Digitalisierung und Datenschutz

Was bedeuten die DSGVO und das DSG für Schulen in Deutschland und in der Schweiz?

Dr. Sven Matthiessen
avony GmbH, Rosenheimerstrasse 1
DE-83104Ostermünchen

Inhalt

1. Einführung: Datenschutz vs. Datensicherheit

Im Folgenden sollen die Datenschutzrichtlinien in Deutschland und in der Schweiz sowie ihre Implikationen insbesondere für den Schulalltag erörtert werden. Nach einer kurzen Begriffsklärung wird auf die jeweiligen Datenschutzgesetze in Deutschland und der Schweiz sowie die in diesem Zusammenhang wichtigen Institutionen eingegangen. Danach werden die Auswirkungen der Datenschutzbestimmungen für die Schulen erörtert, bevor die Problematik der Unvereinbarkeit dieser mit dem US-CLOUD Act diskutiert wird.

In den vergangenen Jahren haben sich im Zuge der Digitalisierung die Anforderungen an die Schulen in Deutschland und der Schweiz in Sachen Datenschutz deutlich verändert. Durch die Corona-Krise kommt verschärfend hinzu, dass viele Schulen händeringend nach Möglichkeiten suchen mit digitalen Unterrichtsmethoden den Schulalltag bestmöglich aufrechtzuerhalten. Hierbei treten eine Reihe datenschutzrechtlicher Probleme zutage, derer vollen Tragweite sich die Schulen oft nur langsam bewusst werden.

Häufig werden die Begriffe Datensicherheit und Datenschutz miteinander verwechselt oder gar synonym verwendet. Dies kann für eine Schule schwerwiegende Konsequenzen haben, da die Wahrung von Datensicherheit nicht automatisch die Einhaltung der Datenschutzbestimmungen bedeutet. Während es bei der Datensicherheit um den Schutz der Daten allgemein geht, sollen beim Datenschutz personenbezogenen Daten vor Missbrauch geschützt werden. Die Datensicherheit wird mit Hilfe von technischen Lösungen gewährleistet, der Datenschutz dagegen wird durch gesetzliche Vorschriften definiert. Insofern bedingt Datenschutz immer Datensicherheit, Datensicherheit wiederum bedeutet noch keinen Datenschutz nach DSGVO (Datenschutz-Grundverordnung der Europäischen Union), bzw. DSG (Datenschutzgesetz der Schweiz).

1.1. Datensicherheit

Datensicherheit kann in die folgenden drei Kernaspekte aufgeteilt werden:

- Zutrittsschutz: Vergleichbar mit dem Schloss an einer Tür
- Zugangsschutz: Wird durch ein Passwort geregelt, vergleichbar mit dem passenden Schlüssel für das Schloss
- Zugriffsschutz: Regelt die Berechtigung der Benutzung (Schlüsselinhaber, Firewall)

Den Kern der Datensicherheit bilden insofern Maßnahmen, die den Schutz sämtlicher Daten vor Missbrauch (Kontrollierbarkeit), Verfälschung (Integrität), Verlust (Verfügbarkeit) und unberechtigter Zugriffe (Vertraulichkeit) gewährleisten.

1.2. Datenschutz

Unter dem Begriff Datenschutz versteht man primär den Schutz der Persönlichkeit in Bezug auf den Umgang bzw. die Verarbeitung von persönlichen und personenbezogenen Daten. Es geht um die informelle Selbstbestimmung der Person, den Schutz der Privatsphäre. Es ist das individuelle Recht eines jeden Menschen, dass er grundsätzlich darüber entscheiden darf, welche persönlichen Daten wann und für wen zugänglich sind. Klare Richtlinien in Form von verbindlichen Gesetzen und Verordnungen regeln die Bedingungen. In der Schweiz regelt das DSG und in der Europäischen Union die DSGVO die Bestimmungen zum Schutz personenbezogener Daten

2. Was regeln DSGVO und DSG?

2.1. Was ist die DSGVO?

Die Datenschutz-Grundverordnung (DSGVO) ist eine von der Europäischen Union erlassene Verordnung, die seit dem 25. Mai 2018 den gemeinsamen Datenschutzrahmen der EU bildet. Ziel der Verordnung ist es, die Regeln zur Verarbeitung personenbezogener Daten durch private und öffentliche Datenverarbeiter innerhalb der Union zu vereinheitlichen. So sollen personenbezogene Daten innerhalb der EU geschützt und der freie Datenverkehr innerhalb des Europäischen Binnenmarkts gesichert werden.

