum Katalog förderfähiger Maßnahmen gehört in erster Linie der Aufbau und Betrieb eines Netzwerks als Grundlage für alle weiteren Dienste. Diese Dienste werden zumeist für bestimmte Gruppen von Nutzern über virtuelle lokale Netzwerke bereitgestellt. Hieraus resultieren datenschutzrechtliche Verpflichtungen, die im Prinzip denen eines mittelständischen Unternehmens entsprechen.

Was bedeutet dies?

5.1 Information & Zustimmung

Die Schule muss alle Nutzer - datenschutzrechtlich die Betroffenen - in angemessener Weise über die Datenverarbeitung informieren (Art. 12-14 DSGVO). Dies bezieht sich vor allem auf Angaben

zum Zweck der Verarbeitung, Angaben zu den verarbeiteten Daten selber sowie Hinweisen zu Rechten, welche die Betroffenen haben (Art. 15-21 DSGVO). Wenn die Nutzung außerhalb eines Vertragsverhältnisses erfolgt - dies wird man immer dann annehmen können, wenn die Verarbeitung nicht das Verhältnis Schüler-Schule und den verfassungsrechtlichen Bildungsauftrag als Zweck betrifft - ist darüber hinaus regelmäßig eine Einwilligung der Betroffenen erforderlich, die wiederum sachgerecht zu gestalten ist (Art. 6-8 DSGVO).

Die geschilderten rechtlichen Anforderungen an Information und Einwilligung können nach einem guten Jahr Praxiserfahrung mit der DSGVO als bekannt vorausgesetzt werden. Hinweise und Aufsätze hierzu sind ebenso wie eine Vielzahl von Vorlagen - wenn auch in höchst unterschiedlicher Qualität - im Internet verfügbar. Die rechtlich gebotene Kommunikation mit den Betroffenen stellt Schulen nicht vor hohe Hürden.

5.2 Technikgestaltung - Netzwerk

An der Schnittstelle von Recht und Technik findet sich die zentrale Anforderung des Datenschutzrechts, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die personenbezogenen Daten der Betroffenen zu schützen (insbesondere Art. 24, 25, 28 DSGVO). Die zitierten Regelungen haben die gesamte IT im Auge und hierbei auch die Beschaffung, anlässlich derer datenschutzrechtliche Anforderungen von vornherein berücksichtigt werden müssen (Stichwort: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellung).

Worum geht es dabei?

Typischerweise zu beschaffende zentrale Netzwerk-Komponenten - in Schulen wie Unternehmen - sind:

- Router
- Firewall
- Switche
- WLAN-Access Points
- Endgeräte (Infotafeln, Whiteboards, Tablets für den Unterricht etc.).

Die Schule wird typischerweise mehrere leistungsfähige Internetanschlüsse benötigen und die dazu gehörenden Router. Die in den Routern integrierten einfachen Abwehrmittel wie Packet Inspection stellen datenschutzrechtlich bereits eine technische und organisatorische Maßnahme zum Schutz personenbezogener Daten dar, welche genutzt werden sollte, um eine erste (kleine) Hürde für externe Angreifer zu errichten.

Da die wenigsten Router über umfangreiche Firewallkomponenten verfügen, wird typischerweise hinter den oder die Router eine dedizierte Firewall (UTM: Unified Threat Management)[9] geschaltet. Diese übernimmt eine Vielzahl von Aufgaben, die aus sicherheitstechnischer, datenschutzrechtlicher und auch ökonomischer Sicht erwünscht sind, konkret:

- Gefahrenminimierung (sicherheits- und datenschutzrechtlich relevant) (Viren, Trojaner, Hacking jeder Art),
- Load balancing (Lastverteilung)
- Fall back (LTE, UMTS) für die Internetanschlüsse.
- Sachgerechte Aufteilung lokaler Netze nach benötigten Protokollen und zugehörigen Filtern, soweit nicht über lokale Server (SPAM, Content).
- Verwaltung von Nutzern und ihrer Zugriffsrechte
- Vergabe von Netzwerkadressen
- Über VPN sichere, verschlüsselte Zugriffsmöglichkeiten von extern auf die internen Netze. (z.B. für Schulleitung und Lehrerkollegium).

