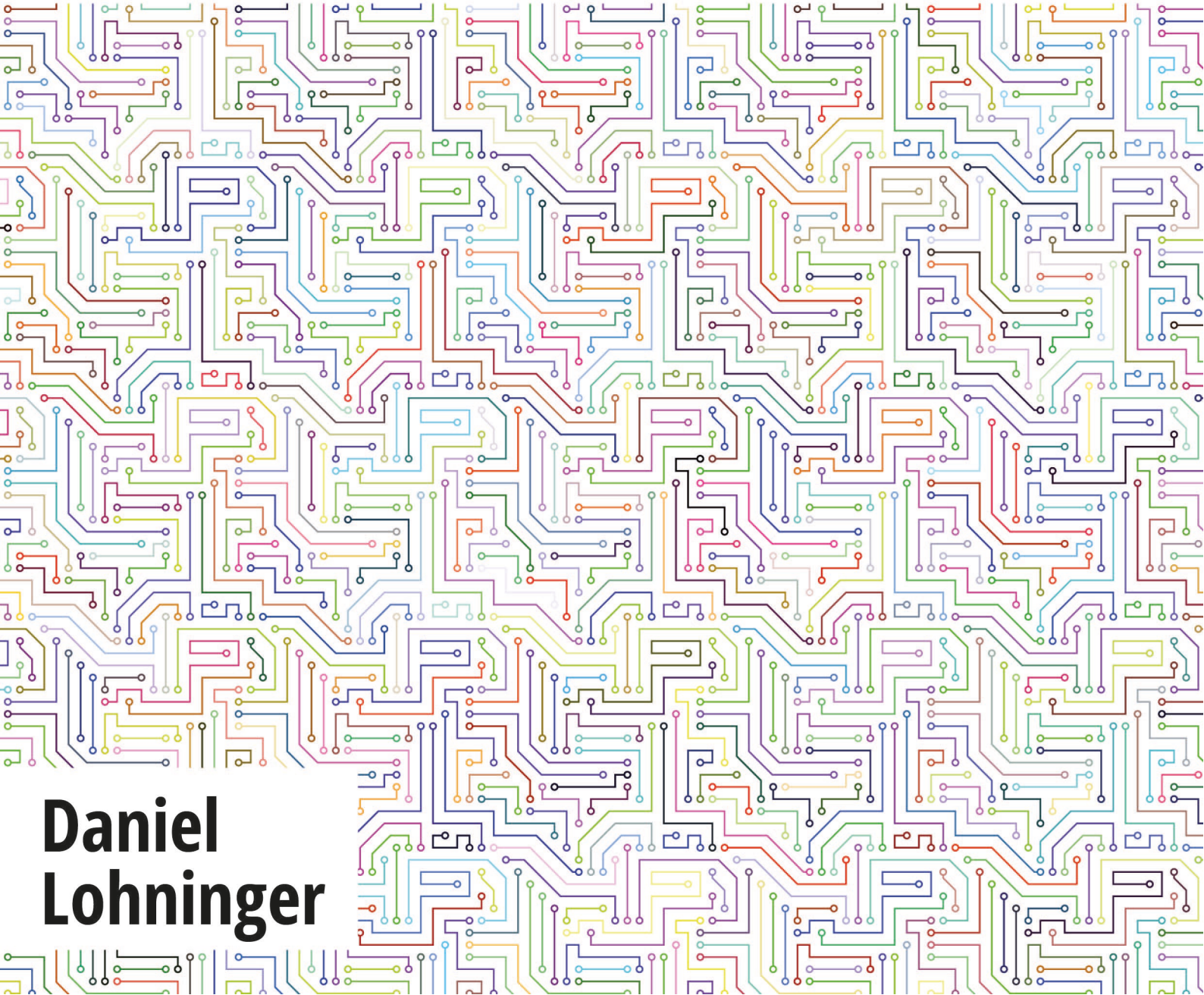
Datenschutz und die Auswirkungen der DSGVO auf Schulen



Daniel Lohninger

Autor: Daniel Lohninger

Letzte Änderungen: Juni 2018

Kontakt: daniel@lohninger.work

1. Inhalt

1. Inhalt ... 3

2. Abstract ... 5

3. Das Recht auf Datenschutz ... 6

3.1. Begriff und rechtliche Verankerung ... 6

3.2. Schulrechtliche Regelungen zum Datenschutz ... 9

3.2.1. Bildungsdokumentationsgesetz ... 9

3.2.2. Schulunterrichtsgesetz ... 11

4. Die EU-Datenschutzgrundverordnung ... 12

4.1. Entstehung und Bedeutung ... 12

4.2. Überblick über die DSGVO ... 13

4.2.1. Erwägungsgründe ... 14

4.2.2. Öffnungsklauseln ... 14

4.2.3. Kapitel I - Allgemeine Bestimmungen ... 15

4.2.4. Kapitel II – Grundsätze ... 16

4.2.5. Kapitel III - Rechte der betroffenen Personen ... 17

4.2.6. Kapitel IV – Verantwortlicher und Auftragsverarbeiter ... 17

4.2.7. Kapitel V Internationaler Datenverkehr ... 18

4.2.8. Kapitel VI Unabhängige Aufsichtsbehörde ... 19

4.2.9. Kapitel VII Zusammenarbeit und Kohärenz ... 19

4.2.10. Kapitel VIII Rechtsbehelfe, Haftung und Sanktionen ... 20

4.2.11. Kapitel IX – XI ... 21

4.3. Novellierung des DSG 2000 ... 21

4.4. Datenschutz-Anpassungsgesetze Bildung ... 22

5. Änderungen für die Schulen ... 24

5.1. Überblick 24

5.2. Datenschutzverantwortliche(r) an den Schulen ... 24

5.3. Datenschutzbeauftragter ... 24

5.4. Dokumentationspflicht/Anwendungsverzeichnis ... 25

5.5. Informationspflichten ... 25

5.6. Alter für die Einwilligung ... 26

5.7. Lehrmaterial 26

6. Datenschutz aus Sicht der Schülerinnen und Schüler 27

6.1. Überblick 27

6.2. Recht auf transparente Information 27

6.3. Recht auf Auskunft 29

6.4. Recht auf Vergessenwerden und Richtigstellung 30

6.5. Pflichten 31

6.6. Selbstbestimmtes Leben im digitalen Zeitalter 31

7. Datenschutz aus Sicht der Lehrkräfte 32

7.1. Überblick 32

7.2. Die Schülerverwaltung 32

7.2.1. Vorgeschriebene Anwendungen 32

7.2.2. Kennwörter 33

7.2.3. Eigene Aufzeichnungen 36

7.3. E-Learning-Tools im Unterricht 36

7.3.1. Lernplattformen 37

7.3.2. Pseudonymisierung 39

7.3.3. Appberechtigungen 39

7.4. Kommunikation über Messenger 41

7.4.1. WhatsApp und Facebook Messenger 41

7.4.2. Alternativen 43

7.5. Kameraüberwachung in der Schule 46

7.6. Themen für den Unterricht 47

7.6.1. Soziale Medien 47

7.6.2. Privatwirtschaftliche Überwachung - Überwachungskapitalismus 50

7.6.1. Staatliche Überwachung 52

8. Literaturverzeichnis 55

9. Abbildungsverzeichnis 61

10. Anhang 62

10.1. Experteninterviews 62

10.1.1. Interview mit MinR Dr. Thomas Menzel 62

2. Abstract

Die EU-Datenschutzgrundverordnung bildet einen Meilenstein im Recht auf Datenschutz. In dieser Arbeit gehe ich der Frage nach ob und wenn ja welche Auswirkungen sie auf die österreichischen Schulen hat. Dazu stütze ich mich auf die Analyse von Gesetzestexten und auf Fachliteratur und ergänze es mit den Erkenntnissen aus einem Experteninterview mit dem Datenschutzbeauftragten des Bundesministeriums für Bildung, Wissenschaft und Forschung.

Nach einem kurzen geschichtlichen Abriss des Themas Datenschutz, wird die rechtliche Situation beleuchtet und die Entstehung und der Inhalt der EU-DSGVO beschrieben. In der Mitte der Arbeit, erläutere ich die herausgefundenen Änderungen für die Schulen. Veränderungen ergeben sich vor allem durch neue Begrifflichkeiten, eine Umstellung in der Dokumentation von Datenverarbeitungsvorgängen, sowie der notwendigen Bestellung von Datenschutzbeauftragten. Auch wurde das Mindestalter für die Einwilligung in eine Datenspeicherung und Datenverarbeitung nun gesetzlich festgelegt. Eine weitere Vertiefung des Themas Datenschutz mit den Neuerungen wird in der Folge noch aus Sicht der Schülerinnen und Schüler und aus Sicht der Lehrkräfte dargelegt.

3. Das Recht auf Datenschutz

3.1. Begriff und rechtliche Verankerung

Datenschutz ist ein in der zweiten Hälfte des 20. Jahrhunderts entstandener Begriff. Je nach Betrachtungsweise wird Datenschutz verstanden als Schutz vor missbräuchlicher Datenverarbeitung und Schutz der Privatsphäre, sowie das Recht auf informationelle Selbstbestimmung. Dieses lässt sich als Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen, erklären. Also wem wann welche seiner persönlichen Daten zugänglich sein sollen, aber auch der Schutz des Persönlichkeitsrechts bei der Datenverarbeitung. Dazu gehört z.B. das Recht am eigenen Bild. Der Datenschutz muss sich dabei mit den Anforderungen einer sich immer weiter digitalisierenden Gesellschaft weiterentwickeln, um den mit den technologischen Möglichkeiten einer zunehmend digitalen und vernetzten Informationsgesellschaft angemessen zu sein und um bestehenden Tendenzen zum Abbau von Privatsphäre, dem Ausufern staatlicher Überwachungsmaßnahmen bis zum Aufbau von Überwachungsstaaten und der Entstehung von Datenmonopolen von Privatunternehmen entgegenwirken. (Datenschutzbeauftragter-Info.de, 2014)

Das Thema Privatsphäre hat in den Überlegungen zum Verhältnis von Staat zu Bürgerinnen und Bürgern schon früh eine Rolle gespielt, so wurde z.B. in den USA ein verfassungsrechtliches „Right to be alone“ postuliert. 1890 entwickelten Samuel D. Warren und der spätere Bundesrichter Louis D. Brandeis das „Right to Privacy“, nach dem jedem Individuum das Recht zustehe, selbst zu bestimmen, inwieweit seine „Gedanken, Meinungen und Gefühle“ und entsprechende personenbezogene Informationen anderen mitgeteilt werden sollten. (Warren, Brandeis, 1890)

Das erste wirkliche Datenschutzgesetz ist das Hessische Datenschutzgesetz für die öffentliche Verwaltung des Landes Hessen. Es trat 1970 in Kraft und ist damit das älteste formelle Datenschutzgesetz der Welt. Das deutsche Bundesverfassungsgericht hat dann in einem Urteil ein Grundrecht auf informationelle Selbstbestimmung festgestellt. Danach können Betroffene grundsätzlich selbst darüber entscheiden, wem sie welche persönlichen Informationen bekannt geben. (Genz,, 2004, S. 9)

Rechtsgrundlage für den Datenschutz in Österreich ist das Datenschutzgesetz 2000 (DSG 2000), das seit es 1978 verfasst wurde mehrmals novelliert wurde. Österreich war einer der ersten europäischen Staaten mit einer eigenen Behörde für den Datenschutz. Diese Datenschutzbehörde (DSB)[1] kontrolliert die Einhaltung des Datenschutzes. Auch für sie ergeben sich Veränderungen durch die DSGVO die im Verlauf dieser Arbeit noch erläutert werden. (RIS, 2018)

In der am 4. November 1950 in Rom unterzeichneten Europäischen Menschenrechtskonvention (EMRK) findet sich in Artikel 8 das Recht auf Achtung des Privat- und Familienlebens, das als Grundlage für den Datenschutz gilt. Dort heißt es: „(1) Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs.“[2]

„Eine Gesellschaft, in der die Menschenrechte nicht verbürgt sind, hat keine Verfassung“, heißt es in Artikel 16 der Menschen- und Bürgerrechtserklärung von 1789, einem der Grundlagentexte, mit denen die Demokratie und Freiheit in Frankreich begründet wurden. In Österreich, das der EMRK 1958 beigetreten ist, hat diese seit 1964 rückwirkend Verfassungsrang. Das österreichische Bundes-Verfassungsgesetz hat keinen eigenen Grundrechtekatalog. Im Kern der österreichischen Grundrechtsgesetzgebung steht die Europäische Menschenrechtskonvention als eine von drei Säulen, gemeinsam mit dem „Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger“, das seit 1918 in den Rechtsbestand der Republik übernommen wurde und nach jüngerer Entwicklung die „Charta der Grundrechte der Europäischen Union“, die die Grundlage einer Verfassung der Europäischen Union bildet und seit 2012 ebenfalls als Maßstab für Verfassungskonformität beim Verfassungsgerichtshof gilt. (Postlmayr, 2018)

Je nach Betrachtungsweise wird Datenschutz verstanden als Schutz vor missbräuchlicher Datenverarbeitung, Schutz des Rechts auf informationelle Selbstbestimmung,

[1] DSB war bis 2014 DSK, die Datenschutzkommission

[2] https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Bundesnormen&Dokumentnummer=NOR12016939

Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und auch Schutz der Privatsphäre. Der Wesenskern eines solchen Datenschutzrechts besteht dabei darin, dass die Machtungleichheit zwischen Organisationen und Einzelpersonen unter Bedingungen gestellt werden kann. (saferinternet.at, 2018)

Datenschutz ist also immer auch Schutz vor einer Machtungleichheit im Verhältnis von Firmen zu Konsumentinnen und Konsumenten und einem Staat zu seinen Bürgerinnen und Bürgern. Politik- und Rechtswissenschaftler Manfried Welan dazu: „Ganz allgemein sind die heutigen Verfassungen Museen der politischen Geschichte. In ihnen sind politische Erfindungen enthalten, die aus Erfahrungen mit politischer Macht entstanden sind. Die Erfahrung des Machtmissbrauchs war die Mutter vieler politischer Erfindungen gegen den Machtmissbrauch. Alle unsere politischen Institutionen sind Erfindungen, die theoretisch ausgedacht, experimentell erprobt und durch Innovationen weiterentwickelt wurden. Denken wir an das Wahlrecht, den Parlamentarismus, das Mehrheitsprinzip, die Bindung an Verfassung und Gesetz, an die Kontrollen durch unabhängige Einrichtungen und vor allem an die Grund- und Freiheitsrechte.“ (Welan, 2002)

Die rechtliche Konsequenz aus dem Grundrecht auf Datenschutz heißt für die Schulleitung wie für andere Verantwortliche im Schulbereich, dass personenbezogene Daten nur unter Beachtung des Grundrechts auf Datenschutz verwendet werden dürfen. (Lachmayer, Menzel, 2017)

3.2. Schulrechtliche Regelungen zum Datenschutz

Es gibt zwei Gesetze welche rechtlichen Regelungen für die meisten Datenverarbeitungen an Schulen enthalten. Hier werden insbesondere die gesetzlichen Grundlagen für die Datenverarbeitung von Schülerinnen und Schülern, für die keine Einwilligung notwendig ist geregelt. Beide Gesetze werden momentan novelliert. Zum Großteil umfassen die Änderungen nur Anpassungen an die Begriffe der DSGVO. Eine Ausnahme bildet die „durchgehende Bildungsdokumentation" auf die im folgenden Unterkapitel genauer eingegangen wird.