Die DSGVO gilt in allen Mitgliedstaaten und darf grundsätzlich durch nationale Regelungen weder aufgeweicht noch verschärft werden. Allerdings ist es den Mitgliedstaaten durch verschiedene Öffnungsklauseln möglich, Einzelaspekte des Datenschutzes auf nationaler Ebene zu regeln. In Deutschland sollen das Bundesdatenschutzgesetz vom 30. Juni 2017 sowie die Änderung weiterer Gesetze die Überführung des nationalen Datenschutzes in die DSGVO regeln. Allgemein kann gesagt werden, dass die durch die DSGVO bedingten Neuregelungen keine tiefgreifende Veränderung zu den zuvor in Deutschland geltenden Datenschutzvorschriften darstellen. Dennoch regelt die DSGVO einige Aspekte des Datenschutzes neu, bzw. präzisiert sie, insbesondere bei den Grundsätzen zur Verarbeitung personenbezogener Daten. Nichteinhaltung dieser Grundsätze wird mit außerordentlich hohen Geldstrafen geahndet, bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes eines Unternehmens.[1]

Ein entscheidender Punkt der DSGVO in Verbindung mit nicht in der EU ansässigen Unternehmen ist das Marktortprinzip, nach welchem das europäische Datenschutzrecht auch für außereuropäische Unternehmen gilt, die ihre Waren und Dienstleistungen in der EU anbieten. Insofern findet die DSGVO auch dann Anwendung, wenn die Datenverarbeitung mit einem Angebot in Zusammenhang steht, das sich an Personen im Unionsgebiet richtet, unabhängig davon, ob die Datenverarbeitung inner- oder außerhalb der EU stattfindet.[2]

2.2. Was ist das DSG?

Das DSG orientiert sich grundsätzlich an der DSGVO. So wie die DSGVO innerhalb der gesamten EU gilt, erstreckt sich der Geltungsbereich des DSG auf die gesamte Schweiz. Es gibt jedoch einige Unterschiede zwischen den beiden Verordnungen: beim DSG ist die Bearbeitung von Personendaten

[1] Datenschutz-Grundverordnung, Art. 83 (6), https://dejure.org/gesetze/DSGVO/83.html [Aufruf am 03. Mai 2020].
[2] Datenschutz-Grundverordnung, Art. 3 (1), https://dejure.org/gesetze/DSGVO/3.html [Aufruf am 03. Mai 2020].

grundsätzlich erlaubt, soweit die Persönlichkeit einer betroffenen Person nicht verletzt wird. Bei der DSGVO ist dies grundsätzlich verboten, es sei denn es besteht hierfür eine rechtliche Grundlage. Während bei der DSGVO ein Datensubjekt das Recht auf Übertragbarkeit der persönlichen Daten hat, ist dies beim DSG nicht der Fall. Die verschiedenen hier tangierten Rechte (Berichtigung ungenauer persönlicher Daten, Recht auf Einschränkung der Verarbeitung, Widerrufsrecht etc.) sind abgesehen vom Auskunftsrecht zwar nicht konkret im DSG definiert, werden aber anderweitig vom Schweizer Rechtssystem geregelt und sind insofern auch durchsetzbar.[3] Insgesamt sind die rechtlichen Konsequenzen, die sich aus DSGVO und DSG ergeben, für die jeweiligen Bürger und juristischen Personen in der EU und der Schweiz weitgehend identisch.