Die Firewall ist die zentrale Komponente in einem Schulnetz. Ihre Einrichtung und Überwachung sowie die ständige Anpassung / Erweiterung, um neue Bedrohungen zu erkennen und diese abzuwehren, erfordert hohe IT-Kompetenz. Dies beginnt bei der Anschaffung, denn die Hardware - wie auch die eingesetzte Software - muss ‚backdoor-free' sein, um das Ausspähen von Daten zu verhindern[10]. Kann dies nicht gewährleistet werden, ist von der Anschaffung abzusehen, da diese dann einen Verstoß gegen datenschutzrechtliche Regelungen darstellt. Einen möglichen Ausweg bieten „Backdoor-Freiheits-Garantien" der Komponenten-Hersteller in Verbindung mit konkreten vertraglichen Zusicherungen der IT-Dienstleister.

Die Wahrnehmung der geschilderten Aufgaben als Nebenjob oder in der Freizeit wird den gestiegenen technischen und rechtlichen Anforderungen und der zentralen Rolle, welche das Netzwerk für die Digitalisierung einnimmt, nicht gerecht. Wie in jedem Unternehmen sind auch hier IT- und Datenschutzkompetenz gefragt. Im IT-Bereich werden zu diesem Zweck vielfach sogenannte SLAs (Service Level Agreements) mit externen IT-Spezialisten und Wartungsverträge abgeschlossen. Diese betreffen die UTM selbst, die allfälligen Softwarebestandteile, Antivirus, Content- und Spamfilter sowie generell alle weiteren Netzwerkkomponenten. Der Abgleich mit den Bestimmungen des Datenschutzrechts und die nachhaltige Einhaltung dieser Bestimmungen obliegt dem zwingend vorzusehenden Datenschutzbeauftragten, welcher über rechtliche und technische Kenntnisse verfügt. Diese Aufgabe wird bereits heute von den Schulen regelmäßig extern vergeben.

---

[9] Inhaltlich setzt ein UTM-System eine Funktionskombination voraus, welche unterschiedliche Sicherheitsaufgaben auf einer Plattform vereint. Ziel des UTM ist es, an einem zentralen Punkt Sicherheit für das gesamte Netzwerk zu erlangen.

[10] Im Jahr 2014 wurde durch den Whistleblower Edgar Snowden u. a. bekannt, dass die US-amerikanische NSA (National Security Agency) gezielt Router, Switche und andere Netzwerkkomponenten von Herstellern wie Cisco, HP und anderen vor dem Export mit eigenen Software-Ergänzungen (backdoors) versehen hatte, um sich ggfls. später hierüber Zugang zu den damit ausgestatteten Netzwerken zu verschaffen.

5.3 Technikgestaltung - Lokale Netze

Im Hinblick auf den Bildungsauftrag der Schulen ist die Errichtung eines lokalen Netzes, welches von Schülern für Unterrichtszwecke genutzt werden kann, nach diesseitiger Einschätzung rechtlich geboten. Tatsächlich dürften die Schulen im Hinblick auf das Effizienzpotenzial eines Netzwerks auch weitere Abläufe vorsehen und insoweit voneinander getrennte weitere lokale Netze (LANs) mit entsprechenden Zugangsberechtigungen einrichten, sei es verkabelt oder als kabellose WLANs. Typische (W-)LANs an Schulen sind:

- LAN für die Schüler / den Unterricht zu Lernzwecken
- LAN für Schulleitung und Verwaltung zu administrativen Zwecken
- LAN für das Lehrerkollegium zu Kommunikationszwecken
- LAN für Telekommunikation zu Kommunikationszwecken
- LAN für Eltern zu administrativen Zwecken bei minderjährigen Schülern

Eine physikalische Trennung der Netze, sprich der Verkabelung einschließlich der Hard- und Software scheitert regelmäßig an baulichen Voraussetzungen und auch an den hiermit verbundenen Kosten. Daraus resultieren zusätzliche Anforderungen an die Netzwerkkomponenten (Switche, WLAN-APs), welche in der Praxis auch gut und datenschutzrechtlich sicher erfüllt werden können. Im Einzelnen handelt es sich um folgende Kriterien:

- Managebar Layer-2[11] oder besser
- VLAN[12]-Unterstützung
- Multi-SSID[13]

Je nach Größe der Schule, baulichen Gegebenheiten (WLAN-Ausleuchtung!) und der Anzahl der lokalen Netzwerke kann dies zu einer nennenswerten Anzahl von Switchen und WLAN-APs[14] führen, die jeweils mit mehreren VLANs und / oder SSIDs eingerichtet und verwaltet werden müssen. Einrichtung und Pflege von Firmware und Software-Updates sowie Veränderungen erfordern aus IT-Sicht eine fachkompetente Betreuung. Dies gilt auch in datenschutzrechtlicher Sicht, da sämtliche hier durchgeführten Maßnahmen für das technische und organisatorische Datenschutzniveau bedeutsam sind. Aus diesem Grunde kommt hier meist ein Netzwerk-Management-System (NMS) zum Einsatz, welches als Administrationssoftware die Verwaltung des gesamten Netzes ermöglicht. Hierzu gehören alle Maßnahmen zur Behebung von Fehlern und