3.2.1. Bildungsdokumentationsgesetz

Das Bildungsdokumentationsgesetz (BilDokG) ist am 1. Jänner 2003 in Österreich in Kraft getreten und bildet eine zentrale gesetzliche Grundlage für die Datenerfassung im Schulbetrieb. Das Gesetz sieht z.B. eine statistische Meldepflicht von Schülerinnen- und Schülerdaten der Schulen zum Zweck der Verarbeitung einer Bundesstatistik vor. Folgende Daten werden lt. BilDokG erfasst:

- die Namen (Vor- und Familiennamen, einschließlich allfälliger akademischer Grade),
- im Fall, dass eine Schülerkarte mit Lichtbild auszustellen ist ein Lichtbild, auf dem der Kopf erkennbar und vollständig abgebildet sein muss,
- das Geburtsdatum,
- die Sozialversicherungsnummer,
- das Geschlecht,
- die Staatsangehörigkeit,
- die Anschrift am Heimatort und, sofern zusätzlich vorhanden, des der Bildungseinrichtung nächst gelegenen Wohnsitzes (Zustelladresse) entsprechend den Angaben der Erziehungsberechtigten bzw. der Schülerin oder des Schülers
- das Beginndatum der jeweiligen Ausbildung unter Angabe deren Bezeichnung,
- das Beendigungsdatum und die Beendigungsform der jeweiligen Ausbildung unter Angabe der Bezeichnung der beendeten Ausbildung und

- das allfällige bildungseinrichtungsspezifische Personenkennzeichen (z.B. Matrikelnummer),
- das von den Erziehungsberechtigten bzw. der Schülerin oder dem Schüler angegebene Religionsbekenntnis,
- das erste Jahr der allgemeinen Schulpflicht,
- eine festgestellter sonderpädagogischer Förderbedarf,
- die Eigenschaft als ordentlicher oder außerordentlicher Schüler,
- die Schulkennzahl,
- die Schulformkennzahl,
- mit dem Schulbesuch zusammenhängende Daten über die Verletzung der Schulpflicht, die Teilnahme an Unterrichts- und Betreuungsangeboten, den Schulerfolg, die Schul- bzw. Unterrichtsorganisation, den Bildungsverlauf sowie die Inanspruchnahme von Transferleistungen aus dem Familienlastenausgleich nach Maßgabe der Anlage 1,

Außerdem sind wenn nötig insbesondere folgende Daten gemäß § 3 Abs. 2 Z 8 schülerbezogen zu verarbeiten:

- Daten im Zusammenhang mit der Aufnahme der Schülerinnen und Schüler sowie in Zusammenhang mit der Durchführung von Aufnahme- und Eignungsprüfungen;
- für die Ausgestaltung der Unterrichtsordnung (etwa Klassenbildung, Stundenplan, Befreiungen, Anmeldung zum Betreuungsteil) erforderliche Daten;
- für die Ausstellung von Zeugnissen, Schulnachrichten und Schulbesuchsbestätigungen erforderliche Daten;
- Daten zur Beurteilung für Aufsteigen und Wiederholen von Schulstufen, Abschluss von Modulen sowie zur Feststellung der zulässigen Dauer des Schulbesuchs;
- zur Durchführung von abschließenden Prüfungen und Externistenprüfungen erforderliche Daten;
- Kontaktdaten der Erziehungsberechtigten;
- Kontaktdaten der Schüler- und Elternvertreter.

Ein weiteres Element des BilDokG ist in § 2 Abs 3 die Festlegung der Schulleitung als datenschutzrechtlich Verantwortliche im Sinne des Art. 4 Z 7 DSGVO. Die Schulleitung war auch in der alten Version des Gesetzes verantwortlich für die Datenverarbeitung der Schülerinnen und Schüler, die Begrifflichkeiten wurden aber auch hier der DSGVO angepasst. (BilDokG, 2017)

3.2.2. Schulunterrichtsgesetz

Das Schulunterrichtsgesetz (SchUG) ist ein Bundesgesetz über die Ordnung von Unterricht und Erziehung, die Rechte und Pflichten und das Verhältnis von Lehrpersonen und Schülerinnen und Schülern zueinander. Es gilt für alle im Schulorganisationsgesetz (SchOG) geregelten Schulen.

Enthalten sind auch Regelungen zur Datenerfassung und Datenverarbeitung. Dies wird hier anhand des Beispiels des Klassenbuchs erläutert. Laut §77 Abs. 2 SchUG haben Klassenbücher insbesondere Aufzeichnungen zu enthalten über:

- Schule, Schulart, Schulstandort, Schuljahr, Klasse bzw. Jahrgang, Schulformkennzahl,
- Namen der Schülerinnen und Schüler,
- Unterrichtsgegenstände (Stundenplan),
- Namen der unterrichtenden Lehrerinnen und Lehrer,
- Termine für Schularbeiten und Tests,
- Anmerkungen zu den einzelnen Unterrichtsstunden: Beginn und Ende der Unterrichtsstunde, behandelter Lehrstoff, durchgeführte Prüfungen, besondere Vorkommnisse wie z.B. Abweichungen vom Stundenplan (Stundentausch, Supplierung, Entfall, Schulveranstaltungen u.a.),
- Anmerkungen zu den einzelnen Schülerinnen oder Schülern: Fernbleiben, Aufgaben und Funktionen, besondere Vorkommnisse u.a.

Außerdem ist im selben Paragraphen geregelt, dass besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO nur dann im Klassenbuch vermerkt werden dürfen, wenn deren Dokumentation ein erhebliches öffentliches Interesse darstellt. (SchUG, 2017) und (DSAG-Bildung, 2018)

4. Die EU-Datenschutzgrundverordnung

4.1. Entstehung und Bedeutung

Mit der EU-Datenschutz-Richtlinie, die bis 1998 in nationales Recht umgesetzt werden musste, wurde zum ersten Mal eine Basis für ein einheitliches Datenschutzniveau in der EU und dem europäischen Wirtschaftsraum geschaffen. Eine Richtlinie der EU ist immer nur eine Vorgabe die dann von den Staaten der EU in nationales Recht umgesetzt werden muss. Es hat sich allerdings gezeigt, dass diese Richtlinie in den einzelnen Mitgliedstaaten sehr unterschiedlich ausgelegt wurde. Um diesen Umstand zu beseitigen und um in Europa für den Datenschutz einen homogenen Rechtsraum zu schaffen wird seit 2011 an einer einheitlichen Regelung gearbeitet. Dies sollte durch eine Datenschutzgrundverordnung gelingen. Eine Verordnung ist direkt in allen Mitgliedsstaaten gültig, sie in nationale Gesetze zu gießen ist nicht notwendig. Mit diesem Bemühen um eine einheitliche Regelung begann in Brüssel die größte Lobbyschlacht welche EU bis jetzt gesehen hat. Besonders große US-Unternehmen nahmen dabei eine starke Rolle ein und traten gegen eine Limitierung der Datennutzung auf. Andererseits beeinflussten die Enthüllungen von Edward Snowden über Massenüberwachung die Debatte in Richtung mehr Datenschutz. Als direkte Folge dieses Lobbyings wurden im Gesetzgebungsprozess rekordverdächtige 3100 Änderungsanträge gestellt. Viele Abänderungstexte wurden direkt von den Lobby-Papieren der Industrie und einer Datenschutz-NGO kopiert. Die Lager waren dabei recht klar. Konservative und wirtschaftsliberale EU-Abgeordnete traten für eine Abschwächung des Schutzniveaus ein. Sozialdemokratische, linke, grüne und gesellschaftsliberale EU-Abgeordnete versuchten ein höheres Schutzniveau zu verankern. Am 21. Oktober 2013 hat das Europäische Parlament die durch den Grünen Europaabgeordneten Jan-Phillip Albrecht ausgearbeitete Verhandlungsposition mit überwältigender Mehrheit angenommen. Die Mitgliedsstaaten haben im Rat und in der Gruppe "Informationsaustausch und Datenschutz" (DAPIX) den Komissionsvorschlag ausarbeiteten. Dort gab es eine Mehrheit, die Wirtschaftsinteressen und Deregulierung vor einen stärkeren Datenschutz stellten. Die Mitgliedsstaaten beharrten in vielen Bereichen auch auf bestehende nationalen Regelungen oder der Schaffung von Ausnahmen. Die weitere Einigung auf den endgültigen Text fand vor

allem abseits des formalen Gesetzgebungsprozesses, hinter verschlossenen Türen statt. Es wurde zwar eine gemeinsame Position der Institutionen herbeigeführt, jedoch fehlen entsprechende Begleitmaterialien die für die Interpretation der finalen Aspekte des Textes hilfreich wären. Es wurden sogar Einigungen mit „Tabellen" erzielt, in denen „Tausch-Vorschläge" eingetragen wurden – frei nach dem Motto „Streichst du mir A, gebe ich dir B". Die entsprechende Nachvollziehbarkeit der finalen Verhandlungen ist daher nicht gegeben. Max Schrems zu Rechtsunsicherheiten: „Die DSGVO sollte das Datenschutzrecht in 28 Mitgliedsstaaten unmittelbar regeln. Der Versuch, einen kleinsten gemeinsamen Nenner bei teils stark divergierende Positionen und Traditionen in den Mitgliedsstaaten zu finden, führte jedoch oft zu mangelnder Bestimmtheit, großen Rechtsunsicherheiten und umfangreichem Interpretationsbedarf. Viele im DSG 2000 und anderen nationalen Gesetzen bisher klar geregelte Fragen werden mangels klarerer Regelung in der DSGVO zukünftig vom EuGH gelöst werden müssen. Bis dies in jahrelangen Verfahren geschieht, bestehen teilweise erhebliche Rechtsunsicherheiten." Obwohl die DSGVO auf keinen Fall perfekt ist, stellt sie dennoch einen Meilenstein für den Datenschutz dar und wird das Datenschutzniveau in Europa weiter erhöhen. Auch in Hinblick auf globale Entwicklungen ist eine starke Position der EU im Datenschutz, die auch gegenüber internationalen Konzernen einklagbar ist, wichtig. Die DSGVO ist am 25. Mai 2016 in Kraft getreten und wird gemäß Art. 99 am 25. Mai 2018 gültig. (Schrems, 2016, S.33-37) (edps.europa.eu, 2018)

4.2. Überblick über die DSGVO

Zielsetzungen der DSGVO sind ein einheitlicher Rechtsschutz für alle Betroffenen in der EU und eine einheitliche Regeln für die Datenverarbeitung innerhalb der EU, außerdem die Gewährleistung eines starken und einheitlichen Vollzuges. Dazu gibt es z.B. Änderungen beim Vorgehen der Datenschutzbehörden, so wurden die Strafen für Verstöße massiv erhöht und befinden sich auf dem Niveau des Kartellrechts. Die datenschutzrechtliche Terminologie ist in bestimmten Bereichen neu. So wird bspw. der bisherige Auftraggeber zum „Verantwortlichen" und der Dienstleister zum „Auftragsverarbeiter". Mehr dazu in der Erläuterung von Kapitel IV der DSGVO. Die DSGVO umfasst 173 Erwägungsgründe und 99 Artikel. Sie gliedert sich in 11 Kapitel.

Im Folgenden werden einige wesentliche Aspekte der verschiedenen Kapitel beleuchtet. (Schmidl, 2018, S. 4-5)

4.2.1. Erwägungsgründe

Neben dem eigentlichen Gesetzestext sind jeweils auch die Erwägungsgründe angeführt. Das sind Erläuterungen, die z. B. völkerrechtlichen Verträgen oder EU-Rechtsakten vorangestellt werden und dadurch aufzeigen sollen, welche Überlegungen zum Erlass des Gesetzes geführt haben und damit die Interpretation des Gesetzes vereinfachen. Da es so massives Lobbying bei der Gestaltung der DSGVO gab und die Positionen so divergierend waren, ist man, um überhaupt zu einer Einigung zu kommen, etwas ausgewichen und es kam zu einer **Verlegung verbindlicher Regelungen in die „Erwägungen“**. Bei vielen strittigen Punkten konnte im Text der DSGVO keine Einigung erzielt werden, jedoch akzeptierte die jeweils andere Seite eine Verschiebung der vorgeschlagenen Regelung in die eben genannten Erwägungen der DSGVO. Max Schrems beschreibt diesen Prozess und das daraus resultierende Problem so: „Die Erwägungsgründe sind aber rechtlich nicht verbindlich. Die eine Seite konnte sich damit begnügen, dass sich eine Regelung in der DSGVO wiederfindet, die andere Seite konnte gleichzeitig behaupten, dass sich diese Regelung nicht im verbindlichen Text befindet. Ein erheblicher Anteil von Detailregelungen findet sich durch diese Vorgehensweise nur in den Erwägungen und ist aus dem Gesetzestext weder abzuleiten noch zu erahnen. Formal sind diese Regelungen damit regelmäßig nicht beachtlich. In der Praxis werden sich wohl Gerichte und Aufsichtsbehörden trotzdem auf diese Erwägungen stützen. In der Rechtsanwendung ist damit für erhebliche Rechtsunsicherheit gesorgt: Je nach Position werden Betroffene und Verantwortliche jeweils vertreten, dass ein bestimmter Erwägungsgrund integraler Teil der DSGVO ist – oder aber durch den Gesetzestext nicht unterstützt wird und damit unbeachtlich sei.“ (Schrems, 2017, S.34-35)

4.2.2. Öffnungsklauseln

Außerdem finden sich in der DSGVO viele sogenannte Öffnungsklauseln. Hier besteht für die Mitgliedstaaten der EU die Möglichkeit, durch nationale Gesetze die Bestimmungen der DSGVO zu spezifizieren und zu konkretisieren. In vielen Mit-

gliedsstaaten bestehen umfangreiche und differenzierte nationale Sonderregelungen und Vorrechte einzelner Industriezweige. Auch im staatlichen Bereich finden sich solche sehr spezifischen nationalen Abweichungen. Der Versuch diese Sonderregelungen beizubehalten, hat zu vielen Öffnungsklauseln in der DSGVO geführt. Bei grenzüberschreitenden Sachverhalten besteht daher auch hier weiterhin eine gewisse Rechtszersplitterung. (Schrems, 2017, S.34)

4.2.3. Kapitel I - Allgemeine Bestimmungen

Im ersten Kapitel wird unter anderem der **sachliche Anwendungsbereich** (Art. 2) der DSGVO geklärt. Die DSGVO findet Anwendung auf **personenbezogene Daten** (Art. 4), das sind Daten die einer Person zugeordnet sind oder zugeordnet werden können wenn diese Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen, unabhängig von dem Ausmaß der Verarbeitung. In Art. 3 wird außerdem auf den **räumlichen Anwendungsbereichs** eingegangen. Primär ist für Verantwortliche oder Auftragsverarbeiter, die ihre Niederlassung im Unionsgebiet haben, die DSGVO anwendbar. Nach Art. 3 Abs. 2 findet die DSGVO aber auch Anwendung, wenn die Datenverarbeitung durch einen nicht im Unionsgebiet niedergelassenen Verantwortlichen oder Auftragsverarbeiter erfolgt wenn sie die personenbezogenen Daten von Unionsbürgerinnen und Bürgern oder ihnen angebotene Waren betreffen (unabhängig von einer etwaigen Zahlung für Waren u/o Dienstleistungen). Dies gilt auch, wenn die Datenverarbeitung darauf zielt das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt. Im Artikel 4 werden die **Begriffsbestimmungen** (Art. 4) vorgenommen. Vor in Kraft treten der DSGVO hat die Datenschutzrichtlinie (DSRL) die Richtung für die gesetzliche Umsetzung des Datenschutz auf nationaler Ebene vorgegeben. Da das aber zu den in Kapitel 4.1 Entstehung und Bedeutung beschriebenen Problemen geführt hat wird die DSRL von der DSGVO abgelöst und ungültig. Die Begriffsbestimmungen der DSGVO (Art. 4) übernehmen vielfach die Begriffsbestimmungen der DSRL, enthalten aber auch viele neue Begriffe, wie z.B.

- Profiling (Art. 4 Z 4),
- Pseudonymisierung (Art. 4 Z 5),

- Verletzung des Schutzes personenbezogener Daten (Art. 4 Z 12; Data Breach),
- genetische und biometrische Daten sowie Gesundheitsdaten (Art. 4 Z 13 bis 15),
- Hauptniederlassung (Art. 4 Z 16),
- Vertreter, Unternehmen und Unternehmensgruppe (Art. 4 Z 17 bis 19),
- Aufsichtsbehörde und betroffene Aufsichtsbehörde (Art. 4 Z 21 und 22),
- grenzüberschreitende Verarbeitung (Art. 4 Z 23),
- maßgeblicher und begründeter Einspruch (Art. 4 Z 24),
- Dienst der Informationsgesellschaft (Art. 4 Z 25),
- internationale Organisation (Art. 4 Z 26).