2.3. Was sind EDÖB und BfDI?

Der EDÖB (der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte) ist in der Schweiz für Datenschutz und Informationsfreiheit zuständig. Er hat seinen Sitz in Bern, seit Juni 2016 hat Adrian Lobsiger dieses Amt inne. Der Datenschutzbeauftragte berät nicht nur Ämter, sondern auch Privatpersonen. In Deutschland gibt es mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) eine ähnliche Einrichtung zur Überwachung und Durchsetzung des Datenschutzes. Der BfDI ist zur Überwachung und Durchsetzung der DSGVO unter anderem bei Bundesbehörden, öffentlichen Stellen und Postdienstunternehmen zuständig. In der allgemeinen Privatwirtschaft sind allerdings die Aufsichtsbehörden der Länder zuständig. Bürger, die «ihr Recht auf Informationszugang» nach dem Informationsgesetz gefährdet sehen, können den BfDI anrufen. Dieser kann dann bei der Durchsetzung vermittelnd tätig werden, allerdings selbst keine Informationen herausgeben. Seit Januar 2019 ist Ulrich Kelber Bundesbeauftragter für den Datenschutz und Informationsfreiheit in der Bundesrepublik. In der EU nimmt der Europäische Datenschutzbeauftragte (EDSB) diese Aufgaben auf der supranationalen Ebene wahr: «Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Einrichtung der EU und hat nach Artikel 52 Absatz 2 der Verordnung (EU)2018/1725 „im Hinblick auf die Verarbeitung personenbezogener Daten [...] sicherzustellen, dass die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere ihr Recht auf Datenschutz, von den Organen und Einrichtungen der Union geachtet werden“; er ist gemäß Artikel 52 Absatz 3 „für die Beratung der Organe und Einrichtungen der Union und der betroffenen Personen in allen Fragen der Verarbeitung personenbezogener Daten“ zuständig.»[4]

3. Welche Daten sind besonders schützenswert und was bedeutet das für die Schulen?

Im Rahmen des DigitalPakt Schule wurden in Deutschland vom Bund 5 Milliarden Euro für den Digitalisierungsprozess deutscher Schulen bereitgestellt. Die Schulen sollen hierbei eigenverantwortlich eine digitale Infrastruktur entwickeln; dies betrifft insbesondere auch die Schaffung eines Netzwerkes, über welches dann die ausgesuchten Dienste laufen sollen. Der Betrieb eines schuleigenen Netzwerks und dessen Nutzung durch Schüler, Lehrer und Dritte (z. B. Eltern) geht mit der Verarbeitung einer Vielzahl personenbezogener Daten einher. Datenschutz und die Einhaltung der DSGVO spielen daher bei der Digitalisierung von Schulen eine, wenn nicht DIE zentrale Rolle.

---

[3] PwC Schweiz, *Was bringt die Revision des Schweizer Datenschutzgesetzes mit sich, und wie hängt dies mit der DSGVO und der ePrivacy-Verordnung zusammen?* https://www.pwc.ch/de/publications/2018/E-DSG_Revision-des-Schweizer-Datenschutzgesetzes.pdf [Aufruf am 04. Mai 2020].

[4] European Data Protection Supervisor, *Stellungnahme 2/2019: Stellungnahme des EDSB zu dem Mandat für die Verhandlung eines Abkommens zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln*, https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_eu_us_agreement_e-evidence_en_de.pdf [Aufruf am 04. Mai 2020].

Ziel der DSGVO ist es, alle von einer Datenverarbeitung betroffenen Personen zu schützen. Im Schulbetrieb betrifft dies alle personenbezogenen Daten von im Schulnetzwerk aktiven Akteuren sowie anderweitig dort verarbeiteten Daten weiterer Personen. Insofern ist nach § 4 Nr. 7 DSGVO auch die Schule und nicht der Schulträger verantwortlich für die Durchsetzung des Datenschutzes.[5] Da jedoch alle Förderanträge in Hinblick auf die Digitalisierung einer Schule vom jeweiligen Schulträger gestellt werden müssen, ist eine enge Zusammenarbeit zwischen diesen beiden Institutionen unabdingbar. Sind die vom Schulträger beantragten Fördermaßnahmen nicht DSGVO-konform, so wäre die Schule am Ende rechtlich in der Haftung, sollten diese Maßnahmen bewilligt und implementiert werden. Es liegt insofern im Eigeninteresse der Schule von vornherein den Antragsweg gemeinsam mit dem Schulträger zu begleiten.