---

[11] Der Switch leitet in einem Netzwerk die Datennachrichten auf dem sog. Layer 2 = Schicht 2 (auch: Data Link Layer) weiter. Der Layer 2 übernimmt damit den Aufbau und die Kontrolle einer Verbindung, die Aufteilung des Datenstroms in Bitblöcke, die Erkennung von Fehlern und die Regelung des Zugriffs auf das Übertragungsmedium.

[12] VLAN = Virtual Local Area Network = Logisches Teilnetz innerhalb eines Switches oder eines gesamten physischen Netzwerks.

[13] SSID=Service Set Identifier. Frei wählbarer Name für ein WLAN.

[14] WLAN AP= Wireless Local Area Network Access Point. Elektronisches Gerät, welches den kabellosen Zugang in ein Datennetz ermöglicht.

Ausfällen, das Ausrollen von Firmware- und Sicherheitsupdates und das Einpflegen neuer Netze (z.B. WLANs). Diese Management- und Kontrollfunktionen zählen in Teilen unzweifelhaft zu den technischen und organisatorischen Schutzmaßnahmen, welche die Schule wie jedes Unternehmen zum Schutz personenbezogener Daten vorhalten muss. Damit gilt aber auch hier, dass diese Tätigkeit sachgerecht und im Einklang mit den datenschutzrechtlichen Anforderungen nur von qualifizierten Personen mit ausreichenden Fachkenntnissen wahrgenommen werden kann. Eine Tätigkeit ohne qualifizierte Kenntnisse oder in der Freizeit wird den Anforderungen nicht gerecht und gefährdet in datenschutzrechtlicher Sicht das angemessene Schutzniveau, zu dessen Einhaltung Unternehmen wie Schulen gemäß Art. 32 DSGVO verpflichtet sind. Auch insoweit stellt daher eine Vergabe an qualifizierte externe Dienstleister auf Grundlage entsprechenden SLAs/ Wartungsverträgen [15] eine probate Lösung dar.

5.4 Netzwerkmanagement im Auftrag

Die geschilderte Komplexität der Anforderungen an das Schulnetz, verbunden mit einem Mangel an geeignetem eigenen (IT-)Personal, veranlassen viele Schulen, Lösungen möglichst umfangreich auszulagern. Datenschutzrechtlich ist dies möglich, wenn die Dienstleister als Auftragsverarbeiter im Sinne von Art. 28 DSGVO tätig werden. Dem liegt die gesetzgeberische Vorstellung zu Grunde, dass eine der Parteien - hier die Schule - die Verantwortung für die Daten hat und auch behält, sich aber zur Erledigung einzelner Aufgaben eines Dienstleisters bedient, den sie kontrolliert und datenschutzrechtlich „im Griff hat." Mit diesen Vorgaben sind zugleich die rechtlichen Rahmenbedingungen in Art. 32 DSGVO aufgezeigt, welche von der Schule als verantwortliche Auftraggeberin unbedingt einzuhalten sind, insbesondere:

- Die Sicherstellung geeigneter technischer und organisatorischer Schutzmaßnahmen auch beim Auftragnehmer;
- Eine klare Benennung und Regelung der zu verarbeitenden Daten und der Verarbeitungszwecke;
- Die Sicherstellung der Verarbeitung nur auf dokumentierte Weisung der Schule;
- Das Vorliegen einer Verpflichtung der Mitarbeiter des Auftragnehmers zur Vertraulichkeit.

Die Vergabe des gesamten Netzwerkmanagements geht über das Modell einer - prinzipiell unkritischen - Externalisierung einzelner Leistungen hinaus, bleibt aber zulässig, wenn folgende Bedingungen erfüllt sind:

[15] SLA = Service Level Agreement. Vereinbarung zwischen Eigentümer bzw. Nutzer eines Netzwerks und einem technischen Dienstleister, der die Verfügbarkeit von Netzwerk und evtl. von Diensten in abgestufter Form zusichert.

5.4.1 Management als Zweckbestimmung

Der Verarbeitungszweck muss klar bestimmt sein. Problematisch ist insoweit, ob die Bezeichnung des Verarbeitungszweckes als „Netzwerkmanagement" rechtlich ausreichend, oder ob nicht eine Strukturierung und Detaillierung geboten ist. Letzteres ist im Hinblick auf die in Art. 5 Abs. II normierte Rechenschaftspflicht der verantwortlichen Schule anzuraten. Aus der Leistungsbeschreibung eines seriösen Auftragnehmers sollte dies auch ohne weiteres zu entwickeln sein.