(Schmidl, 2018, S. 6-7)

4.2.4. Kapitel II – Grundsätze

Die Grundsätze der Datenverarbeitung sind weitgehend ident mit jenen der DSRL. Art. 6 regelt die **Rechtmäßigkeit der Verarbeitung**. Hier ist festgelegt, dass die Verarbeitung von Daten unzulässig ist, außer es liegt ein Rechtfertigungsgrund vor (Verbot mit Ausnahmen). Art. 7 legt die **Bedingungen für die Einwilligung** fest (und zwar detaillierter als es bisher die DSRL tat). Art. 8 nimmt ausdrücklich Bezug auf die **Bedingungen für die Einwilligung eines Kindes** in Bezug auf Dienste der Informationsgesellschaft und ist für den Schulbereich natürlich relevant. Damit wird dem Umstand der fortschreitenden Digitalisierung und der Nutzung von Informationsdiensten auch durch Minderjährige Rechnung getragen. Art. 9 enthält die Voraussetzungen für die Verwendung sensibler Daten. Das sind besondere Kategorien personenbezogener Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person. Sensible Daten haben besonderen Schutz. Art. 10 legt schließlich fest, unter welchen Voraussetzungen personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden dürfen. (Schmidl, 2018, S. 8)

4.2.5. Kapitel III - Rechte der betroffenen Personen

Kapitel III regelt jene **Datenschutzrechte**, die eine betroffene Person hat. Die Art. 13 und 14 legen die Informationspflichten gegenüber Betroffenen fest. Demnach sind Betroffene darüber zu informieren, von wem, auf welcher Rechtsgrundlage und zu welchem Zweck ihre Daten verarbeitet und an wen sie übermittelt werden. Der EuGH misst diesen Informationspflichten großen Wert bei, weil diese die Voraussetzungen dafür schaffen, dass Betroffene ihre Rechte (**Auskunft**, **Richtigstellung**, **Löschung**, **Widerspruch**) ausüben können. Neben den bisherigen Rechten auf Auskunft (Art. 15), **Berichtigung** (Art. 16), **Löschung** (Art. 17; ausgeweitet zum „**Recht auf Vergessenwerden**“) und **Widerspruch** (Art. 21) werden neue Rechte eingeführt. So sieht Art. 18 das **Recht auf Einschränkung der Verarbeitung** vor. Demnach kann ein Betroffener vom Verantwortlichen die Einschränkung der Verarbeitung verlangen wenn beispielsweise die Richtigkeit der Daten von der Betroffenen Person bestritten wird. Art. 20 räumt einem Betroffenen das **Recht auf Datenübertragbarkeit** ein. Damit wird eine gesetzliche Grundlage für Datenaustausch zwischen ähnlichen technischen Systemen sichergestellt. Man soll also Daten zwischen Anbietern transferieren können oder die eigenen Daten von Anbietern in eine sonstige technische Umgebung übertragen. Art. 23 regelt, in welchen Voraussetzungen die Union und die Mitgliedstaaten die normierten **Rechte und Pflichten einschränken** dürfen. (Schmidl, 2018, S. 10)

4.2.6. Kapitel IV – Verantwortlicher und Auftragsverarbeiter

Die DSGVO nimmt stärker als die bisherigen Regelungen Verantwortliche und Auftragsverarbeiter in die Pflicht. **Verantwortlicher** ist jene Person die über die Verarbeitung der personenbezogenen Daten entscheidet. Verantwortliche sind z.B. in Firmen meist die CEOs. Der oder die Verantwortliche bildet den Hauptfokuspunkt der datenschutzrechtlichen Regulierung. (Feiler, Horn, 2017, S197)

Auftragsverarbeiter ist jemand der personenbezogene Daten im Auftrag und auf Weisung einer oder eines Verantwortlichen verarbeitet. Der Auftragsverarbeiter entscheidet nicht über Mittel und Zwecke der Datenverarbeitung. (Feiler, Horn, 2017, S. 183)

Art. 27 enthält Regelungen für Verantwortliche und Auftragsverarbeiter, die nicht im Unionsgebiet niedergelassen sind. Das bisher genutzte DVR-Meldeverfahren und das DVR selbst wird es nicht mehr geben. Bisher mussten bestimmte Datenverarbeitung laut DVR-Meldepflicht bekanntgegeben werden. Stattdessen verpflichtet Art. 30 Verantwortliche und Auftragsverarbeiter ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Dieses ist auf Anfrage der Aufsichtsbehörde vorzulegen. Für diese Verpflichtung gibt es Ausnahmen für kleine Unternehmen oder Einrichtungen wenn diese nicht z.B. sensible Daten verarbeiten. Daneben werden Verantwortliche verpflichtet, vor Inbetriebnahme eines neuen Datenverarbeitungssystems eine **Datenschutz-Folgenabschätzung** (Art. 35) durchzuführen. Hierbei werden die Risiken eines Verarbeitungsvorgangs für die Betroffenen beurteilt. Diese ist durchzuführen wenn die Verarbeitung nach dem ersten Eindruck ein hohes Risiko für die Betroffenen darstellt. Neu ist die Verpflichtung der **Meldung von Verletzungen des Schutzes personenbezogener Daten** an die Aufsichtsbehörde (Art. 33) und gegebenenfalls Betroffene von der Verletzung zu verständigen (Art. 34). Auch neu ist die verpflichtende **Bestellung eines Datenschutzbeauftragten** (Art. 37 bis 39) in bestimmten Bereichen. Diese führen die Aufgaben der DSB weisungsungebunden durch und berichten unmittelbar nur der höchsten Managementebene. Für Behörden und öffentliche Stellen wie Schulen ist ein Datenschutzbeauftragter bzw. eine Datenschutzbeauftragte vorgesehen. Die Art. 40 ff bauen das bereits bestehende System der Verhaltensregeln weiter aus. Die Art. 42 und 43 legen fest, dass bestimmte Verarbeitungsvorgänge von der Aufsichtsbehörde oder durch von ihr akkreditierte Zertifizierungsstellen zertifiziert werden können um nachzuweisen, dass die Verarbeitung in Übereinstimmung mit der DSGVO erfolgt. (Schmidl, 2018, S. 11-12)

4.2.7. Kapitel V Internationaler Datenverkehr

Kapitel V regelt die Voraussetzungen für den Datenverkehr mit Empfängern in Drittstaaten oder internationalen Organisationen. Ein derartiger Datenfluss ist nur unter bestimmten Bedingungen zulässig. Die Kernaussage von Kapitel V ist, dass die übermittelten Daten beim Empfänger im Drittstaat demselben Schutz wie in der EU unterliegen sollen. (Schmidl, 2018, S. 13)

4.2.8. Kapitel VI Unabhängige Aufsichtsbehörde

Wie derzeit wird es in jedem Mitgliedstaat zumindest eine unabhängige Aufsichtsbehörde geben. Die Aufgaben und Befugnisse der Datenschutzbehörden werden aber erheblich erweitert (Art. 57 und 58). Zusätzlich gibt es auf europäischer Ebene das European Data Protection Board (ESDB), den Europäischen Datenschutzausschuss. Diese Stelle wird für die Einhaltung der Datenschutzgrundverordnung, die Aufsicht über die nationalen Datenschutzbehörden und teilweise auch die Interpretation der DGVO zuständig sein. Andrea Jelinek, Chefin der österreichischen Datenschutzbehörde, wird die Vorsitzende des ESDB. (derstandard, 2018)

Art. 58 normiert drei Arten von Befugnissen. Zum einen sind dies Untersuchungsbefugnisse die es ihnen ermöglichen z.B. das Verzeichnis für Verarbeitungstätigkeiten einzusehen einschließlich eines Betretungsrechts bestimmter Räumlichkeiten. Zum zweiten werden sogenannte Abhilfebefugnisse eingeräumt, die es der Aufsichtsbehörde ermöglichen, ein rechtswidriges Verhalten abzustellen, durch konkrete Anordnungen oder die Verhängung von Geldbußen (mehr dazu in Kapitel VIII). Zum dritten verfügt die Aufsichtsbehörde über Genehmigungs- und Beratungsbefugnisse. (Schmidl, 2018, S. 14)

4.2.9. Kapitel VII Zusammenarbeit und Kohärenz

In diesem Kapitel sieht die DSGVO eine verstärkte Zusammenarbeit zwischen den einzelnen Aufsichtsbehörden vor. Das bringt eine wesentliche Verbesserung bei grenzüberschreitenden Sachverhalten. So soll unter Einbindung aller betroffenen Aufsichtsbehörden eine abgestimmte Entscheidung getroffen werden. Die bessere Vernetzung bringt auch Verbesserungen für Unternehmen, da Verfahren für den gesamten EU-Raum an einem Standort abgewickelt werden können. Die Aufsichtsbehörde am Sitz der Hauptniederlassung ist die federführende Aufsichtsbehörde. Festgeschrieben sind die Verpflichtung zur wechselseitigen Amtshilfe (Art. 61) und die Möglichkeit zur Durchführung gemeinsamer Maßnahmen der Aufsichtsbehörden (Art. 62). Die Einrichtung des Europäischen Datenschutzausschusses (ESDB) wird definiert (Art. 68). Der Datenschutzausschuss bekommt vielfältige Aufgaben zugewiesen (Art. 70), er darf Stellungnahmen abgeben und verbindliche Beschlüsse

fällen und wird somit auch eine koordinierende Aufgabe für die verbindliche Umsetzung der DSGVO übernehmen. (Schmidl, 2018, S. 15)

4.2.10. Kapitel VIII Rechtsbehelfe, Haftung und Sanktionen

Dieses Kapitel normiert unter anderem das **Recht auf eine Beschwerde** bei einer Aufsichtsbehörde. Nach Art. 80 können sich betroffene Personen von spezialisierten NGOs vor der Aufsichtsbehörde vertreten und Schadenersatz gerichtlich einklagen lassen. Die Mitgliedstaaten können laut DSGVO auch vorsehen, dass diese Einrichtungen auch unabhängig von einer Bevollmächtigung Beschwerde bei der Aufsichtsbehörde einreichen können. (Feiler, Forgó, 2018, S. 340-344)

Die Möglichkeit eines Verbandsklagerechts wurde in keinem EU-Land vollständig umgesetzt. In Österreich ist am 20. April 2018 der Versuch ein Verbandsklagerecht im Zuge der Datenschutzanpassungsgesetze zu schaffen gescheitert. Die SPÖ hatte auf einen Änderungsantrag diesbezüglich bestanden, dieser wurde von der Regierung und vor allem von der ÖVP nicht mitgetragen. Es hätte die Stimmen der FPÖ, ÖVP und der SPÖ bedurft um die nötige zweidrittel Mehrheit für diese Verfassungsmaterie zu erreichen. (Parlamentskorrespondenz Nr. 442, 2018)

Das Verbandsklagerecht gäbe NGOs wie noyb, die neue Organisation von Max Schrems, oder epicenter.works die Chance, Datenschutz auch gegen große Konzerne rechtlich durchzusetzen und Österreich die Chance eine europäische Vorreiterrolle im Bereich Datenschutz einzunehmen. Mit dem Verbandsklagerecht muss nicht jede Nutzerin und jeder Nutzer selbst vor Gericht ziehen und das Risiko tragen ein Gerichtsverfahren gegen Top-Anwältinnen und Anwälte von US-Konzernen zu führen. (Steinhammer, 2018)

Art. 82 bringt auch die **Möglichkeit Schadenersatz** für erlittenen materiellen und immateriellen Schaden zu verlangen. Art. 83 enthält eine große Änderung, er enthält die **Geldbußen** und **Verwaltungsstrafen**. Diese sind jetzt auf dem Niveau vom Kartellrecht und reichen je nach Verstoß bis zu 20 Millionen Euro oder, im Falle eines Unternehmens, bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ist. (Schmidl, 2018, S. 15)

In Art 83 Abs. 7 DSGVO heißt es: „Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können." Österreich hat sich hier in der Umsetzung für eine Straffreiheit von Behörden entschieden. Die Abhilfebefugnisse, also die Möglichkeit der Datenschutzbehörde für die Einhaltung der DSGVO ist davon nicht berührt, aber ziemlich zahnlos.

4.2.11. Kapitel IX – XI

Kapitel IX enthält Vorschriften für besondere Verarbeitungssituationen beispielsweise Freiheit der Meinungsäußerung und Zugang zu amtlichen Dokumenten. Das Kapitel X Delegierte Rechtsakte und Durchführungsrechtsakte regelt die Ausübung der Befugnisübertragung insbesondere der Europäischen Kommission und das Ausschussverfahren. In Kapitel XI, den Schlussbestimmungen sind auch das Außerkrafttreten der DSRL und im letzten Artikel Nr. 99 das Inkrafttreten der DGVO mit 25.05.2016 und die Gültigkeit ab dem 25.05.218 definiert. (Feiler, Forgó, 2017, 355 - 387)

4.3. Novellierung des DSG 2000

Schon im Vorjahr wurde das Datenschutzanpassungsgesetz 2018 beschlossen, das im DSG 2000 die durch die DSGVO notwendig gewordenen Veränderungen vornimmt. Eine Anpassung eines bestehenden Gesetzes nennt man Novellierung.

Die Datenschutz-Grundverordnung ist als EU-Verordnung in jedem EU-Mitgliedsstaat unmittelbar anwendbar. Trotzdem werden die nationalen Gesetze im Sinne einer Vereinheitlichung angepasst. Außerdem enthält die EU-DSGVO, wie oben beschrieben, Öffnungsklauseln und lässt dem nationalen Gesetzgeber gewisse Spielräume. Deshalb wurde in Österreich das „Datenschutz-Anpassungsgesetz 2018", eine Novelle des DSG 2000, beschlossen. Gültig sind diese Änderungen gleichzeitig mit der EU-DSGVO am 25. Mai 2018. Enthalten ist unter anderem die neue Festlegung der Altersgrenze auf 14 Jahre. Der Spielraum den die Verordnung hier lässt,

vom dort angegebenen Alter von 16 abzuweichen, wird von Österreich ausgeschöpft. Enthalten sind auch die Bestimmungen zur Schaffung der Datenschutzbehörde nach EU-Vorgabe, Verwaltungsstrafbestimmungen und sonstige Regelungen. (WKO, 2017)

4.4. Datenschutz-Anpassungsgesetze Bildung

2018 wurde das Datenschutz-Anpassungsgesetz beschlossen. Es enthält neben begrifflichen Änderungen, auch eine im Lichte des Regierungsprogramms interessanten Teil über die Schaffung eines Datenverbundes, ähnlich den Universitäten. Im Folgenden wird dieser Sachverhalt erläutert.

Die „durchgehende Bildungsdokumentation“

Das aktuelle Regierungsprogramm 2017-2022 der ÖVP-FPÖ Bundesregierung sieht auf Seite 63 die Einführung einer durchgehenden Bildungs- und Leistungsdokumentation über den gesamten Bildungsverlauf vor:

„Durchgehende Bildungs- und Leistungsdokumentation für jede Schülerin und jeden Schüler einführen – Entwicklung und Anwendung einheitlicher, digital gestalteter Dokumentationssysteme über den Bildungsfortschritt von Schülerinnen und Schülern, beginnend ab dem verpflichtenden Kindergartenbesuch bis hin zum Abschluss der schulischen Bildungslaufbahn zur Verbesserung der Information an den Nahtstellen.“ (epicenter.works, 2017, S. 63)

Eine Zentralisierung von personenbezogenen Daten über den individuellen Lernerfolg vom Kindergarten bis Universitätsabschluss bedeutet eine inhärente Gefahr. Eine große Menge an zum Teil hochsensiblen Daten in der beschriebenen Form zu speichern, ist meiner Meinung nach aus Datenschutzsicht an sich abzulehnen.