Sowohl bei der Netzwerkinstallation als auch bei der Hard- und Softwarebeschaffung muss die Schule peinlichst genau darauf achten, dass die DSGVO in allen Bereichen eingehalten wird; dies betrifft z.B. die sog. «Backdoorfreiheit», die das Ausspähen von Daten verhindert. Für den IT-Beauftragten der Schule ergibt sich durch die Komplexität der DSGVO-Thematik ein deutlich erhöhter Arbeitsaufwand, der von einer abgestellten Lehrkraft innerhalb von ein oder zwei Wochenstunden kaum zu leisten ist. Insofern wird der externe IT-Beauftragte über kurz oder lang zur Regel werden; DSGVO-konforme *Device Management* Systeme müssen ebenso integraler Bestandteil einer jeden digitalisierten Schule werden.

Für die Schulen in der Schweiz ergeben sich aus dem DSG identische Konsequenzen wie für die deutschen Schulen aus der DSGVO.

Aus diesen Konsequenzen ergibt sich die nächste Frage für die Schulen: welche der vielen auf dem Bildungsmarkt verfügbaren Dienste sind überhaupt datenschutzrechtlich unbedenklich?

4. Was ist der CLOUD Act und was bedeutet er für Deutschland und die Schweiz?

Ein entscheidender Aspekt bei der DSGVO- bzw. DSG-Konformität ist die Vereinbarkeit mit dem CLOUD Act, dem grundsätzlich alle amerikanischen Anbieter unterworfen sind, unabhängig, ob sie die Daten auf einem Server in den USA, in der EU oder anderswo speichern.

4.1. Was ist der CLOUD Act und wie verhält er sich zur DSGVO?

Grundsätzlich haben amerikanische Unternehmen die Möglichkeit über den EU-US Privacy Shield Konformität mit den Regulierungen aus der DSGVO herzustellen. Dieses Abkommen verpflichtet Unternehmen, die ihre Daten in den USA verarbeiten, die Rechte aller involvierten Personen gemäß den Richtlinien der DSGVO zu beachten. Eine große Anzahl auch namhafter Unternehmen ist dem EU-US Privacy Shield auch bereits beigetreten, allerdings bedeutet dies keineswegs Rechtssicherheit für die betroffenen Verbraucher in der EU. Dies liegt daran, dass es US-Behörden unabhängig von der jeweiligen nationalen Rechtslage möglich ist, über den Patriot Act (ein US-Bundesgesetz aus dem Jahre 2001) Zugriff auf die Server amerikanischer Unternehmen und ihrer Töchter zu bekommen. Für eine Schule in der EU oder in der Schweiz würde dies bedeuten, dass eine Behörde wie das FBI oder die NSA bei Ermittlungen gegen den Dienstleister selbst dann Daten aus dem Schulnetz auslesen könnte, wenn diese lokal gespeichert wären.[6] Der CLOUD Act (engl. Clarifying Lawful Overseas Use of Data Act) als US-Bundesgesetz aus dem Jahre 2018 präzisiert noch einmal die Zugriffsrechte amerikanischer

[5] Eric Heitzer, *Der Digitalpakt Schule. Eine datenschutzrechtliche Herausforderung*. (Köln: Integrity. Gesellschaft für Datenschutz, Geldwäscheprävention und Compliance, 2019), S. 6.
[6] Ebenda, S. 14.