5.4.2 Besondere Anforderungen an den Auftragnehmer

Im Anwendungsfall der Schulen gilt es sodann zu beachten, dass die IT-Komponenten, nämlich das Netzwerk, physisch in der Schule vorhanden sind. Lediglich die *Funktion* eines Netzwerk-Administrators, System-Administrators o. ä. ist hier mangels eigenen geeigneten Personals an einen oder mehrere externe Dienstleister zu vergeben. Durch die eingangs beschriebene enge Verflechtung der Firewall mit den nachfolgenden Netzwerk-Komponenten bietet sich sogar eine Vergabe an **einen** verantwortlichen Auftragnehmer für das gesamte Netzwerkmanagement an.

Diese Lösung ist in datenschutzrechtlicher Sicht allerdings anspruchsvoll, denn wer **das Netzwerk managt, hat den umfassenden Zugriff auf sämtliche Daten.** Die für Auftragsverarbeiter fortgeltenden Anforderungen (s.o., Ziff. 5.4) erhalten daher aufgrund des risikobasierten Ansatzes der DSGVO nochmals eine Schärfung und dies aus gutem Grund: So ist es auf Ebene des Netzwerkmanagements technisch ohne weiteres möglich, beliebige Datenströme mitzuschneiden und extern automatisiert auszuwerten. Diese Korrelationen können sodann zielgerichtet zur (nahezu) unmerklichen Manipulation von Nutzern und Meinungen verwendet werden[16]. Einmal innerhalb eines lokalen Netzwerk, können die Zugangsdaten der Nutzer ausgeforscht und etwa ihre Beziehungsgeflechte innerhalb der Schule, aber auch etwaige private Kontexte (oftmals über Social Media-Accounts) offengelegt werden[17].

Die umfassende Managementtätigkeit durch Auftragnehmer erfordert daher in besonderem Maße eine vertragliche Regelung der Kontrollmechanismen, die Etablierung eines Berichtswesens und möglicherweise auch die Androhung von Sanktionen, um auszuschließen, dass der Auftragnehmer seine faktische Machtfülle als Administrator zu Lasten der Betroffenen missbraucht. All dies sollte einhergehen mit einer sorgfältigen Auswahl und Überprüfung des Dienstleisters, mit dem

---

[16] Erinnert sei an die jüngsten prominenten Eingriffe in den Fällen : NSA-Affäre (Snowden-Enthüllungen) und Cambridge Analytica (s.u.).

[17] Das englische Unternehmen Cambridge Analytica hatte sich illegal mehrere Millionen Datensätze von Facebooknutzern beschafft und hierfür Persönlichkeitsprofile erstellt. Durch den Einsatz von Algorithmen für künstliche Intelligenz wurde versucht, die Betroffenen in Benutzergruppen von sozialen Netzwerken zu manipulieren und so Einfluss auf das Wahlverhalten zu nehmen. Lt. einem Bericht der österreichischen Tageszeitung der Standard v. 26.10.2017 zahlte die Trump-Administration 5,9 Mio. € an das Unternehmen.

schlussendlich ja eine effiziente und partnerschaftliche Kooperation im Interesse aller Nutzer angestrebt wird und kein von Angst geprägtes Verhältnis.

Insofern sind besondere Anforderungen an die oder den Dienstleister zu stellen, zuallererst, dass die Verarbeitung im Geltungsbereich der DSGVO erfolgen sollte und diese damit als Schutzgesetz umfänglich zugunsten der Betroffenen anwendbar ist.

5.4.3 Auftragnehmer in Drittstaaten, insbesondere in den USA

Ist ein Dienstleister außerhalb des Europäischen Wirtschaftsraumes ansässig und verarbeitet er Daten von EU-Bürgern, so befindet er sich gem. Art. 2 Abs. II DSGVO zwar im Anwendungsbereich der DSGVO; Umsetzung und Durchsetzbarkeit sind aber nicht ohne weiteres sichergestellt, so dass bei Beauftragung zwingend ein vergleichbares Schutzniveau sicherzustellen ist. Dies lässt sich grundsätzlich durch die Verwendung sogenannter Standardvertragsklauseln der EU[18] absichern. Alternativ kann dies auch auf Grundlage zu verhandelnder bilateraler Regelungen erfolgen, datenschutzrechtlich sogenannte Binding Corporate Rules.