Es sieht aber so aus, als wäre die „durchgehende Bildungsdokumentation“ wie im Regierungsprogramm gefordert in der Novellierung des Bildungsdokumentationsgesetzes enthalten und von den Legisten des Bildungsministeriums sauber gelöst. Hier wird nämlich ein Datenverbund der Schulen (§ 7c sowie Anlage 4 in der vorliegenden Entwurfsfassung) implementiert, ähnlich dem Datenverbund des universitären und hochschulischen Bereichs. Dieser soll den elektronischen Transfer, der schon jetzt bei Aufnahme von Schülerinnen und Schülern gesetzlich zu erfassenden

Daten, ermöglichen. Jetzt müssen die Daten bei jedem Schulwechsel neu eingegeben werden. Dies soll den derzeit nicht unerheblichen Verwaltungsaufwand an den Schulstandorten, bei der Aufnahme von Schülerinnen und Schülern, verringern. Dazu wird beim Datenverbund, dem Austrian Education System Network (AESN) keine eigene Datenbank befüllt, sondern eine Verarbeitung bzw. Übermittlung der Schülerdaten nur zwischen den zwei beteiligten Bildungseinrichtungen erfolgen („Peer-to-Peer"-Architektur"). Außerdem werden die Daten nur für die Schule, die sie aufgrund des Schulwechsels braucht, freigegeben. Im Verbund werden die Daten dann nach Abruf durch die entsprechende Schule wieder gelöscht. Und es werden keine weiteren zu den aktuell zu erfassenden Daten hinzugefügt. (DSAG-Bildung, 2018)

Diese datenschutzfreundliche Lösung ist nach meiner Meinung sehr zu begrüßen und es bleibt zu hoffen, dass man sich weiter an starkem Datenschutz orientiert, statt ein ausuferndes Bildungsdokumentationssystem wie z.B. in Estland zu installieren, das jede Verhaltensauffälligkeit vom Kindergarten an dokumentiert. Niemand kann voraussagen, ob diese Daten nicht einmal geleaked werden oder einfach eine gesetzliche Regelung geschaffen wird, die den Zugriff in weit größerem Maß ermöglicht. (E-Estonia, 2018)

Auch bildungspolitische Gründe sprechen gegen eine überschießende Umsetzung, wie in Estland. Dort haben die Eltern in Echtzeit Zugriff auf die Leistungsbeurteilungen und andere Informationen zum Verhalten ihrer Kinder in der Schule. Im Sinne einer während des Heranwachsens zu erlernenden, Selbstständigkeit halte ich es für kontraproduktiv, den jetzt schon bestehenden Trend zu „Helikoptereltern", also hyperprotektiven Eltern, noch zu verstärken. (Spitzer, 2015)

5. Änderungen für die Schulen

5.1. Überblick

Die DSGVO zeigt auch Auswirkungen auf die österreichischen Schulen. Es wird „Privacy by Design“ implementiert und es wird der Grundsatz „Facebook und WhatsApp sind fürs Wohnzimmer die Lernplattform ist fürs Klassenzimmer“ etabliert. Es wird also eindeutig noch mehr Augenmerk auf Datenschutz gelegt.

5.2. Datenschutzverantwortliche(r) an den Schulen

Es ist wie nach alter Rechtslage die Schulleiterin oder der Schulleiter der Datenschutzverantwortliche; d.h. die Beurteilung über die datenschutzrechtliche Einordnung von E-Learningplattformen oder sonstige Tools, die Lehrkräfte an der Schule im Unterricht verwenden, obliegt der Schulleitung. Für sie gibt es Ansprechpartner im Bundesministerium für Bildung, Wissenschaft und Forschung und beim Landesschulrat. In der Praxis werden sie sich oft an der Expertise des Fachpersonals in den Schulen, wie den IT-Kustoden, orientieren. Generell gilt sowohl für die alte wie für die neue Rechtslage bei Servern die nicht von der Schule selber betrieben werden, aber sich im EU-Raum befinden, sollten die Schulen eine Vereinbarung zur Auftragsdatenverarbeitung mit dem Dienstleister, dem Auftragsdatenverarbeiter, abschließen. (Menzel, 2017)

5.3. Datenschutzbeauftragter

Es wird einen Datenschutzbeauftragten im Ministerium geben. Diese Funktion nimmt Ministerialrat Dr. Thomas Menzel wahr. Und es wird einen Datenschutzbeauftragten in jedem Landesschulrat geben. Der Landesschulrat wird auch die Datenschutzaspekte für den Bereich der Bundesschulen im eigenen Bundesland übernehmen. Es muss also keine Schule einen Datenschutzbeauftragten bestellen. Es zeichnet sich aber ab, dass neben Hochschulen zum Teil auch Schulen eigene Datenschutzbeauftrage ernennen, um die eigene (Hoch)schulleitung zu unterstützen. Die erforderliche vierstündige bis eintägige Schulung von Schulleiter/innen, Administratoren und IT-Kustoden wird vom Ministerium angestrebt. Datenschutz wird

auch im Curriculum der zukünftigen Schulleiterausbildung verankert. Auch Schulungsmaterial zum Selbststudium wird zur Verfügung gestellt.[3] (Menzel, 2017)

Eine Bestellung eines oder einer Datenschutzbeauftragten an jeder Schule macht auf Grund der Komplexität, der laufenden technischen Veränderungen, der Vielzahl an betroffenen Bereichen nicht nur Sinn, sondern ist meiner Meinung nach sehr empfehlenswert.

5.4. Dokumentationspflicht/Anwendungsverzeichnis

Die bisherigen Meldepflichten und Genehmigungspflichten im Datenverarbeitungsregister fallen weg. Dafür muss aber jede eigene Anwendung in einem Verzeichnis der Verarbeitungstätigkeiten (VdV) dokumentiert werden. Das BMBWF will die Schulen bei der Umstellung weitestgehend entlasten. Alles was als Standardanwendungen an Schulen ausgerollt wird und wurde, alle Anwendungen die das Ministerium oder ein Landesschulrat den Schulen vorgibt, also Sokrates Web an den Pflichtschulen oder Sokrates an den Bundesschulen, WebUntis als elektronisches Klassenbuch, Lernplattformen wie Moodle oder lms.at oder andere sind Anwendungen die vom Ministerium ausgehen und für die sich das Ministerium auch um die DSGVO konforme Umsetzung kümmert. Für Anwendungen die Schulen selbstständig einsetzen müssen sie sich auch um die Führung eines VdV kümmern.

5.5. Informationspflichten

Die Schule und das Bundesministerium für Bildung müssen die Schüler bzw. Eltern vollständig und in verständlicher Form über die Datenverarbeitung informieren. Zu erfolgen hat dies bei neuen Datenverarbeitungen schon bevor sie beginnt. Für die vor in Kraft treten der DSGVO gemachten Datenverarbeitungen kann sie nachgereicht werden. Enthalten sein müssen die Datenkategorien, also was wofür gespeichert wird und an wen es weitergegeben wird. Dieser Informationspflicht ist das BMBWF bis jetzt nicht nachgekommen.

[3] http://pubshop.bmb.gv.at/detail.aspx?id=648

5.6. Alter für die Einwilligung

Das Mindestalter für die Einwilligung in Datenspeicherung und Verarbeitung wurde geregelt. Aus den Bedingungen für die Einwilligung eines Kindes in Bezug auf die Dienste der Informationsgesellschaft und dem DSG lässt sich ableiten, dass für Kinder bis zum 14. Lebensjahr die Eltern die Ansprechpartner sind an die sich die Information zu richten hat. Die DSGVO (Art 8 Abs 1 DSGVO) sieht hier prinzipiell eine Altersgrenze von 16 Jahren vor, ermöglicht aber den Nationalstaaten auch eine geringere Altersgrenze festzulegen, die jedoch nicht unter dem vollendeten dreizehnten Lebensjahr liegen darf. Österreich hat dies in der Novellierung des DSG (§ 4 Abs 4 DSG) ausgeschöpft und die Altersgrenze auf 14 Jahre festgelegt. (Feiler, 2018, S. 121)

5.7. Lehrmaterial

Auch Lehrmaterialien wie Schulbücher sollten von Anleitungen zu datenschutzmäßig fragwürdigem Verhalten bereinigt werden. In gängigen Schulbüchern fanden sich bisher solche Aufbereitungen die schon länger von Datenschützern kritisch gesehen wurden. So wurde z.B. das Thema E-Mail unkritisch anhand eines Gmail-Kontos erläutert und die Schülerinnen und Schüler dazu angeleitet sich ein solches E-Mailkonto bei Google zu erstellen. (Kopeinigg, 2016)

6. Datenschutz aus Sicht der Schülerinnen und Schüler

6.1. Überblick

Für das Verwenden personenbezogener Daten bedarf es entweder einer gesetzlichen Grundlage (etwa im DSG, im SchUG oder im BilDokG) oder einer Zustimmung der Schülerinnen und Schüler bzw. der Erziehungsberechtigten.

Überdies muss das Verwenden personenbezogener Daten verhältnismäßig sein. Die Verwendung darf also nur dann erfolgen, wenn sie geeignet ist, das damit verbundene Ziel zu erreichen, wenn sie unbedingt notwendig ist und nicht übermäßig in die Grundrechte eingreift. (Lachmayer, Menzel, 2018, S. 24)

Die Schulleitung ist Verantwortlicher im Sinne der DSGVO und unterliegt gegenüber der Schülerin oder dem Schüler im Einzelfall einer Auskunftspflicht, einer Richtigstellungspflicht und einer Löschungspflicht wie hier weiter ausgeführt wird.

6.2. Recht auf transparente Information

Ein Hauptanliegen des europäischen Gesetzgebers war die Stärkung individueller Rechte von Betroffenen, also von Menschen, deren Daten verarbeitet werden. Ein wesentlicher Teil dieses Kapitels behandelt die Transparenz- und Informationsverpflichtungen gegenüber Betroffenen.

Im Artikel 12 Absatz 1 der DSGVO heißt es:

„Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten. Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch. Falls von der betroffenen Person verlangt, kann die Information mündlich erteilt werden, sofern die Identität der betroffenen Person in anderer Form nachgewiesen wurde.“ (Pollir et al., 2017, S. 42)

Welche Daten von Schülerinnen und Schülern gespeichert und verarbeitet werden ist wie weiter oben beschrieben gesetzlich geregelt. Schülerinnen und Schüler haben jedenfalls aufgrund der DSGVO das Recht auf vollständige Transparenz und Information darüber (Art 13 DSGVO), welche ihrer Daten auf welche Weise verarbeitet werden. Dies ist elementar, damit Betroffene ihre Rechte überhaupt ausüben können. Der Grundsatz der Transparenz definiert, dass für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst sind und gegebenenfalls zusätzlich visuelle Elemente verwendet werden (Icons oder Bildsymbole, ErwGr 58 und Art 12 Abs 7 DSGVO). Erfolgt die Verarbeitung aufgrund eines „berechtigten Interesses" und nicht aufgrund einer Einwilligung der betroffenen Person oder einer gesetzlichen Grundlage, muss mitgeteilt werden, welche berechtigten Interessen vom Verantwortlichen verfolgt werden. Wenn sich etwas an der Datenverarbeitung ändert, also andere Daten gesammelt oder Daten zu einem anderen Zweck verarbeitet oder zusammengeführt werden, müssen die Betroffenen ebenfalls über diese Änderung informiert werden. So muss eine Schülerin oder ein Schüler beispielsweise darüber informiert werden, wenn über ihn/über sie im Zuge von Profiling-Prozessen Entscheidungen automationsunterstützt getroffen werden. Dieses Recht auf Information auch bei Änderungen, ist vor allem in Zeiten von massivem Ausbau der digitalen Strukturen des Staates und der Schulverwaltung wichtig. Wie Ministerrat Dr. Menzel im Experteninterview (Experteninterview, Menzel, 2017) sagt, wird man um der gesetzlichen Forderung nachzukommen, alle den Bund betreffenden Anwendungen die nötigen Informationen auf einer Webseite online stellen.

Wenn Daten von Schülerinnen und Schülern über und für andere Anwendungen als jene des Bundes gespeichert werden sind die Betreiberinnen und Betreiber der Anwendung für die Auskunft der Information zuständig. Also im Fall einer an einer Schule entwickelten und genutzten Anwendung ist die Direktion der jeweiligen Schule zuständig. (Menzel, 2017)

Um dem Erziehungsauftrag, Schülerinnen und Schüler zu informierten Bürgerinnen und Bürgern zu machen, nachzukommen und dem Text der EU-DSGVO „*...in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell*

an Kinder richten" zu folgen ist zu hoffen, dass man hier mit gutem Beispiel voran geht und die Chance für die Schaffung eines Best-Practice Beispiels nutzt.

6.3. Recht auf Auskunft

Nach Art 15 DSGVO hat die betroffene Person, also in diesem Fall die Schülerin oder der Schüler sowie Absolventen und Absolventinnen bzw. deren Erziehungsberechtigte, ein Recht auf Auskunft. Dieses umfasst eine Bestätigung, ob personenbezogene Daten verarbeitet werden und das Recht eine Kopie der Daten zu erhalten. Im Unterschied zum Recht auf Datenübertragbarkeit sind Daten der Betroffenen nicht in einer maschinenlesbaren, sondern in einer für sie verständlichen Weise zu übermitteln. (Feiler, Forgó, 2017, S. 143-146)

Wie können Schülerinnen und Schüler bzw. ihre Eltern oder andere Erziehungsberechtigte dieses Recht wahrnehmen? Die Schulleitung ist Verantwortliche/r im Sinne der DSGVO und deshalb auch Ansprechpartner/in für ein Auskunftsbegehren. Diese wissen auch, ob neben den Standardtools zur Schülerverwaltung noch andere schulspezifische Lösungen genutzt werden und miteinzubeziehen sind. Das System Sokrates, das vom Bund zur Speicherung der Schülerdaten verwendet wird, ist eine sogenannte mandantenfähige Datenbank. Die Daten liegen zentral im Rechenzentrum und sind dort verschlüsselt. Nur das jeweilige Personal an einer Schule kann die Daten der Schule einsehen. Auch die Berichte, die aufgrund gesetzlicher Grundlagen, an den Landesschulrat zu schicken sind werden vom Schulleiter erstellt und verschickt. Der Landesschulrat hat keinen direkten Zugriff. Sowohl die Verwaltungsserver, so wie Digi4school, die elektronischen Schulbücher, die beiden Lernplattformen und das elektronische Klassenbuch liegen auf österreichischen Servern. (Menzel, 2017)

Die Auskunft muss wenn sie elektronisch an den Verantwortlichen gestellt wird auch elektronisch beantwortet werden. Die Auskunft kann, wenn die Betroffenen das wollen, ebenso per Brief oder mündlich erteilt werden. Bei den österreichweit genutzten Tools zur Schülerverwaltung würde sich auch die Möglichkeit anbieten einen **Online-Self-Service-Zugang** einzurichten. Damit können Betroffene ihre Daten selbst abrufen. Um die Sicherheit der personenbezogenen Daten zu gewährleisten

wäre in diesem Fall eine Sicherstellung der Identität durch einen strengen Authentifikationsprozess angemessen. (Feiler, Horn, 2017, S. 85)

Die Auskunft muss einmal im Jahr kostenlos sein, bei wiederholten Anfragen darf ein Entgelt, das dem Verwaltungsaufwand entspricht, verlangt werden. Die Auskunft hat innerhalb von vier Wochen zu erfolgen. Im begründeten Einzelfall kann die Frist um zwei Monate verlängert werden. (Feiler, Forgó, 2017, S. 143-144)

6.4. Recht auf Vergessenwerden und Richtigstellung

Das Recht auf Löschung (Art. 17 DSGVO) wird in der DSGVO auch **Recht auf Vergessenwerden** genannt. Betroffene, also Schülerinnen und Schüler oder deren Erziehungsberechtigte, können in gewissen Fällen die Löschung ihrer Daten vom Verantwortlichen, also der Schulleitung, verlangen. Das kann der Fall sein, wenn es keine rechtliche Grundlage (mehr) für die Speicherung gibt. Also wenn Daten zu lange gespeichert wurden oder mehr Daten als gesetzlich vorgesehen sind. Für die gesetzlich festgelegten Daten gibt es genaue Regelungen für die Speicherdauer. So sind z.B. die in den Evidenzen enthaltenen Sozialversicherungsnummern oder Ersatzkennzeichen zwei Jahre nach Abgang der Bildungseinrichtung zu löschen. Daten wie die Teilnahme an Unterrichts- und Betreuungsangeboten, den Schulerfolg, die Schul- bzw. Unterrichtsorganisation und der Bildungsverlauf werden nach 60 Jahren gelöscht. (§ 8 Abs. 5 BilDokG) Ein anderer Fall wären z.B. Daten deren Verarbeitung und Speicherung ein Betroffener zugestimmt hat und nun seine Zustimmung wiederruft. (Feiler, Forgó, 2017, S. 147-150)

In den Erwägungen zu Art. 17 wird dem Recht auf Vergessen spezielle Bedeutung für den Wiederruf von im Kindesalter gegebenen Einwilligungen zugestanden. Insbesondere wenn Kinder die mit der Verarbeitung verbundenen Gefahren nicht in vollem Umfang abschätzen konnten. Dies ist aber nur als Erläuterung zu sehen, da allen Betroffenen dieses Recht (Art 17 Abs 1 lit b DSGVO) ohnehin zusteht. (Feiler, Forgó, 2017, S. 151)

Es gibt außerdem ein **Recht auf Berichtigung** (Art. 16 DSGVO). Das heißt Betroffene können falsche Daten richtig stellen lassen und unvollständige Daten ergänzen. (Feiler, Forgó, 2017, S. 147)

6.5. Pflichten

Es gibt auch ein paar Pflichten bezüglich der personenbezogenen Daten. So haben gemäß § 61 Abs 3 SchUG die Erziehungsberechtigten „die für die Führung der Amtsschriften der Schule erforderlichen Dokumente vorzulegen und Auskünfte zu geben sowie erhebliche Änderungen dieser Angaben unverzüglich der Schule mitzuteilen". Alle Daten die gesetzlich vorgeschrieben sind wird eine Schülerin bzw. ein Schüler oder deren Erziehungsberechtigte bekanntgeben müssen. Wie der Fall liegt, wenn die Schule eine zusätzliche eigenverantwortliche Datenerfassung und Verarbeitung betreibt, wird man sich im speziellen Einzelfall ansehen müssen.