Bundesbehörden auf nicht in den USA gespeicherten Daten. Im CLOUD Act werden IT-Dienstleister mit Sitz in den USA verpflichtet, bei behördlicher oder richterlicher Anordnung Daten auch dann herauszugeben, wenn diese außerhalb der USA gespeichert sind. Der Dienstleister müsste also demzufolge die Daten einer Schule in Deutschland oder der Schweiz an die US-Behörde herausgeben, auch wenn der Dienstleister nicht im Eigentum der Daten ist, sondern diese lediglich administriert. Die von der Datenherausgabe betroffene Person dürfte laut CLOUD Act über den Vorgang seitens des Dienstleisters auch nicht informiert werden; dies wiederum stellt einen unlösbaren Widerspruch zu Art. 48 DSGVO dar, wonach eine solche Herausgabe von Daten nur dann möglich wäre, wenn es ein Rechtshilfeabkommen zwischen der EU und dem die Daten anfordernden Drittland gäbe. Ein solches Abkommen zwischen der EU und den USA existiert nicht, wodurch der amerikanische Dienstleister in Gefahr geriete, gemäß Art. 83 Abs. V DSGVO sanktioniert zu werden, sollte er die Daten an die US-Bundesbehörde herausgeben. Zwar können diese Sanktionen äußerst hoch ausfallen (bis zu 20 Mio. EUR oder 4% des Jahresumsatzes, s.o.), es bleibt aber im Ermessen des Dienstleisters, ob er sich angesichts der ihm drohenden Strafe gegen die Gesetzgebung seines Heimatlandes stellt. Zwar hat der Dienstleister die Möglichkeit gegen die Herausgabe der Daten vor einem amerikanischen Gericht zu klagen, in der Vergangenheit wurden dort die Interessen der USA aber immer höher gewertet als die Persönlichkeitsrechte der betroffenen Personen.

Für die Schule in der EU bedeutet dies, dass sie sich auf äußerst unsicheres Terrain begibt. Zwar hat gem. des CLOUD Acts der Dienstleister Möglichkeiten den US-Behörden gegenüber die Herausgabe der Daten anzufechten, wenn dies die Verletzung der Gesetze des Landes bedeuten würde, in dem die Daten gespeichert sind. Dies gilt, insbesondere wenn es sich bei den Daten um Daten nichtamerikanischer Staatsbürger handelt. Insofern könnte angenommen werden, dass die Risiken eines Datenabflusses in die USA für Unternehmen oder auch Schulen, deren Daten in der EU gespeichert werden, äußerst gering sind.[7] Nichtsdestotrotz bleibt eine Situation von Rechtsunsicherheit. So warnt Michael Scheffler, „Area VP EMEA“ bei Bitglass, vor zwei miteinander unvereinbaren Rechtsauffassungen: «Indem sie [die Unternehmen, Anm. des Autors] sich für Cloud-Anwendungen eines US-Anbieters entscheiden, nehmen sie das ***Risiko eines unberechtigten Zugriffs Dritter*** in Kauf. Ihrer Verpflichtung zu einer Datenschutz-Folgenabschätzung wären sie dementsprechend nicht ausreichend nachgekommen».[8] Auch wenn die Wahrscheinlichkeit eines Datenabflusses ggfs. als gering eingeschätzt werden kann, so bleibt doch in jedem Fall ein Restrisiko und eine rechtliche Unvereinbarkeit zwischen CLOUD Act und DSGVO: «Die DSGVO verlangt von Unternehmen ***vollständige Kontrolle*** über die von ihnen erhobenen Daten und zwar über die gesamte Verarbeitungskette hinweg. Der, CLOUD Act‘, der sich über diese Ebene hinwegsetzt, unterminiert diese Kontrollfunktion.»[9] Schulen sind in diesem Zusammenhang genauso Normadressat wie Unternehmen und müssen von sich aus sicherstellen, dass sie die Daten ihrer Schüler, Mitarbeiter oder ggfs. Dritter gemäß der DSGVO sichern. Tun sie das nicht, machen sie sich u. U. strafbar, bzw. es liegt dann in ihrem Verantwortungsbereich, DSGVO-Konformität wiederherzustellen. Die dafür anfallenden Kosten müssten dann die Schulen selbst tragen. Alles in allem wäre es für eine Schule nicht zu verantworten US-amerikanische Dienstleister mit der Administration ihres Netzwerks zu beauftragen;