Im Verhältnis zu den USA besteht im Rahmen eines Datenschutzübereinkommens, des sogenannten EU-US Privacy Shield, seit 2016 die Möglichkeit für amerikanische Unternehmen, sich konkret benannten datenschutzrechtlichen Bestimmungen zu unterwerfen und sich dadurch selber zu zertifizieren. Die Zertifizierung belegt den Schutz personenbezogener Daten, die aus einem Mitgliedsstaat der Europäischen Union in die USA übertragen werden. Die Europäische Kommission hat dies per Beschluss vom 16.09.2016 für angemessen im Sinne von Art. 45 DSGVO erklärt[19]. Wie auf der offiziellen Webseite des EU-US-Privacy Shield ersichtlich, haben sich bislang 4997 Unternehmen dem Abkommen unterworfen[20].

Dass aufgrund dieser Zusagen ein ausreichendes oder gar ein mit den Regelungen der EU auf Augenhöhe befindliches Datenschutzniveau sichergestellt ist, muss mit Blick auf die Gesetzeslage und jüngste politische Entwicklungen aber ganz klar ausgeschlossen werden und ist auch Gegenstand gerichtlicher Auseinandersetzung. Eine Klage Irlands beim EuG ist seit dem 16.09.2016 anhängig[21].

Worum geht es dabei?

---

[18] Beschluss der EU-Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (Bekannt gegeben unter Aktenzeichen K (2010) 593.

[19] Durchführungsbeschluss (EU) 2016/1250 v. 12.7.2016

[20] Stand: 19.10.2019

[21] EuG, Rs T-670/16

Der EU-U.S. Privacy Shield verpflichtet in den USA datenverarbeitende Unternehmen gegenüber den Betroffenen zwar zur Beachtung ihrer Rechte analog den europäischen Regelungen; er reflektiert aber nicht das gänzlich andere gesetzliche Umfeld mit behördlichen Zugriffsbefugnissen, die dem europäischen Recht fremd sind. Dies betrifft namentlich den USA Patriot Act, der als Reaktion auf die Terroranschläge bereits 2001 als Bundesgesetz vom amerikanischen Kongress verabschiedet wurde. Er ermöglicht US-Behörden wie dem FBI, der NSA oder der CIA, ohne richterliche Anordnung Zugriff auf die Server von US-Unternehmen zu nehmen[22]. Dies schließt auch ausländische Töchter ein, die nach dem US-Gesetz verpflichtet sind, Zugriff auf ihre Server zu gewähren, selbst dann, wenn nationale Gesetze dies untersagen. Bei Ermittlungsmaßnahmen gegen den Dienstleister könnten so etwa die Nutzungsdaten aus dem Schulnetz ausgelesen werden und zwar unabhängig davon, ob diese in den USA oder auf dem lokalen Netzwerk der Schule abgelegt sind.[23]

Flankiert wird der Patriot Act seit 2018 durch den CLOUD Act, welcher 2018 vom amerikanischen Kongress ebenfalls als Bundesgesetz verabschiedet wurde[24]. Das Gesetz befasst sich explizit mit Daten, die nicht in den USA gespeichert sind. Es betrifft insbesondere IT-Dienstleister mit Sitz in den USA und verpflichtet diese bei behördlicher oder richterlicher Anforderung zur Herausgabe von Daten und zwar unabhängig davon, wo diese Daten gespeichert werden, also insbesondere auch dann, wenn diese im Fall der Schule auf einem Speichermedium in Deutschland liegen. Erforderlich ist auch nicht das Eigentum an den Daten, sondern lediglich, dass der Dienstleister die Daten „kontrolliert", was im Falle der Netzwerkadministration der Fall ist. Diese Herausgabeverpflichtung nach amerikanischem Recht kollidiert allerdings mit europäischem Datenschutzrecht: Gemäß Art. 48 DSGVO darf nämlich *„jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, (…) nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind."*

An einem solchen Übereinkommen fehlt es. In der Konsequenz drohen dem Dienstleister bei Befolgung der Herausgabeanweisung aus den USA gemäß Art. 83 Abs. V DSGVO Sanktionen bis zu einer Höhe von 20 Mio. € oder 4% des Jahresumsatzes, je nachdem, welcher Betrag höher ist.