Bei dem Recht auf Auskunft gibt es prinzipiell eine Mitwirkungspflicht der Betroffenen. Dieses wird sich in der Praxis in der Schule im Vergleich zu anderen Bereichen in Grenzen halten, da die Schulleitung über die Schülerinnen und Schüler betreffende Datenverarbeitung informiert sein muss. Das heißt so viel wie „sie wissen schon wo sie suchen müssen".

6.6. Selbstbestimmtes Leben im digitalen Zeitalter

Alle vorangegangenen Ausführungen machen deutlich, wie wichtig das Thema der informationellen Selbstbestimmung für ein auch im Allgemeinen selbstbestimmtes Leben mittlerweile ist. Um dieses selbstbestimmte Leben führen zu können haben die Schülerinnen und Schüler des österreichischen Schulsystems das Recht auf die Problemstellungen unserer Zeit vorbereitet zu werden.

Dafür ist es notwendig, den Datenschutz gerade für Schutzbefohlene genauestens durchzusetzen und dem Thema ausreichend Raum im Unterricht und damit auch in den Lehrplänen zu geben, um die teilweise komplexen Sachverhalte vermitteln zu können. Deshalb ist das neu geschaffene Fach „Digitale Grundbildung" zu begrüßen. Datenschutz wird hier Teil des Lehrplans sein. Ab dem Schuljahr 2018/19 beginnt die flächendeckende Umsetzung für alle Schulen der Sekundarstufe I (NMS, AHS). (bildung.bmbwf.gv.at, 2018)

7. Datenschutz aus Sicht der Lehrkräfte

7.1. Überblick

Dieses Kapitel behandelt das Thema Datenschutz aus Sicht der Lehrkräfte. Es betrifft einerseits Rechte und Pflichten im Arbeitsalltag und bei der Wahrnehmung von Aufgaben in der Schüler(innen)verwaltung, andererseits aber auch das Thema Datenschutz im Unterricht und aus pädagogischer Sicht. Nicht in diesem Kapitel thematisiert werden Bereiche des Datenschutzes die das normale Angestelltenverhältnis einer Lehrkraft betreffen.

Datenschutz im Unterricht hat für Lehrer und Lehrerinnen aus zwei Gründen eine besondere Bedeutung. Erstens kommt ihnen bei der Wahrung von Rechten von Schutzbefohlenen besondere Sorgfaltspflicht zu, andererseits ist die Schaffung von Bewusstsein und Kenntnissen im Bereich Datenschutz für die Schülerinnen und Schüler für ihr gesamtes späteres Leben von Bedeutung. Das Thema Datenschutz für Lehrerinnen und Lehrer beinhaltet den Aufbau eines Bewusstseins dafür, wann und in welchem Zusammenhang Daten von Schülerinnen und Schülern verwendet werden und die Weitergabe von Daten und dessen Begründung, also wem gebe ich die Daten weiter und wieso? Des Weiteren geht es um Schutzmaßnahmen, die verhindern sollen, dass Daten in falsche Hände geraten und um den richtigen Umgang mit Apps und Software. Lehrkräfte müssen eigenständig entscheiden mit welchen Apps sie arbeiten und einschätzen, ob Firmen dabei Schüler(innen)daten sammeln. Auch das Löschen von Daten - damit diese nicht unnötig gesammelt werden - muss im Fokus stehen. Daten die nicht mehr gebraucht werden müssen umgehend gelöscht werden. (Lachmayer, Menzel, 2017, S. 2)

7.2. Die Schülerverwaltung

7.2.1. Vorgeschriebene Anwendungen

Die meisten der Anwendungen für die Schülerverwaltung (WebUntis, SokratesWeb, etc.) wie ein elektronisches Klassenbuch werden vom Bund zur Verfügung gestellt. Bei Anwendungen die dem Lehrpersonal vorgeschrieben werden, wie eine E-

Mailadresse zur Kommunikation oder das Benutzen eines elektronischen Klassenbuches zur Erfassung von Anwesenheit und anderen Daten von Schülerinnen und Schülern liegt die Verantwortung für datenschutzkonforme Umsetzung nicht bei der Lehrperson. Sehr wohl aber dafür was ins Klassenbuch eingetragen wird. Sensible Daten (sexuelle Orientierung, politische Meinung etc.) dürfen nur dann im Klassenbuch vermerkt werden, wenn deren Dokumentation ein erhebliches öffentliches Interesse darstellt. Also wenn es sich um einen gravierenden Vorfall handelt und die sensiblen Daten zur Darstellung unbedingt notwendig sind. (Menzel, 2017)

7.2.2. E-Mails

Es sollten für die schulische Kommunikation (LehrerInnen, SchülerInnen, Eltern, etc.) nur die Schul-E-Mail-Konten genutzt werden. Berufliche Kommunikation über private E-Mail-Adressen zu führen oder weiterzuleiten ist wie in anderen Berufen auch nicht zu empfehlen. Um Datenschutz im E-Mailverkehr wirklich umzusetzen sollte PGP-Verschlüsselung für alle Personen im Schulwesen implementiert werden. PGP ist eine Möglichkeit die es seit den 90ern gibt um Ende-zu-Ende-Verschlüsselung im Emailverkehr zu nutzen. Von allen Nationalratsabgeordneten in Österreich hatte 2018 nur einer diese Verschlüsselungsmöglichkeit nachweislich genutzt. Österreich hinkt hier also insgesamt nach.

7.2.3. Kennwörter

Die wichtigste Aufgabe der Lehrerinnen und Lehrer, den Datenschutz in der Schülerverwaltung betreffend ist der verantwortungsvolle Umgang mit Kennwörtern, mit denen der Zugang zu Anwendungen geschützt ist. Fahrlässigkeit in diesem Bereich ist kein Kavaliersdelikt und kann dienstrechtliche Konsequenzen nach sich ziehen.

Welches Verhalten fällt unter Fahrlässigkeit und welches ist lediglich ein sicherheitstechnischer Makel? Unter fahrlässiges Verhalten fällt zum Beispiel eindeutig das unsichere Verwahren von Kennwörtern, egal ob beabsichtigt oder unbeabsichtigt. Ein Beispiel dafür ist der berühmte Klebezettel mit dem Kennwort am Bildschirm.

Ein anderes Beispiel ist das unbeabsichtigte öffentlich machen von Kennwörtern. Hier gab es einen beispielhaften Fall eines Abteilungsvorstands an einer HTL. Die HTL hatte zwei WLANs. Ein schnelles da nur wenige Lehrer dieses nutzten, und ein

langsameres das für die Schüler angelegt worden war. Er wollte seinen Schülern und Schülerinnen etwas Gutes tun und schrieb an die Tafel sein Kennwort um ihnen einen Zugang zu schnellerem Internet zu ermöglichen, vergaß dabei allerdings, dass er auch gleichzeitig das Passwort für seinen SokratesWeb-Zugang preisgab. (Menzel, 2017)

Ein anderes Beispiel dafür wie schnell Daten öffentlich werden können ist der Fall eines Direktors der seinen Verwaltungs-PC am Schreibtisch stehen hatte. Auf diesem PC hatte er ein paar Briefe an den Bürgermeister der Gemeinde geschrieben, in denen er bittet einige Kollegen disziplinarrechtlich abzumahnen, weil sie laufend 10 Minuten zu spät zum Unterricht kamen. Und dann hat dieser Kollege sein WindowsKennwort im öffentlich im Internet gespeichert. Er stand mit dem Curser an der falschen Stelle, hat dort sein Kennwort eingegeben und auf Enter gedrückt. Damals hat sich Anonymous gerade darauf spezialisiert Lücken im Bildungsbereich zu finden, hat dann dieses Kennwort des Direktors entdeckt und die komplette Festplatte von ihm heruntergeladen und ins Internet gestellt. Es haben zwar nur einige wenige Insider mitbekommen, dass diese Briefe online standen, aber das ist nur passiert weil das Kennwort nicht sicher verwahrt wurde. (Menzel, 2017)

Am letzten Beispiel sieht man eine der Gefahren die es mit sich bringt, wenn ein Kennwort für mehrere Accounts genutzt wird. Lehrerinnen und Lehrer sollten daher keine Kennwörter unnötig doppelt vergeben oder gar ein und dasselbe Kennwort für alle ihre Zugänge verwenden. Auch wenn es praktisch erscheint, erhöht sich die Gefahr dadurch sehr. Wird das Kennwort einer Anwendung durch einen Angreifer ermittelt, bleibt für den Angreifer der Zugriff auf eine andere Anwendung weiterhin verwehrt wenn diese mit einem eigenen Passwort geschützt ist.

Der letzte Hinweis gehört schon zur Gruppe der allgemeinen Sicherheitshinweise für Kennwörter. Dazu gehören noch das regelmäßige Wechseln von Kennwörtern und das Wählen von komplexen Kennwörtern.

Nicht komplex sind alle Kennwörter aus die aus Wörtern bestehen oder in einem Zusammenhang mit dem Nutzer stehen (Geburtsdatum etc.). Kennwörter die die Komplexitätsanforderungen erfüllen bestehen aus einer zufälligen Folge von Groß-

und Kleinbuchstaben, Zahlen und Sonderzeichen und sind mindestens 8 Zeichen lang.

Die unten stehende Tabelle zeigt wie lange jemand mit purer Rechenkraft braucht, um alle möglichen Kombinationen durch zu probieren und ein Kennwort mit 4 bis 12 Zeichen zu knacken. (Beutenmüller, Greinert, 2018)

Maximale Rechenzeit eines Brute-Force-Angriffs bei 1 Milliarde Schlüsseln pro Sekunde

	Passwortlänge								
Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**	**11 Zeichen**	**12 Zeichen**
10 [0-9]	<1 ms	<1 ms	1 ms	10 ms	100 ms	1 Sekunde	10 Sekunden	2 Minuten	17 Minuten
26 [a-z]	<1 Sekunde	<1 Sekunde	<1 Sekunde	8 Sekunden	4 Minuten	2 Stunden	2 Tage	42 Tage	3 Jahre
52 [A-Z;a-z]	<1 Sekunde	<1 Sekunde	20 Sekunden	17 Minuten	15 Stunden	33 Tage	5 Jahre	238 Jahre	12.400 Jahre
62 [A-Z;a-z;0-9]	<1 Sekunde	<1 Sekunde	58 Sekunden	1 Stunde	3 Tage	159 Tage	27 Jahre	1.649 Jahre	102.000 Jahre
96 (+Sonderzeichen)	<1 Sekunde	8 Sekunden	13 Minuten	21 Stunden	84 Tage	22 Jahre	2.108 Jahre	202.000 Jahre	19 Mio Jahre

Abbildung 1 Auswirkung unterschiedlicher Kennwortkomplexität

Die Wahl guter Kennwörter und deren Verwaltung sind deshalb das A und O jedes sicherheitsbewussten PC-Anwenders. Um dies problemlos zu bewältigen bedient man sich am besten einer eigenen Software zur Generierung und Verwaltung von Kennwörtern. Dabei werden die Kennwörter verschlüsselt auf der Festplatte abgelegt und können von dort per Klick abgerufen werden. So kann man problemlos eine große Anzahl komplexer Kennwörter verwalten. Hier gibt es eine große Auswahl und auch kostenlose Open- Source-Varianten wie z.B. KeePass. Damit kann man auch lange Kennwörter problemlos verwalten und zufällige Kennwörter in beliebiger länge generieren.

Kennwörter sollten nur über verschlüsselte Kanäle übertragen werden, dazu bieten sich Messenger mit sicherer Verschlüsselung oder E-Mails mit PGP-Verschlüsselung an. Auf Messenger werde ich im Kapitel 7.6 genauer eingegangen. Warum man Mails mit sensiblen Daten verschlüsseln sollte und wie man das einfach und sicher umgesetzt werden kann, wird hier in Folge kurz erläutert.

Unverschlüsselte Mails sind wie Postkarten, jeder der sie in die Hände bekommt kann sie lesen. Open PGP ist ein standardisiertes Datenformat für verschlüsselte und digital signierte Daten. Damit lassen sich unter anderem auch E-Mails verschlüsseln. Damit bekommt unsere Postkarte ein Kuvert. Es gibt Plugins für die E-Mail-Clients Outlook und Thunderbird, damit lassen sich E-Mails mit einem Mausklick

Ver- und Entschlüsseln. Das zugrundeliegende kryptografische Verfahren benutzt ein Schlüsselpaar aus zwei zusammengehörigen Schlüsseln, einem öffentlichem und einem geheimen. Der öffentliche Schlüssel kann beliebig geteilt werden, den brauchen andere um eine E-Mail zu verschlüsseln. Der private Schlüssel bleibt immer privat, das stellt sicher dass man nur selbst E-Mails wieder verschlüsseln kann. (OpenPGP.org, 2016)

7.2.4. Eigene Aufzeichnungen

Eigene Aufzeichnungen müssen natürlich weiterhin nicht nur möglich sein sondern sind auch notwendig. Lehrkräfte müssen Leistungen von Schülerinnen und Schülern mitdokumentieren um zu einer möglichst objektiven Leistungsbeurteilung zu kommen. Soweit die Einspruchsfristen z.B. bei Leistungsbeurteilungen bestehen, müssen die Aufzeichnungen auch aufbewahrt werden (gesetzliche Grundlage). Wenn diese Aufzeichnungen elektronisch geführt werden ist Datensicherheit und Datenschutz zu beachten. Wenn ich als Lehrkraft Microsoft mit mein Schulkonto nutze um solche Aufzeichnungen zu führen, ist die rechtliche Situation durch die Verträge mit dem Bildungsministerium gedeckt. Ein Googlekonto im Gegensatz dazu ist denkbar ungeeignet um Daten über Schüler zu speichern. Google analysiert alle Informationen bis in die Textinhalte von E-Mails. Das notwendige Datenschutzniveau um Daten von bzw. über Schutzbefohlene zu speichern ist hier keinesfalls gegeben. Bei allen anderen Möglichkeiten ist die rechtliche und technische Situation zu beurteilen. Das notwendige Wissen ist hier Voraussetzung. Lehrkräfte sollten sich ihrer Verantwortung bewusst sein und möglichst sichere Varianten bevorzugen. Eventuell wird es zu diesem Thema noch Richtlinien vom Bildungsministerium oder dem Landesschulrat geben. Zum jetzigen Zeitpunkt sind mir noch keine bekannt. Es ist aber von gewissen Vorgaben auszugehen, da die Schulleitung weisungsbefugt ist gilt sie auch in diesen Fällen als Verantwortliche(r).