[7] Caitlin Potratz Metcalf & Peter Church, *U.S. CLOUD Act and GDPR – Is the Cloud still safe?* https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe [Aufruf am 10. Mai 2020].
[8] datensicherheit.de, *DSGVO vs. CLOUD Act: EU-Unternehmen im Spannungsfeld.* https://www.datensicherheit.de/dsgvo-cloud-act-eu-unternehmen-spannungsfeld [Aufruf am 10. Mai 2020].
[9] Ebenda.

auch dann, wenn sich dieser dem o.g. Privacy Shield verpflichtet, da letzterer vollkommen unabhängig vom CLOUD Act betrachtet werden muss.[10]

4.2. Wie verhält sich der CLOUD Act zum DSG?

Für die Schweiz stellt das DSG identische Anforderungen an die Schule wie die DSGVO in Deutschland und der EDÖB stellt klar, dass «Personendaten nicht ins Ausland bekannt gegeben werden [dürfen], wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen **angemessenen Schutz** gewährleistet (Art. 6 Abs. 1 DSG). Unter diesen Umständen können Personendaten nur ins Ausland bekannt gegeben werden, wenn eine der in Art. 6 Abs. 2 DSG aufgeführten Bedingungen erfüllt ist.»[11] In seiner Erläuterung rät der EDÖB abschließend: «Falls aufgrund der Risikoeinschätzung bezüglich der Verarbeitung von Personendaten in der Cloud Zweifel bestehen, ist von einer Auslagerung der Daten abzusehen.»[12]

4.3. Zusammenfassung

Der CLOUD Act steht in einem grundsätzlichen Widerspruch sowohl zur DSGVO als auch zum DSG. Über den CLOUD Act ist es amerikanischen Bundesbehörden möglich, sogar ohne Gerichtsbeschluss die Herausgabe von Daten, die von amerikanischen Dienstleistern (darunter Anbieter von Cloud-Lösungen) gespeichert wurden, zu fordern. Die betroffene Person wird darüber nicht in Kenntnis gesetzt; die US-Dienstleister können den Datenabfluss zwar theoretisch unterbinden, wenn Nicht-US-Bürger involviert sind, müssen dies aber nicht tun. Darüber hinaus ist es, etwa bei E-Mailverkehr, oft gar nicht möglich, die Daten von EU- sowie Schweizer Bürgern vor dem Zugriff durch US-Behörden vollumfänglich zu schützen. Das Recht auf informelle Selbstbestimmung der Bürger in der EU und in der Schweiz kann unter diesen Voraussetzungen nicht garantiert werden.

5. Welche Auswirkungen hat die Unvereinbarkeit von CLOUD Act und DSGVO/ DSG auf Schule in Deutschland und der Schweiz?

Wie oben bereits beschrieben ist die Schule der Normadressat der Datenschutzrichtlinien in Deutschland und der Schweiz. Insofern obliegt es ihr schon bei der Beantragung von Fördermitteln darauf zu achten, dass alle Datenschutzrichtlinien eingehalten werden. Die meisten Berührungspunkte mit dem Thema Datenschutz ergeben sich für die Schule neben dem Aspekt der Netzwerksicherheit bei der Frage der Speicherung von Daten in einer Cloud und, gerade im Zuge der Corona-Krise, beim E-Learning.