Würde eine Schule folglich einen US-Dienstleister mit dem Netzwerkmanagement beauftragen, müsste sie das Dilemma widerstreitender Rechtsordnungen und damit ein im Falle einer Herausgabeanordnung nicht vorhersehbares Verhalten des Dienstleisters bei Vertragsschluss in Kauf nehmen. Inwieweit die Schule sich als Verantwortliche und primäre Normadressatin der Datenschutzregelungen durch die Auswahl eines solch „latent gefährdeten" Dienstleisters selber

---

22 USA Patriot Act, 107th US Congress, Public Law 107-56-Oct. 26, 2001

23 Für cloudbasierte Dienstleistungen bestehen weitere Eingriffsmöglichkeiten, s. dazu unten Ziff. 5.5

24 Clarifying Lawful Overseas Use of Data Act = CLOUD Act, 115th US Congress, Public Law 115-141-Mar. 22,2018. Entgegen seiner Schlagwortbezeichnung regelt das Gesetz nicht Cloud-spezifische Sachverhalte.

ordnungswidrig verhält, ist bislang nicht geklärt. Bei Anwendung üblicher Sorgfaltspflichten wird man angesichts der im Unternehmensumfeld inzwischen bekannten Problematik aber schwerlich argumentieren können, das Risiko sei nicht bekannt oder nicht vermeidbar gewesen. Die Beauftragung eines US-Dienstleisters, der der Anordnung einer auf seinem Heimatmarkt ansässigen Behörde Folge leistet, ist daher als eine fahrlässige Verletzung datenschutzrechtlicher Verpflichtungen zu Lasten der Betroffenen zu bewerten. Schwer wiegt nach diesseitiger Einschätzung, dass die Verletzung bereits bei Beauftragung denkbar und insoweit vorhersehbar ist und zugleich alternative Möglichkeiten bestehen, Dienstleister zu beauftragen, welche uneingeschränkt dem europäischen Datenschutzrecht unterfallen.

Fazit: Die Wahrnehmung von Netzwerkmanagement-Aufgaben durch US-amerikanische Unternehmen ist auch im Rahmen einer Auftragsverarbeitung datenschutzrechtlich riskant und nach diesseitiger Bewertung mit der DSGVO nicht vereinbar. Dies gilt selbst dann, wenn die beauftragten Unternehmen sich zur Beachtung des Privacy-Shield verpflichtet haben. Diese Einschätzung korrespondiert mit der Bewertung des US Department of Justice, welche den CLOUD Act als ein vom Privacy-Shield gänzlich unabhängiges und nicht betroffenes Instrument bewertet[25].

5.5 Netzwerkmanagement in der Cloud

Als technische Alternative zur klassischen Dienstleistertätigkeit und faktisch parallel zur rechtlichen Terminologie der Auftragsverarbeitung hat sich ein rasant wachsender Markt für Cloud-Lösungen entwickelt. Hier kann der Auftraggeber zwischen ganz unterschiedlichen Auslagerungsmodellen wählen, die Hardware, Software oder IT-Gesamtsysteme und deren Administration betreffen. Cloud-Anbieter werben typischerweise mit den erheblichen Kostenvorteilen aufgrund nicht erforderlicher Beschaffungen und - je nach Inhalt der Cloud - der Überlegenheit der skalierbaren technischen Lösungen (höhere Übertragungsgeschwindigkeiten, Schutz vor Datenverlust, flexible Zugriffe von verschiedenen Standorten, zentralseitige Aktualisierung).

Angesichts der geschilderten Personalproblematik und der - trotz Fördermaßnahmen - erforderlichen Investitionen drängt sich für viele Schulen die Frage auf, ob die günstigste Lösung nicht in der Cloud liegt. Hierbei ist allerdings die Ausgangslage in Erinnerung zu rufen: Netzwerkkomponenten (WLAN Access Points etc.) und Endnutzergeräte sind vorhanden bzw. durch die Schule anzuschaffen. Die Anschaffung spezifischer (Nicht-Standard) Software ist nicht Gegenstand der Fördermaßnahmen[26].

---

[25] Vgl. insoweit die umfangreichen Interpretationshinweise des U-S. Department of Justice in: DOJ White Paper, April 2019, abrufbar unter: www.justice.gov/CLOUDAct.

[26] Damit scheiden die gängigen Cloud-Modelle „Infrastructure as a Service“ und „Software as a Service“ aus.