7.3. E-Learning-Tools im Unterricht

Es gibt unzählige Tools im Internet die sich für den Unterricht eignen. Bekannte Beispiele wären Learningapps.org und KAHOOT.it. Wenn man als Lehrperson eines dieser Angebote nutzen möchte gibt es ein paar Punkte zu berücksichtigen.

7.3.1. Lernplattformen

Lernplattformen sind Content Management Systeme (CMS) die der Bereitstellung von Lerninhalten und der Organisation von Lernvorgängen dienen. Im E-Learning und Blended Learning sind Lernplattformen von großem Nutzen um z.B. Aufgaben zur Verfügung zu stellen, Abgaben zu ermöglichen, Bewertungen durchzuführen und zu erhalten und anderes. (Schulmeister, 2005, S.11–19)

Mit dem Datenschutz halten es die verschiedenen Lernplattformen recht unterschiedlich. Die Vielfalt der unterschiedlichen Systeme und wie man ihre datenschutzrechtliche Eignung einteilen kann sei an drei Beispielen erläutert.

Moodle

Moodle ist eine OpenSource Software also ein gemeinschaftlich weiterentwickeltes, frei verwendbares Produkt, dessen Quellcode einsehbar und veränderbar ist. Es ist es immer zu begrüßen wenn OpenSource-Systeme im öffentlichen Bereich genutzt werden statt Steuergeld in proprietäre Systeme zu stecken. Moodle kann in der vom Bund zur Verfügung gestellten Version genutzt werden oder selbst auf einem Server betrieben werden.

Edmodo

Edmodo ist ein soziales Lernnetzwerk für Lehrerinnen und Lehrer, Schülerinnen und Schüler und Eltern. Es wurde 2008 in Kalifornien (USA) entwickelt und ist vor allem optisch an Facebook angelegt. Aufgrund des schlechten Datenschutzniveaus in den USA soll diese Plattform aber nur noch mit Pseudonym genutzt werden. Sensible Daten wie Leistungsbeurteilungen von österreichischen Schülerinnen und Schülern haben dort nichts verloren. (Menzel, 2017)

Eigene Anwendungen

Wenn eigene Anwendungen von Lehrkräften oder Schulen entwickelt werden sind diese auch für die DSGVO konforme Umsetzung verantwortlich. Konkret ist die Schulleiterin bzw. der Schulleiter verantwortlich. Diese sollen sich von den IT-Kustoden und Kustodinnen beraten lassen und können sich bei der oder dem Daten-

schutzverantwortlichen im Landesschulrat informieren. Die gesetzlichen Rahmenbedingungen müssen eingehalten werden und die technische Umsetzung sich nach diesen richten. (Menzel, 2017)

Im Folgenden werden an dem Beispiel einer Lernplattform für den Informatikunterricht einige Punkte erläutert:

- Serverstandort

Der Serverstandort sollte sich in der EU befinden um dem europäischen Datenschutz zu entsprechen.

- sensible Daten

Werden zum Beispiel Benotungen über die Plattform gegeben sind das zusätzliche sensible Daten die anfallen.

- Kennwörter und Kennwortübermittlung

Die Kennwörter sollten eine ausreichende Komplexität aufweisen und den Schülerinnen und Schülern auf sicherem Weg übermittelt werden (z.B. persönlich oder über verschlüsselte Messenger)

- HTTPS

Es sollte HTPS statt HTTP genutzt werden, da so alle Daten mit dem Server nur verschlüsselt abgerufen und ausgetauscht werden.

- Anwendungsverzeichnis

Das Führen eines Anwendungsverzeichnisses ist eine der Anforderungen die sich aus der EU-DSGVO ergeben. Dieses muss beinhalten

    - Namen und Kontaktdaten des bzw. der Verantwortlichen, des Vertreters bzw. der Vertreterin sowie eines oder einer etwaigen Datenschutzbeauftragten,
    - die Rechtsgrundlage für die Datenverarbeitung (z.B. eine eingeholte Einwilligung),
    - Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,

- den Zweck der Verarbeitung,
- Beschreibung der Verarbeitung,
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
- allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

7.3.2. Pseudonymisierung

Wenn eine Nutzung des Dienstes mit der Anmeldung der Schülerinnen und Schüler einhergeht gibt es die Möglichkeit Pseudonyme zu nutzen.

Je aussagekräftiger die Datenansammlung ist (z. B. Einkommen, Krankheitsgeschichte, Wohnort, Größe), desto größer ist die theoretische Möglichkeit, diese auch ohne Klarnamen einer bestimmten Person zuzuordnen und diese identifizieren zu können. Da bei vielen Diensten nur Anmeldedaten und die Daten die während der Nutzung entstehen (Punktestand, Ergebnisse bei Spielen, Tests etc.) gespeichert werden, stellt die Nutzung von Pseudonymen eine geeignete Technik dar, um diese Tools schnell und einfach datenschutzfreundlich zu nutzen. (Feiler, Horn, 2017, S. 194)

Wichtig ist, dass alle zur Identifikation geeigneten Daten pseudonymisiert werden, also wird z.B. als Nickname nicht der reale Name verwendet und die E-Mailadresse darf den Namen der Schülerin oder des Schülers nicht enthalten und sollte nur für diese und ähnliche Zwecke genutzt werden.

7.3.3. Appberechtigungen

Auch für Smartphones gibt es immer mehr Anwendungen die für den Unterricht interessant sind. Da es wünschenswert ist, dass Smartphones sinnvoll in den Unterricht integriert werden, sollten Lehrkräfte wissen wie sie diese hinsichtlich ihrer datenschutzrechtliche Dimension einschätzen.

Wenn Anwendungen auf dem Smartphone installiert werden, verlangen diese Zugriff auf bestimmte Funktionen und Bereiche, sogenannte Berechtigungen. Berechtigungen geben an, auf welche Funktionen oder Daten diese App zugreifen darf. So

können Anwender einer App zum Beispiel erlauben, auf die Liste seiner Kontakte oder auf die Informationen zu seinem Standort zuzugreifen.

Je, nach Funktionsumfang der Anwendung sind unterschiedliche Berechtigungen notwendig. Es gibt viele Apps die keine oder kaum Berechtigungen verlangen aber auch viele die umfangreichen Zugriff verlangen. Das ergibt sich aus der Intention der Entwicklerinnen und Entwickler die von OpenSource-Projekten bis zu Geschäftsmodellen reichen die das Sammeln von großen Mengen an Daten beinhalten.

Die Berechtigungen können nach der Installation der App geändert werden. Da dies auf älteren Androidgeräten nicht möglich ist und die Anleitung zu den benötigten Einstellungen nicht jede Lehrkraft für alle in einer Klasse vorhandenen Geräte geben kann, sollten nur Anwendungen benutzt werden die von vornherein keine unzulässigen Daten sammeln. (Datenschutzbeauftragter-Info, 2017)

Am Beispiel der Taschenlampen-Apps zeigt sich gut wie viele dieser Apps übermäßige Berechtigungen einholen um Zugriff auf möglichst viele Daten zu haben. Ganz abgesehen davon, dass die meisten Smartphones eine Taschenlampenfunktion haben und dafür keine eigene App notwendig ist, gibt es auch Apps die nur die für den Funktionsumfang notwendigen Berechtigungen einholen. Gerade im LearningApp-Bereich gibt es viele Apps die nur notwendige Zugriffe benötigen. (Holtkemper, 2018)

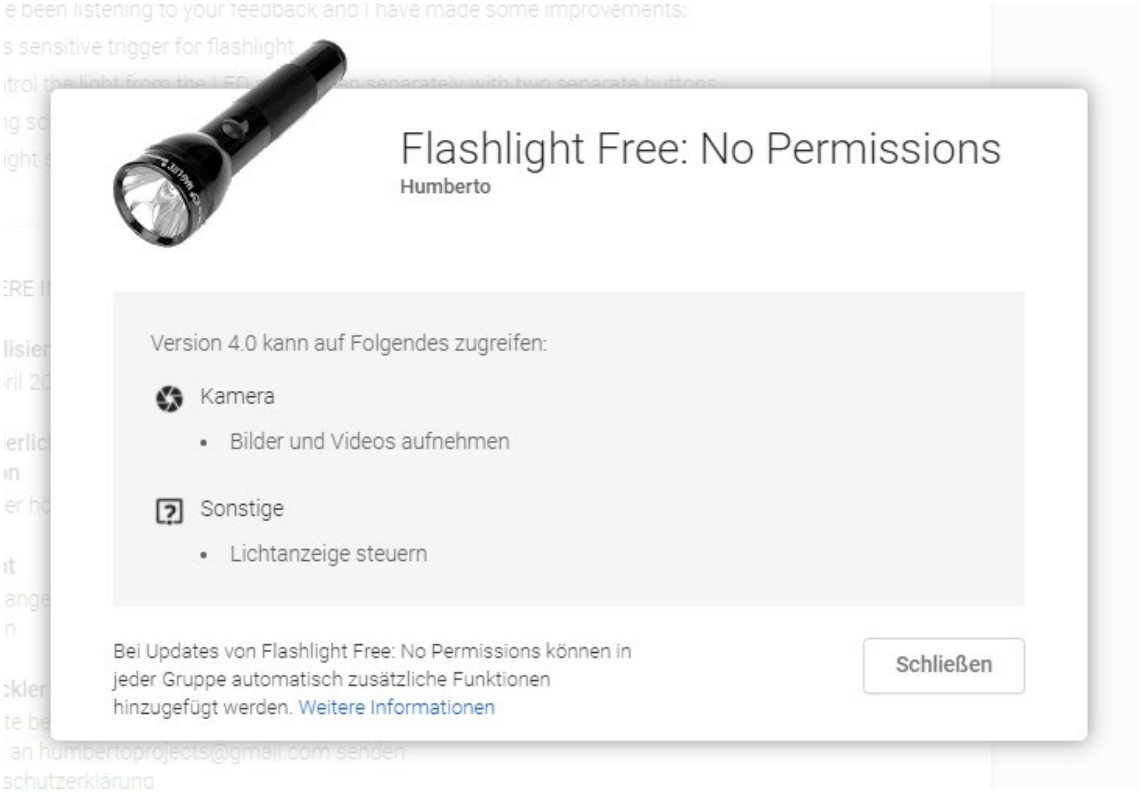


Abbildung 2: Beispiel für eine App mit vernünftigen Appberechtigungen

Wenn die Geräte auf denen die Schülerinnen und Schüler arbeiten, zum Beispiel Pads, die der Schule gehören, können auch so genannte Managed Devices eingesetzt werden um die gegebenen Berechtigungen zu limitieren bzw. nur vorher geprüfte Apps zur Installation zu zulassen. Hierbei behält der Administrator der Schule die Kontrolle über die Geräte. (Mobile-Managed-Device, 2016)

7.4. Kommunikation über Messenger

Das Kommunizieren über Messenger ist heute weiter verbreitet als Telefonieren und SMS. Vor allem bei Jugendlichen ist diese Form mit Abstand am beliebtesten. (derstandard, 2017)

Da bietet es sich doch geradezu an Messenger auch für den Unterricht oder die Kommunikation innerhalb der Klasse zu nutzen. Aber nicht jeder Messenger ist als datenschutzrechtlich unbedenklich einzustufen und somit ohne weiteres geeignet.

7.4.1. WhatsApp und Facebook Messenger

WhatsApp und der Facebook-Messenger, genau wie Facebook selbst, sind aus datenschutzrechtlicher Sicht zu problematisch für den Einsatz im Unterricht. Diese

Sicht ist neben Datenschützern auch offizieller Standpunkt des Bildungsministeriums (Menzel, 2017)

Rechtlich gedeckt ist durch die ab Mai 2018 geltende Datenschutzgrundverordnung maximal die rein private Nutzung von WhatsApp. Laut Art 2 Abs 2 der EU-DSGVO findet das Datenschutzgesetz keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Das trifft zu wenn man WhatsApp auf einem Smartphone installiert, dass ausschließlich für private Zwecke genutzt wird. (Pollirer et al., 2017, S.7)

WhatsApp ist seit 2014 Teil von Facebook Inc., deren Geschäftsmodell es ist, die Daten der Nutzer zu kommerziellen Zwecken zu sammeln und weiterzuverwenden. (Handelsblatt, 2014)

Der bekannte österreichische Jurist und Datenschutzaktivist Max Schrems hat im Zusammenhang mit Facebook und dem Zugriff des amerikanischen Geheimdienstes NSA auf die Daten das Safe-Harbor-Abkommen vor dem europäischen Gerichtshof 2015 zu Fall gebracht. Dieses Abkommen hatte ermöglicht, dass die USA als sicherer Hafen für die Daten von EU-Bürgern galten da ein ähnliches Datenschutzniveau existieren würde und ohne weitere Regelungen in die Vereinigten Staaten transferiert werden konnten. Das Nachfolgeabkommen EU-US Privacy Shield, das seit 1. August 2016 gültig ist, bringt leider keine wesentliche Verbesserung, da sich inhaltlich zum vorherigen Abkommen nicht viel im Text geändert hat. (Lebert, 2017)

Facebook sammelt alle Daten und Interaktionen mit der Plattform und hält über Tracking-Cookies das Verhalten seiner Nutzer im Internet auch auf anderen Webseiten immer lückenloser fest.

Die Messenger haben mittlerweile zwar Verschlüsselung implementiert, d.h. die Inhalte der Nachrichten werden nicht mehr im Klartext übermittelt, Facebook analysiert allerdings alle Metadaten die in der Kommunikation anfallen. Also wer mit wem, wann und wie oft kommuniziert. Auch mit Metadaten alleine lassen sich sehr aussagekräftige Profile von Usern erstellen.

Zudem muss man um WhatsApp nutzen zu können, seine gesamten gespeicherten Kontakte Facebook zugänglich machen. Die App fordert außerdem Zugriff auf den Geräte- und App-Verlauf, die Identität des Handybesitzers, seine Kontakte, seinen Standort, seine SMS, Fotos, Medien und -andere Dateien; auf seine Kamera und sein Mikrofon, seine WLAN-Verbindungsinfos und seine Geräte-ID sowie die Anrufinformationen. Deshalb wäre es absolut fahrlässig von einer Lehrperson WhatsApp zur Kommunikation mit Schülerinnen und Schülern einzufordern. (Datenschutz: WhatsApp, 2015)

Als Beispiel für eine gerade noch akzeptable WhatsApp-Nutzung nennt der Datenschutzverantwortliche des Bildungsministeriums MinRat Mag. Thomas Menzel: „Ich kenne das so: Wenn WhatsApp-Gruppen für den Unterricht genutzt werden, dann nicht weil der Lehrer sagt ihr müsst WhatsApp nutzen sondern, dass die Klasse selbst schon eine WhatsApp-Gruppe hat und der Lehrer gefragt wird ob er nicht beitreten wollte, könnte oder dürfte damit er da sinnvoll mitkommunizieren kann.“ (Menzel, 2017) Ich kann dem aber nur abraten, da die Lehrkraft hier die Vorbildfunktion zu wahren hat.