5.1. Datenschutz und Cloud-Lösungen

Das Speichern von Daten in einer Cloud stellt datenschutztechnisch eine der größten Herausforderungen für eine Schule dar. Um sicherzugehen, dass keinerlei Daten abfließen und somit die DSGVO/ das DSG nicht verletzt wird, muss sichergestellt werden, dass der Server, auf dem die Daten gespeichert sind, sich in der EU oder der Schweiz befindet und kein Dritter Zugriff auf diese Daten hat. Zwar verfügen US-amerikanische Anbieter über Server in diesen Ländern, jedoch können sie aufgrund des CLOUD Acts nicht absolut garantieren, dass eine amerikanische Bundesbehörde nicht doch Zugriff auf die gespeicherten Daten verlangt. Entscheidet sich eine Schule also dafür, ihre digitalen Geräte über ein Mobile Device Management-System zu administrieren und Daten dann auf

[10] Heitzer, S. 15.
[11] Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), *Erläuterungen zu Cloud Computing,* https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html [Aufruf am 10. Mai 2020].
[12] Ebenda.

einem externen Server zu speichern, so muss sie sicherstellen, dass sich dieser Server in der EU/ in der Schweiz befindet und der Anbieter zu 100 % den Schutz der Daten garantieren kann.

5.2. Datenschutz und E-Learning

Auch und gerade in Verbindung mit dem in Zeiten der Corona-Krise plötzlich in den Mittelpunkt gerückten E-Learning spielt das Thema Datenschutz eine entscheidende Rolle. Viele Schulen, ad hoc mit der Notwendigkeit konfrontiert ihre Schüler online mit Unterricht versorgen zu müssen, griffen vorschnell zu Messenger-Diensten wie WhatsApp und Konferenzlösungen wie Zoom. Aufgrund der oben dargelegten Datenschutzproblematik haben sich diese Schulen damit auf rechtlich gefährliches Terrain begeben. So hat der Datenschutzbeauftragte des Landes Baden-Württemberg bereits Ende April 2020 vor der Verwendung von Zoom gewarnt und auch ausdrücklich auf die Möglichkeit von rechtlichen Verwarnungen und Untersagungen den Schulen gegenüber hingewiesen. Die von Seiten des Datenschutzbeauftragten vorgebrachten Hauptkritikpunkte gegen Zoom sind dabei die Mängel in puncto Sicherheit und Datenschutz sowie die unnötige Erhebung und Verwertung von Nutzerdaten.[13] Der hessische Datenschutzbeauftragte wiederum äußerte harsche Kritik an der Verwendung von WhatsApp durch viele Lehrer, die er als «datenschutzrechtlich unterbelichtet» bezeichnete. Hier sei äußerst problematisch, dass WhatsApp mit der Vielzahl der gespeicherten Nutzerdaten Beziehungs- und Interessenprofile bilden könne sowie Zugriff auf alle im Mobiltelefon gespeicherten Kontakte habe.[14] In Baden-Württemberg und Hessen werden Lehrer entsprechend dazu aufgefordert datenschutzkonforme Messenger-Dienste zu nutzen.

6. Zusammenfassung

Das Thema Datenschutz hat durch den Lockdown im Zuge der Corona-Krise und der damit verbundenen Homeschooling-Problematik noch einmal zusätzlich an Brisanz gewonnen. Dies gilt sowohl in Deutschland als auch in der Schweiz, wo die jeweiligen Datenschutzverordnungen (DSGVO in der EU und DSG in der Schweiz) weitestgehend idente Anforderungen an ihre Adressaten stellen. Vielen Akteuren im Bereich Schule sind Ausmaß und Konsequenzen des Datenschutzes für ihre Institution nicht wirklich bewusst. Ein Kernproblem hierbei ist die häufig synonyme Verwendung der Begriffe «Datenschutz» und «Datensicherheit». Während «Datensicherheit» lediglich ein Aspekt von «Datenschutz» ist, stellt letzterer eine Rechtsnorm dar, die es von allen adressierten Akteuren strikt einzuhalten gilt. In diesem Zusammenhang ist für Schulen in Deutschland und der Schweiz insbesondere der Konflikt zwischen der DSGVO/ dem DSG auf der einen und dem US-CLOUD Act auf der anderen Seite von entscheidender Bedeutung. Viele Schulen haben unter dem Druck ihren Unterricht schnellstmöglich digital gestalten zu müssen auf Messenger-Dienste und Videoplattformen zurückgegriffen, die nicht den Richtlinien der DSGVO/ des DSG entsprechen. Da die Schule der Normadressat bei der Durchsetzung des Datenschutzes ist, trägt sie auch die Konsequenzen bei Verstössen gegen oder Nichteinhaltung desselben. Insofern liegt es im ureigenen Interesse der Schule, dass sie sich bei der Digitalisierung konsequent datenschutzkonform verhält. Es ist daher nicht übertrieben festzustellen, dass der Datenschutz und die Einhaltung der entsprechenden gesetzlichen Normen eine äußerst wichtige Rolle im Digitalisierungsprozess der Schullandschaft in Deutschland und der Schweiz spielen wird.