Der für die Schule allein relevante Anwendungsfall bleibt - auch in der Cloud - somit der des Netzwerkmanagements, synonym die Management-Cloud. Diese unterscheidet sich datenschutzrechtlich allerdings nicht von der klassischen Wahrnehmung auf Grundlage eines Dienstleitungsvertrages (s.o.). Denn die DSGVO sieht im Falle der Aufgabenwahrnehmung durch Dritte allein das Instrument der Auftragsverarbeitung in Art. 28 DSGVO vor. Soweit im Umfeld der Cloud-Diskussion daher der Eindruck entstanden ist, hier bestünde eine weitere, effizientere Möglichkeit der Auslagerung, so ist dies falsch: Die alternative Übertragung auf einen Dienstleister dergestalt etwa, dass dieser die Verantwortung in eigener Regie übernimmt - und die Schule damit aus der Verantwortung entlassen würde - ist nicht vorstellbar. Eine solche Funktionsübertragung würde nämlich voraussetzen, dass Lehrer, Schüler und alle weiteren Betroffenen, deren Daten im Schulnetz verarbeitet werden, eine unmittelbare vertragliche Beziehung mit dem Dienstleister eingehen und einer Verarbeitung ihrer Daten dort zustimmen. Dies ist rechtlich kaum durchsetzbar. Dass die Schulen sich aus der Verantwortung für das Schulnetz gänzlich zurückziehen und damit jede Kontrollfunktion verlieren, würde zudem den bildungspolitischen Auftrag der Schulen unterlaufen.

Das Management in der Cloud ist für die Schulen hiernach möglich, wenn die Kontrollfunktion über den Dienstleister erhalten bleibt. Dies gilt insbesondere vor dem Hintergrund der von nahezu allen Anbietern verwandten technischen Lösung des sogenannten Software Defined Networking (SDN). Hierbei werden die unteren Funktionen eines Netzwerks in virtuelle Dienste abstrahiert, so dass die einzelnen Geräte vor Ort (in der Schule) nicht mehr manuell administriert werden müssen. Über die beiden Zweige ‚Control Plane' und ‚Data Plane' steuert die SDN-Applikation, welche Daten wohin und wie auf welche Netzwerk-Geräte gesendet werden. Gleichzeitig bedingt dies, dass auch Nutzungsdaten des (Schul-)Netzes zumindest in aggregierter Form vom externen SDN-Dienstleister erfasst und vorgehalten werden. In dieser Form des Remote Network Management verlassen also immer Daten das lokale Schulnetz und werden extern verarbeitet. Solange dies im Rahmen des Verarbeitungszweckes (Netzwerkmanagement) erfolgt bzw. erforderlich ist und die weiteren Regelungen der DSGVO beachtet werden, ist dies datenschutzrechtlich nicht zu beanstanden.

Wichtig bleibt aber immer, dass zumindest ein Mitarbeiter der Schule vorhanden ist, der in der Benutzung der NMS-Software geschult ist und als ‚vor-Ort-Projektleiter' kleinere Anpassungen am Netzwerk vornehmen kann. Das setzt wiederum eine abgestimmte und abgestufte Rechteverwaltung der NMS-Software voraus. Der gesamte Managementzugriff von extern auf das Netzwerk muss verschlüsselt erfolgen.

Soweit die Funktion an Dienstleister in Drittstaaten, insbesondere in den USA, vergeben werden soll, bestehen allerdings auch hier erhebliche datenschutzrechtliche Bedenken: Zwar ist analog der Dienstevergabe auch bei Cloud-Services eine Absicherung des europäischen Datenschutzniveaus über Standardvertragsklauseln und Binding Corporate Rules möglich, und die bekannten Cloudanbieter Amazon, Apple, Microsoft und Google machen heute zumeist ausreichende Zusagen. Eine Gewähr für die Sicherheit notwendiger eingesetzter eigener Hardware besteht aber nicht. Die Zugriffsmöglichkeit der NSA auf wesentliche Dienste von Microsoft über ihre Auswertungssoftware

ist belegt[27]. Hinzu kommen die bereits geschilderten gesetzlich abgesicherten und fortbestehenden, erheblichen Zugriffsbefugnisse amerikanischer Behörden auf die Server von US-Unternehmen auch ohne richterliche Anordnung[28].

Hinzu kommt folgendes: Eine europäischen Standards entsprechende Kodifizierung, welche ihren Ausgangspunkt im Schutz personenbezogener Daten als Ausdruck des Rechts jedes Einzelnen auf informationelle Selbstbestimmung nimmt, existiert in den USA bis heute nicht. Mehrere Bundesstaaten haben das Thema zuletzt aufgegriffen, so dass ein datenschutzrechtlicher Flickenteppich mit ganz unterschiedlichen Schutzniveaus künftig nicht auszuschließen ist, insbesondere, wenn der Kongress nicht kurzfristig ein Bundesgesetz auf den Weg bringt, welches den Schutz personenbezogener Daten sicherstellt. Damit ist unter der Trump-Administration aber kaum zu rechnen. Im Gegenteil: Zuletzt wurden die Vorschriften, welche den Internet-Anbietern eine Nutzung personenbezogener Daten zu Werbezwecken u.a. ohne Zustimmung der Nutzer verboten, abgeschafft unter Verweis auf Wettbewerbsgleichheit zu Webseitenbetreibern, die einem solchen Verbot nicht unterlägen.