7.4.2. Alternativen

Es gibt viele brauchbare Alternativen zu den Messengern von Facebook, wie Signal, Wire, Mattermost, Threema und andere. Bei diesen ist man nicht nur rechtlich auf der sicheren Seite, es ist im Besonderen pädagogisch wertvoll den Schülerinnen und Schülern Alternativen nahezubringen und anhand derer die Unterschiede aufzuzeigen und bewusst zu machen. Das bringt einen Mehrwert im technischen Verständnis, in der kritischen Auseinandersetzung des eigenen Konsumverhaltes, der gesellschaftlichen Bedeutung von Technologien, Überwachung und letztlich zur Bildung zu mündigen Bürgerinnen und Bürgern. (Floemer, 2017)

Zwei Beispiele für Android und iOS, an Hand derer die rechtlichen und vor allem technischen Unterschiede sowie die Vielfalt deutlich werden, werden in Folge vorgestellt:

WebUntis App

WebUntis gibt es als SmartphoneApp und Webanwendung und wird vom BMBWF zur Verfügung gestellt. Die Lehrkraft kann dort Hausübungen, den Teststoff und Anderes kommunizieren. Hier steht der Server in Österreich und ist vom BMBWF beauftragt. (Menzel, 2017)

Signal-Messenger

Der Signal-Messenger ist ein Open-Source-Projekt von Open-Whisper-Systems d.h. er ist kostenlos und der Quellcode ist einsehbar. Dadurch kann die Sicherheit von unabhängiger Stelle aus kontrolliert werden und es steckt kein kommerzielles Interesse dahinter. Er bietet verschlüsselte Textnachrichten und Sprachanrufe. Für die Ende-zu-Ende-Verschlüsselung von Nachrichten kommt das freie Signal-Protokoll zum Einsatz. Zusätzlich kann Signal die Nachrichtendatenbank am Gerät verschlüsseln, sodass Nachrichten erst nach einer Kennworteingabe gelesen werden können. (Scherschel, 2017)

Wire – Secure Messenger

Wire ermöglicht Textnachrichten, Telefonanrufe von bis zu fünf Personen in Stereo-Qualität und Videoanrufe. Mit Wire können Nutzer animierte GIF-Dateien direkt in der App verschicken. Außerdem ist es möglich, YouTube-, Soundcloud-, Spotify- und Vimeo-Inhalte direkt in der App mit seinen Kontakten zu teilen. Hinter dem Wire Messenger steht die Firma Wire Swiss GmbH mit Sitz in der Schweiz. Genutzt werden nach Angaben des Unternehmens in der EU befindliche Server womit der rechtliche Schutz durch die EU-DSGVO gegeben ist. Der Quellcode der App und schrittweise auch des Servers sind öffentlich zugänglich. Für die Nutzung von Wire kann man ein Pseudonym benutzen um somit auch keine brauchbaren Metadaten mehr zu erzeugen. (Hurtz, 2017))

Microsoft Teams

Mit den Schulaccounts der LehrerInnen und SchülerInnen lässt sich aus Microsoft Teams nutzen. Dieses Programm bietet mehr Funktionen neben einem Chatprogramm auch Funktionen zum kollaborativen Arbeiten. Gruppen können mit LehrerInnen-Accounts erstellt werden. Die Software ist als Webanwendung im Browser, als Desktopprogramm und als Andoid und iOS App verfügbar.

SchoolFox

Ist ein elektronisches Mitteilungsheft von einer österreichischen Firma. Diese Lösung ist allerdings kostenpflichtig und auf die Kommunikation von LehrerInnen und Eltern zugeschnitten.

7.5. Kameraüberwachung in der Schule

Videoüberwachung wird an vielen österreichischen Schulen zumindest immer wieder angedacht um Problemen wie wiederholtem Diebstahl oder Eindringen von schulfremden Personen zu begegnen. Sie sollte aber nur angewandt werden wenn kein geeignetes anderes Mittel zur Verfügung steht.

Gegen Videoüberwachung sprechen die gleichen Gründe wie an anderen öffentlichen Orten, sie hilft meist nur bei der Aufklärung - zur Abschreckung von Straftaten ist sie meist nicht sehr erfolgreich und es findet eine Verdrängung von Straftaten in nicht überwachte Bereiche statt.

Zusätzlich zu dieser vorsichtigen Herangehensweise gibt es Bereiche die von der Videoüberwachung gänzlich ausgenommen sein müssen, das sind Umkleidebereiche, Toiletten, Klassen und Lehrsäle.

Zum Thema Videoüberwachung in Lehrsälen gibt es ein aktuelles Urteil des europäischen Gerichtshofs für Menschenrechte (EGMR) vom November 2017. Geklagt hatten zwei Professoren der Universität von Montenegro, gegen die Videoüberwachung der Lehrsäle in denen sie unterrichten. Diese wurde eingerichtet um die Lehrtätigkeit zu überwachen und Menschen und Eigentum zu schützen. Der EGMR hat schon in früheren Urteilen festgestellt, dass auch berufliche Aktivitäten vor totaler Videoüberwachung durch Artikel 8 der europäischen Menschenrechte, dem Recht auf Achtung des Privat- und Familienlebens, geschützt sein können, und fand keinen Grund diesen Fall davon auszunehmen. Da die Professorinnen und Professoren in den überwachten Lehrsälen nicht nur Unterricht halten, sondern mit Studenten interagieren, Beziehungen und ihre soziale Identität entwickeln hat der EGMR das Verbot von Videoüberwachung in den Lehrsälen bestätigt. (Judgment Antovic and Mirkovic v. Montenegro - camera surveillance of lecture halls, 2017)

7.6. Themen für den Unterricht

Datenschutz ist immer mehr ein Thema für den Unterricht. Neben Anwenderwissen für Computer und Internetnutzer und dem Kennen der eigenen Rechte und Pflichten geht es hier aber auch darum die Bedeutung des Datenschutz als Grundrecht ohne das eine Demokratie nicht funktionieren kann zu vermitteln. Es bietet es sich hier an auf aktuelle Entwicklungen einzugehen, Themen gibt es genug: der Einfluss von BigData auf demokratische Wahlen, Datenlecks und ihre Folgen, staatliche Überwachung bzw. das Verhältnis von Staat und Bürger.

Zum Schluss gebe ich zu bedenken, dass ein guter Datenschutz LehrerInnen genauso wie allen BürgerInnen zu Gute kommt und unsere demokratischen Grundrechte schützt. Das ist ein Grund zur Freude und sollte auch so vermittelt werden.

7.6.1. Soziale Medien

Facebook und WhatsApp. sind aus datenschutzrechtlicher Sicht, wie weiter oben schon ausgeführt, für die Nutzung in der Schule ungeeignet. Der Umgang mit sozialen Medien, deren Bedeutung für und die Auswirkungen auf die Gesellschaft und den Einzelnen sollten dennoch Thema im Unterricht sein. Das beinhaltet Unterthemen wie:

- Cybermobbing

Als Cyber-Mobbing werden verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen mit Hilfe elektronischer Kommunikationsmittel über das Internet, in Chatrooms, beim Instant Messaging und/oder auch mittels Mobiltelefonen bezeichnet. Dazu gehört auch der Diebstahl von (virtuellen) Identitäten, um in fremdem Namen Beleidigungen auszustoßen oder Geschäfte zu tätigen. Opfer werden durch Bloßstellung im Internet, permanente Belästigung oder durch Verbreitung falscher Behauptungen gemobbt. (help.gv.at, 2018)

- Sexting

Sexting ist die private Kommunikation über sexuelle Themen per Mobile Messaging. Im engeren Sinn handelt es sich um „Dirty Talk“ zur gegenseitigen Erregung. Seit

Verfügbarkeit der Multimedia Messaging Services (MMS) und Instant-Messagern wie WhatsApp, kann damit auch der Versand von erotischem Bildmaterial des eigenen Körpers über Instant-Messaging-Anwendungen durch mobile Endgeräte verbunden sein. Das aus dem anglo-amerikanischen Sprachraum stammende Kofferwort setzt sich aus Sex und texting (engl. „simsen, SMS schreiben“) zusammen. Im Deutschen wird das Wort hauptsächlich für das Versenden von erotischen Selbstaufnahmen per Smartphone oder Internet verwendet. (saferinternet.at, 2018)

Dabei sind Probleme wie ungewollte Veröffentlichung und strafrechtliche Folgen bei unerlaubter Weitergabe Thema, genauso wie ein vernünftiger Umgang mit Vertrauen. (SCHAU HIN!, 2015)

- Urheberrecht

Das österreichische Urheberrecht schützt das geistige Eigentum der Urheber im weiteren Sinn. Als zentrales Gesetz enthält das Urheberrechtsgesetz die erlassenen gesetzlichen Bestimmungen. (RIS, 2015)

Durch die technischen Veränderungen durch das Internet gilt das Urheberrecht als teilweise überholt und wird auch auf europäischer Ebene früher oder später wieder behandelt werden. Projekte wie die Creative Commons, die ein System für eine leichtere Weitergabe unter unterschiedlichen Bedingungen ermöglichen, sind zu thematisieren. (Share Your Work, 2018)

- Recht am eigene Bild

Das Recht am eigenen Bild in Österreich, hier auch speziell Bildnisschutz genannt, ist im § 78 des Urheberrechtsgesetzes (UrhG) geregelt. Gemeint ist damit, dass jeder und jede Mitspracherecht, hat was mit dem eigenen Bild im öffentlichen Raum passiert. (RIS, 2015)

- Fake News

Als Fake News (auch Fake-News oder Fakenews) werden manipulativ verbreitete, vorgetäuschte Nachrichten oder Falschmeldungen bezeichnet, die sich überwiegend im Internet, insbesondere in sozialen Netzwerken zum Teil viral verbreiten, und mitunter auch von Journalisten aufgegriffen werden. Die Quellenbewertung

wird für Schülerinnen und Schüler immer schwieriger, aber auch immer wichtiger. (Brodnig2018)

- Hatespeech/Hassrede

Das Thema Hatespeech und Wut im Internet und deren Auswirkungen sind ein weiteres Themenfeld. Hatespeech, also Hassrede, bezeichnet sprachliche Ausdrucksweisen von Hass mit dem Ziel der Herabsetzung und Verunglimpfung bestimmter Personen oder Personengruppen. (Brodnig, 2016)

- Werbung und Marketing in sozialen Netzwerken

Die sozialen Medien sind von Werbetreibenden als Kanäle etabliert. Schülerinnen und Schüler sollen einerseits Wissen wie soziale Medien als Werbekanäle und zur Kundenkommunikation genutzt werden, um diese in ihrem beruflichen Leben nutzen zu können. Andererseits, um sich als Konsumentinnen und Konsumenten und Bürgerinnen und Bürger einer demokratischen Gesellschaft der Mechanismen moderner Medien bewusst zu sein.

7.6.2. Privatwirtschaftliche Überwachung - Überwachungskapitalismus

Die meisten Schülerinnen und Schüler wissen heutzutage, dass das Durchforsten des Internets keine Privatangelegenheit ist und jeder Besuch, jede Recherche und jeder Kauf eines Produkts auf einer Website von mehr als nur einem Unternehmen mitverfolgt wird.

Es ist aber essenziell für sie zu wissen was passiert wenn private Daten im Netz gesammelt und miteinander verknüpft werden um die Tragweite für ihr Leben und die gesellschaftlichen Auswirkungen zu begreifen und darauf Einfluss nehmen zu können.

Alle betroffenen und Großteiles neuen Problembereiche hier darzustellen würde den Rahmen sprengen. Der Wiener Netzaktivist, Autor und Datenanalyst Wolfie Christl beschreibt die gängigen Praktiken eingehend in seiner Studie „Corporate Surveillance in Everyday Life“. Die Studie findet international viel Beachtung und wird auch von der British intelligence agency GCHQ verwendet. (Christl, 2017)

Personalisierte Werbung wird von vielen als „praktisch“ oder „nervig“, wenn sie daneben liegt manchmal als „dumm“ angesehen.

Dabei kann es sein, dass man aufgrund der Hinterlassung bestimmter Datenspuren, die man bei oder vor einem Kauf bei dem man „zu viel“ bezahlt hat, ohne sein Wissen in die digitale Schublade eines „zahlungskräftigen Konsumenten“ gesteckt wird. Wenn wir im Internet etwas kaufen, rechnen im Hintergrund Algorithmen etwa aus, ob wir einen PC oder Mac benutzen, aus welchem Land wir kommen und vieles mehr. Anhand unserer digitalen Profile können dann Preise unterschiedlich berechnet werden.

Zu Diskriminierung bei Werbeanzeigen kommt es zum Beispiel, wenn jemand gerade auf Jobsuche ist und aufgrund seines Alters oder Geschlechts gewisse Anzeigen gar nicht erst angezeigt bekommt. „ProPublica“ hat in einer Untersuchung herausgefunden, dass beispielsweise Verizon Jobanzeigen nur für eine bestimmte Altersgruppe und einen bestimmten Wohnort freigeschalten hatte. In diesem Fall haben nur Facebook-Nutzer zwischen 25 und 36 Jahren, die sich für Finanzen interessieren

und in Washington leben oder die Stadt in letzter Zeit besucht haben, haben ein bestimmtes Jobinserat zu Gesicht bekommen. (Angwin, Scheiber, Tobin, 2017)

Gezielte Werbung bietet Vorteile für Werbetreibende und führt zu einer zunehmenden Fragmentierung der Gesellschaft, zum Verstärken von sozialen Ungleichheiten und Vorurteilen. Heikel wird es, wenn man plötzlich keinen Kredit bekommt, weil man im falschen Viertel wohnt, auf Facebook mit den falschen Menschen befreundet ist oder ein Antrag abgelehnt wird, weil mitprotokolliert wurde, was man online sonst noch so gemacht hat. Das Hamburger Unternehmen Kreditech greift bei der Berechnung der Kreditwürdigkeit etwa auf umfangreiche Daten über Onlineverhalten zurück.

Wolfie Christl im Gespräch mit Barbara Wimmer für einen Futurezone-Artikel:

„Derartige Entwicklungen lassen sich auch unter dem Schlagwort „ Überwachungskapitalismus“ zusammenfassen. Die größten Datensammler sind dabei ganz klar die Online-Portale Facebook und Google, die wegen ihrer Praktiken immer wieder in Verruf geraten sind. Aber auch Wirtschaftsauskunfteien wie Experian, Equifax sowie klassische Datenhändler wie Oracle oder Acxiom haben digitale Profile von Milliarden von Internet-Nutzern. „Man muss hier vor allem mitbedenken, auf welcher Skalierung sich das abspielt. Durch diese Größenordnungen ergeben sich ganz massive Risiken für Privatsphäre, Freiheit und Demokratie“, sagt Christl.

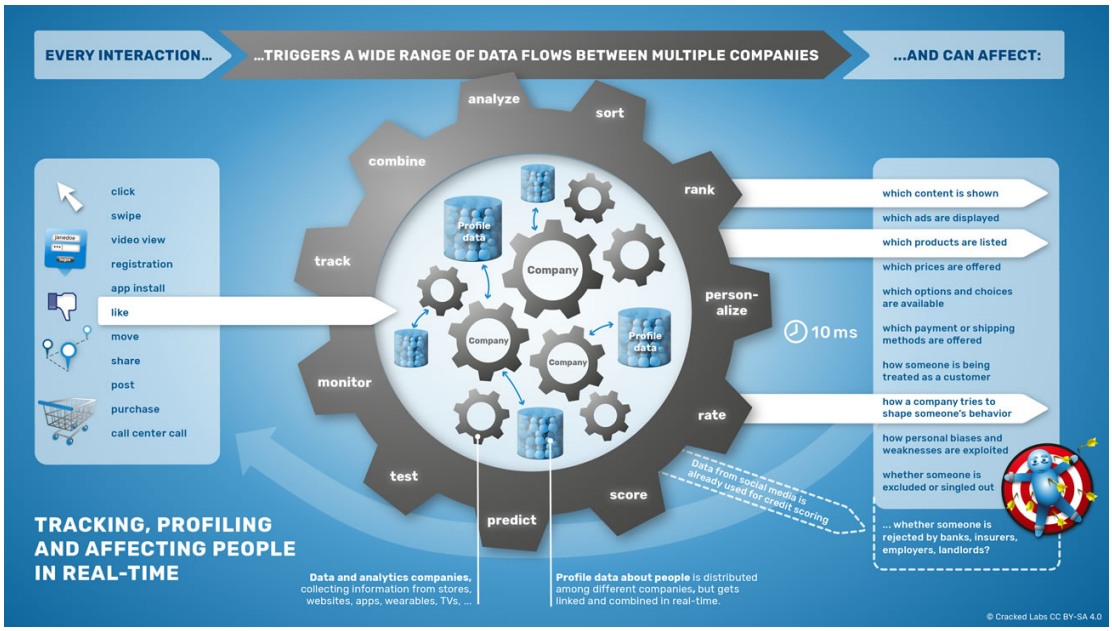


Abbildung 3: Wie sich jede erfasste Tätigkeit auswirkt. (Cracked Labs CC-BY-SA 4.0)

Die Daten werden nämlich häufig miteinander verknüpft, weil sie von den einzelnen Unternehmen zugekauft und in die eigene Datenbank integriert werden. Am Ende weiß man als Nutzer gar nicht mehr, wer eigentlich was über einen weiß und welche Algorithmen über einen anhand von welcher Daten Entscheidungen für einen treffen.