---

[13] News 4 Teachers. Das Bildungsmagazin, *Datenschutzbeauftragter warnt Lehrer vor Videokonferenzdienst Zoom,* https://www.news4teachers.de/2020/04/datenschutzbeauftragter-warnt-lehrer-vor-videokonferenzdienst-zoom/ [Aufruf am 13. Mai 2020].

[14] News 4 Teachers. Das Bildungsmagazin, *Datenschützer kritisiert Lehrer harsch dafür, WhatsApp zu nutzen („unterbelichtet"!),* https://www.news4teachers.de/2019/06/datenchuetzer-kritisiert-lehrer-harsch-dafuer-whatsapp-zu-nutzen-unterbelichtet/ [Aufruf am 13. Mai 2020].

Quellen

Datenschutz-Grundverordnung, Art. 3 (1), https://dejure.org/gesetze/DSGVO/3.html [Aufruf am 03. Mai 2020].

----------Art. 83 (6), https://dejure.org/gesetze/DSGVO/83.html [Aufruf am 03. Mai 2020].

datensicherheit.de. *DSGVO vs. CLOUD Act: EU-Unternehmen im Spannungsfeld.* https://www.datensicherheit.de/dsgvo-cloud-act-eu-unternehmen-spannungsfeld [Aufruf am 10. Mai 2020].

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB). *Erläuterungen zu Cloud Computing.* https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing/erlaeuterungen-zu-cloud-computing.html [Aufruf am 10. Mai 2020].

European Data Protection Supervisor. *Stellungnahme 2/2019: Stellungnahme des EDSB zu dem Mandat für die Verhandlung eines Abkommens zwischen der EU und den USA über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln*. https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_eu_us_agreement_e-evidence_en_de.pdf [Aufruf am 04. Mai 2020].

Heitzer, Eric. *Der Digitalpakt Schule. Eine datenschutzrechtliche Herausforderung*. Köln: Integrity. Gesellschaft für Datenschutz, Geldwäscheprävention und Compliance, 2019.

News 4 Teachers. Das Bildungsmagazin. *Datenschutzbeauftragter warnt Lehrer vor Videokonferenzdienst Zoom,* https://www.news4teachers.de/2020/04/datenschutzbeauftragter-warnt-lehrer-vor-videokonferenzdienst-zoom/ [Aufruf am 13. Mai 2020].

----------*Datenschützer kritisiert Lehrer harsch dafür, WhatsApp zu nutzen („unterbelichtet"!).* https://www.news4teachers.de/2019/06/datenchuetzer-kritisiert-lehrer-harsch-dafuer-whatsapp-zu-nutzen-unterbelichtet/ [Aufruf am 13. Mai 2020].

Potratz Metcalf, Caitlin & Church, Peter. *U.S. CLOUD Act and GDPR – Is the Cloud still safe?* https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe [Aufruf am 10. Mai 2020].

PwC Schweiz. *Was bringt die Revision des Schweizer Datenschutzgesetzes mit sich, und wie hängt dies mit der DSGVO und der ePrivacy-Verordnung zusammen?* https://www.pwc.ch/de/publications/2018/E-DSG_Revision-des-Schweizer-Datenschutzgesetzes.pdf [Aufruf am 04. Mai 2020].