6. Abschließende Bewertung und Empfehlung

Die Digitalisierung stellt die Schulen vor große Herausforderungen. Diese sind zu bewältigen, da sie gesellschaftlich erwünscht und bildungspolitisch erforderlich sind, damit die Schulen ihren verfassungsrechtlichen Auftrag weiterhin erfüllen können.

In technischer Sicht bedürfen die Schulen bzw. deren Träger bei der Schaffung der Voraussetzungen, konkret bei der Errichtung und dem Betrieb eines Netzwerks, kompetenter Unterstützung. Dies bezieht sich auf Beratung zur Erstellung eines Pflichten-/Lastenhefts sowohl für die Konzeption des Netzwerks (strukturell, logisch) als auch eines Mengengerüsts der benötigten Komponenten sowie im Anschluss an die Betreuung.

Während die Schulen bei der Ausgestaltung dieser Auftragsverhältnisse frei sind, gelten datenschutzrechtlich zwingend die Anforderungen, welche die DSGVO an Auftragsverarbeiter und die damit korrelierende Vertragsgestaltung stellt.

Dies beschränkt den Kreis zulässiger Dienstleister. Dies gilt insbesondere für die hier in Rede stehenden Cloud-basierten Management-Lösungen, welche dem Dienstleister ein erhebliches Missbrauchspotential einräumen. Dem ist durch die Auswahl qualifizierter Anbieter, die Vereinbarung weitreichender datenschutzrechtlicher Zusicherungen und insbesondere effektive Kontrollmechanismen zu begegnen.

---

[27] Bericht der Zeitschrift Focus v. 27.10.2013. Betroffen waren u.a. die Dienste Hotmail, Outlook und Skype.

[28] Rechtsgrundlage hierfür ist der US Patriot Act, der als Folge der Terroranschläge vom 11.9.2001 am 26.10.2001 vom US-Kongress verabschiedet wurde.

Nach diesseitiger Einschätzung erfüllen Anbieter aus Drittstaaten diese Voraussetzungen oft nicht, dies gilt insbesondere für Anbieter aus den USA, aber auch aus China, die in erheblichem Umfang Zugriffen staatlicher Stellen ausgesetzt sind.[29]

Die Auswahl eines unqualifizierten Dienstleisters stellt aber bereits einen Verstoß gegen datenschutzrechtliche Bestimmungen dar und kann ein Bußgeld auslösen. Für Schulen gelten insoweit die gleichen Konsequenzen, die auch Unternehmen treffen. Deutlich schwerer wiegen die Konsequenzen, wenn es tatsächlich zu einer unzulässigen Datenherausgabe kommt: Übermittelt etwa der von der Schule beauftragte US-amerikanische Cloud-Anbieter in Folge einer Herausgabeanweisung einer amerikanischen Behörde Daten von Schülern und Lehrern in die USA, drohen der Schule Bußgelder gem. Art. 83 DSGVO in einer Höhe bis zu 20 Mio. €. und zusätzlich Schadensersatzforderungen der Betroffenen gem. Art. 82 DSGVO.

Die Schulen können diese unerwünschten und möglicherweise auch gravierenden Konsequenzen vermeiden, wenn sie bei der Auswahl von Dienstleistern konsequent auf europäische Unternehmen setzen, die in einem intensiven Wettbewerb mit US-amerikanischen Dienstleistern stehen und mindestens gleichwertige Lösungen bereithalten.

* * *

[29] Erfassung und Auswertung von Daten erfolgen in China durch private und staatliche Stellen, die diese auswerten und sich auch wechselseitig zur Verfügung stellen. Ein effektives Recht auf informationelle Selbstbestimmung existiert in China nicht. Die Informationsinteressen des Betroffenen sind kaum geschützt und unzulässige Datenverarbeitung überall vorhanden, vgl. Xie, "*Informationelle Selbstbestimmung im Privatrecht und deren Hinweise für den chinesischen Schutz der personenbezogenen Information*", Dissertation, Hamburg 2017. Illustrativ hierzu auch: Deutschlandfunk, Weltzeit vom 2.1.2019, abrufbar unter: https://www.deutschlandfunkkultur.de/datenkrake-china-wo-staat-und-firmen-alles-speichern.979.de.html?dram:article_id=437240