„Wir müssen dieses System des exzessiven Datensammelns über Einzelne durchbrechen. Die Schnittstellen, an denen Daten miteinander verknüpft werden, sind dabei wesentlich. Durch die Verknüpfung von Datenbanken unterschiedlicher Firmen steigen die Risiken enorm“, warnt Christl. Online-Tracking, wie es derzeit gemacht wird, kennt nämlich kaum noch Grenzen.

„Man kann sich das Machtungleichgewicht zwischen Daten sammelnden Firmen und Einzelpersonen vorstellen wie beim Pokerspiel. Die eine Seite hat die Karten verdeckt, die andere muss mit offenen Karten spielen. Es wird immer die Seite verlieren, deren Karten aufgedeckt liegen. Wie beim Pokern können Firmen das gesammelte Wissen gegen uns verwenden. Sie können die Handlungen von Internet-Nutzern besser beeinflussen, manipulieren, sie austricksen oder einfach das meiste aus ihnen herausholen“, sagt Christl im Gespräch mit der futurezone.

„Wenn wir aktuell irgendeine bekanntere Website besuchen, dann hat die im Schnitt 30 bis 40 Tracker von Drittparteien eingebaut, die über jeden Klick von uns informiert werden. Firmen behaupten oft, diese Daten wären anonym, nutzen aber meist eindeutige Identifikationscodes, mit denen man die gleiche Person über Lebensbereiche hinweg verfolgen und die Daten immer wieder zuordnen kann. Man braucht nicht immer einen Namen, um Menschen zu identifizieren“, erklärt Christl. „Und oft wissen die Firmen dabei gar nicht, dass sie Daten auch mit Mitbewerbern teilen“, so der Datenanalyst. (Wimmer, 2018)

7.6.1. Staatliche Überwachung

Die Technik schafft auch neue Möglichkeiten von Überwachung. Diese Möglichkeiten werden nicht nur von autoritären Regimen genutzt, auch westliche Demokratien haben Begehrlichkeiten Überwachungstechnik im großen Rahmen einzusetzen.

„Wir müssen erst den richtigen Mittelweg finden zwischen neuen technischen Überwachungsmöglichkeiten und den Grund- und Freiheitsrechten“, meint dazu Otmar Lendl vom österreichischen Computer Emergency Response Team (CERT). (Radio Dispositiv, 2018)

China startet gerade das größte Volkserziehungsprogramm der Welt, ein umfassendes Bürgerbewertungssystem, das „Social Credit System“. Dort gibt der Staat seinen Bürgerinnen und Bürgern Noten. Wer zum Beispiel über das Internet gesunde Babynahrung bestellt oder seine Eltern öfter besucht erhält Pluspunkte. Wer hingegen bei Rot über die Straße geht, sich online pornografisches Material ansieht oder zu viel Zeit mit Computerspielen verbringt, muss mit Abzügen rechnen. Bürger die einen hohen Score erreichen, sollen z.B. vergünstigte Kredite erhalten oder eine bessere Krankenversicherung. Bei einem schlechten Ergebnis ist mit Sanktionen zu rechnen. Das System ist mit künstlicher Intelligenz ausgestattet und lernfähig. Gesichtserkennung und Bewegungsprofile runden die lückenlose Überwachung ab. (Lee, 2018)

Während moderne Gesellschaften eine bisher nicht gekannte Heterogenität und Komplexität in kultureller und sozialer Hinsicht herausgebildet haben, basiert die Idee der staatlich vermittelten Ordnung auf der Annahme, dass einfache Klassifikationssysteme ausreichen, um solche Gesellschaften zu regieren. Gerade in westlichen Demokratien wird Terrorismus derzeit als eine der zentralen Bedrohungen unserer Gesellschaft verstanden und dient als Begründung für den Ausbau unterschiedlichster Überwachungsmaßnahmen. Andererseits ist die tatsächliche Wahrscheinlichkeit einem terroristischen Anschlag zum Opfer zu fallen extrem unwahrscheinlich. Auch das subjektive Sicherheitsgefühl, so es denn betroffen ist, ist hier irreführend. Es verblassen die Opferzahlen sowohl der Angriffe auf die New Yorker Twin Towers, als auch alle anderen prominenten Attacken im Vergleich zu den Todesfällen, die durch Verkehrsunfälle, medizinische Kunstfehler oder ungesunde Ernährung verursacht werden. Die eigentliche Wirksamkeit terroristischer Anschläge bemisst sich nicht an der Zahl der Opfer, sondern an der Wirkung auf die Wahrnehmung der Bürgerinnen und Bürger. Der Einfluss von Terror auf die Gesellschaft ist

auf die politische Diskussion und die Reaktion der staatlichen Behörden am größten. (Tschohl, C., Scheucher, E., Kargl, D., Luksan, J., Czadilek, A., Waloschek, H., Kreissl, R., Klinger, K., Hötzendorfer, W., Möchel, E., 2017)

8. Literaturverzeichnis

Angwin, J., Scheiber, N., Tobin, A. (2017). Dozens of Companies Are Using Facebook to Exclude Older Workers From Job Ads. ProPublica, 20.12.2017. Verfügbar unter: https://www.propublica.org/article/facebook-ads-age-discrimination-targeting [20.02.2018]

Anonymisierung und Pseudonymisierung (2017).Wikipedia, 13.09.2017. Verfügbar unter: https://de.wikipedia.org/w/index.php?title=Anonymisierung_und_Pseudonymisierung&oldid=169039302 [06.12.2017]

BilDokG (2018). Bildungsdokumentationsgesetz. Verfügbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20001727 [13.04.2018]

bildung.bmbwf.gv.at (2018). Digitale Grundbildung Verfügbar unter: https://bildung.bmbwf.gv.at/schulen/schule40/dgb/index.html [23.04.2018]

Beutenmüller, F., Greinert, F. (2018). checkdeinpasswort.de (2011). Verfügbar unter: https://checkdeinpasswort.de/ [23.04.2018]

Brodnig, I. (2018). Ist das Fake News? Infografik. Verfügbar unter: https://www.brodnig.org/2018/03/10/ist-das-fake-news-infografik/ [23.04.2018]

Brodnig, I. (2016). Das Internet ist kein egalitärer Raum – mein Vortrag vom Netzpolitischen Abend.Verfügbar unter: https://www.brodnig.org/2016/01/18/das-netz-ist-kein-egalitarer-raum-mein-vortrag-vom-netzpolitischen-abend/ [23.04.2018]

Christl, W.(2017). Corporate Surveillance in Everyday Life. Verfügbar unter: http://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf [20.02.2018]

Datenschutzbeauftragter-Info.de (2014). Begriff und Geschichte des Datenschutzes. Datenschutzbeauftragter_Info.de, 28.05.2014. Verfügbar unter: https://www.datenschutzbeauftragter-info.de/begriff-und-geschichte-des-datenschutzes/ [24.04.2018]

Datenschutzbeauftragter-Info.de (2017). Smartphone-App Berechtigungen – Erforderlich oder ein Ärgernis?. Datenschutzbeauftragter_Info.de, 14.11.2017. Verfügbar

unter: https://www.datenschutzbeauftragter-info.de/smartphone-app-berechtigungen-erforderlich-oder-ein-aergernis/ [19.04.2018]

Datenschutz: WhatsApp (2015). Konsument, 26.03.2015. Verfügbar unter: https://www.konsument.at/geld-recht/datenschutz-whatsapp [13.02.2018]

derstandard (2017). Junge texten lieber mit WhatsApp statt zu telefonieren. DerStandard, 31.10.2017. Verfügbar unter: https://derstandard.at/2000066980196/Junge-texten-lieber-mit-WhatsApp-statt-zu-telefonieren [13.02.2018]

derstandard (2018). Österreichische Datenschützerin wird Chefin der neuen EU-Datenschutzbehörde (2018). derstandard.at, 07.02.2018. Verfügbar unter: derstandard.at/2000073812006/Oesterreichische-Datenschuetzerin-wird-Chefin-der-neuen-EU-Datenschutzbehoerde [15.04.2018]

DSAG-Bildung (2018). Datenschutz-Anpassungsgesetz Bildung. Verfügbar unter: https://www.parlament.gv.at/PAKT/VHG/XXVI/ME/ME_00008/index.shtml#tab-Uebersicht [13.04.2018]

edps.europa.eu (2018). Entwicklungsgeschichte der Datenschutz-Grundverordnung. Verfügbar unter: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_de [20.04.2018]

E-Estonia (2018). education. Verfügbar unter: https://e-estonia.com/solutions/education/ [20.04.2018]

epicenter.works (2017). Regierungsprogramm 2017-2022 (Farbcodiert). epicenter.works, 17.12.2017. Verfügbar unter: https://epicenter.works/document/823 [16.02.2018]

Feiler, L., Forgó, N. (2017). EU-DSGVO Kurzkommentar. Wien: Verlag Österreich GmbH

Feiler L., Horn B. (2018). Umsetzung der DSGVO in der Praxis. Wien: Verlag Österreich GmbH

Floemer, A. (2017). Whatsapp-Alternativen: Das können die Messenger von Telegram über Threema bis Wire. t3n, 11.10.2017. Verfügbar unter: https://t3n.de/news/whatsapp-alternativen-blick-430632/ [11.02.2018]

Genz, A. (2004). Datenschutz in Europa und den USA. Wiesbaden: Deutscher Universitäts-Verlag

Handelsblatt (2014). WhatsApp gehört jetzt zu Facebook. Handelsblatt, 06.10.2014. Verfügbar unter: http://www.handelsblatt.com/unternehmen/it-medien/kauf-abgeschlossen-whatsapp-gehoert-jetzt-zu-facebook/10800722.html [23.04.2018]

help.gv.at (2018). Was ist Cyber-Mobbing, Cyber-Bullying, Cyber-Stalking?. Verfügbar unter: https://www.help.gv.at/Portal.Node/hlpd/public/content/172/Seite.1720710.html [23.04.2018]

Holtkemper, L. (2018). App-Berechtigungen richtig vergeben: Das sollten Sie wissen, Connect,de, 23.01.2018. Verfügbar unter: http://www.connect.de/ratgeber/app-berechtigungen-android-smartphone-sinnvoll-datenschutz-3197625.html [16.02.2018]

Hurtz, S. (2017). Dieser Messenger ist privater als Whatsapp und kann mehr als Threema . sueddeutsche.de, 20.01.2017. Verfügbar unter: http://www.sueddeutsche.de/digital/whatsapp-alternative-wire-dieser-messenger-ist-privater-als-whatsapp-und-kann-mehr-als-threema-1.3150299 [23.04.2018]

Judgment Antovic and Mirkovic v. Montenegro - camera surveillance of lecture halls. (2017). European Court Of Human Rights, 28.11.2018. Verfügbar unter: http://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-5927767-7571421&filename=Judgment%20Antovic%20and%20Mirkovic%20v.%20Montenegro%20-%20camera%20surveillance%20of%20lecture%20halls.pdf [20.12.2017]

Kopeinigg, C. Landerer, C., Madritsch, R., Micheuz, P., Perger, P., Pichler, C., Wassnig, S. (2018). Office und Publishing 1 - HAS. Braunschweig: Westermann Druck

Lachmayer, K., Menzel, T. (2017). Datenschutz, IT-Sicherheit und Urheberrechte in der Schulverwaltung. Verfügbar unter: http://pubshop.bmb.gv.at/detail.aspx?id=648 [10.04.2018]

Lebert, Y. (2017). Schrems gegen Facebook: Eine gute und eine schlechte Nachricht, netzpolitik.org, 14.11.2017.Verfügbar unter: https://netzpolitik.org/2017/schrems-gegen-facebook-eine-gute-und-eine-schlechte-nachricht/ [23.04.2018]

Lee, F. (2018). Social Scoring in China - Im Reich der überwachten Schritte. taz, 10.02.2018. Verfügbar unter: http://www.taz.de/!5480926/ [23.04.2018]

Menzel, T. (2017). Experteninterview am 03.11.2017 im BMBWF, siehe Anhang

OpenPGP.org (2016). About – OpenPGP. openpgp.org, 15.08.2016. Verfügbar unter: https://www.openpgp.org/about/ [16.02.2018]

Parlamentskorrespondenz Nr. 442 (2018). Nationalrat: Umfassende Datenschutzanpassungen samt ELGA-Datenschutz-Entschließung für Registerforschung. 20.04.2018. Verfügbar unter: https://www.parlament.gv.at/PAKT/PR/JAHR_2018/PK0442/index.shtml [21.04.2018]

Pollirer, H.-J. & Weiss, E. & Knyrim, R. & Haidinger, V. (2017). DSGVO Datenschutz-Grundverordnung. Wien: MANZ'sche Verlags- und Universitätsbuchhandlung

Postlmayr, A. (2018). Geschichtliche Entwicklung der EMRK. Verfügbar unter: http://www.emrk.at/ [22.04.2018]

Radio Dispositiv (2018). Die Sache mit der Sicherheit – Otmar Lendl zu Fragen der IT-Security. [Radiointerview] Wien. Radio Orange 94.0, 31.03.2018. Verfügbar unter: https://cba.fro.at/371696 [23.04.2018]

RIS (2015). Urheberrechtsgesetz. Urh-Nov 2015 BGBl. I Nr. 99/2015 Verfügbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10001848 [19.04.2018]

RIS (2018). Verfügbar unter: Gesamte Rechtsvorschrift für Datenschutzgesetz 2000. 23.04.2018. Verfügbar unter: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 [23.04.2018]

saferinternet.at (2018). Datenschutz. Verfügbar unter: https://www.saferinternet.at/datenschutz [23.04.2018]

saferinternet.at (2018). Flyer Sexting. Verfügbar unter: https://www.saferinternet.at/uploads/tx_simaterials/Flyer_Sexting.pdf [23.04.2018]

SCHAU HIN! (2018). Nacktbilder aufs Handy – Phänomen Sexting. Schau hin, 31.08.2015. Verfügbar unter: https://www.schau-hin.info/news/artikel/nacktbilder-aufs-handy-phaenomen-sexting.html [14.02.2018]

Scherschel, F. (2017). Krypto-Messenger Signal schützt Kontaktdaten vor den Server-Betreibern, heise.de, 27.09.2017. Verfügbar unter: https://www.heise.de/security/meldung/Krypto-Messenger-Signal-schuetzt-Kontaktdaten-vor-den-Server-Betreibern-3844545.html [23.04.2018]

Schmidl, M. (2018). Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung Leitfaden. Verfügbar unter: https://www.dsb.gv.at/datenschutz-grundverordnung [14.04.2018]

Schrems, M. (2016). Die DSGVO als Produkt von Lobbyismus und Tauschhandel. In Knyrim, R. (Hrsg.), DSGVO (S.33-37). Wien: Manz'sche Verlags- und Universitätsbuchhandlung

Schulmeister, R. (2005). Zur Didaktik des Einsatzes von Lernplattformen. In: Maike Franzen (Hrsg.): Lernplattformen. Web-based Training 2005. Empa-Akademie: Dübendorf, Schweiz2005, S.11–19.

Share Your Work (2018). Creative Commons. Verfügbar unter: https://creativecommons.org/share-your-work/ [14.02.2018]

Smartphone-App Berechtigungen – Erforderlich oder ein Ärgernis?. (2017) Datenschutzbeauftragter – Info, 14.11.2017 Verfügbar unter: https://www.datenschutzbeauftragter-info.de/smartphone-app-berechtigungen-erforderlich-oder-ein-aergernis/[08.12.2017]

Spitzer, M. (2015). Helicopter-Eltern. Geist und Gehirn, Nervernheilkunde 1-2/2015. Verfügbar unter: http://www.znl-ulm.de/Veroeffentlichungen/Geist_und_Gehirn/NHK15_Helicopter-Eltern.pdf [122.04.2018]

Steinhammer, E. E. (2018). Nur gemeinsam können wir Datenschutz durchsetzen, mit einem Verbandsklagerecht. epicenter.works, 17.04.2018. Verfügbar unter: https://epicenter.works/content/nur-gemeinsam-koennen-wir-datenschutz-durchsetzen-mit-einem-verbandsklagerecht [19.04.2018]

Tschohl, C., Scheucher, E., Kargl, D., Luksan, J., Czadilek, A., Waloschek, H., Kreissl, R., Klinger, K., Hötzendorfer, W., Möchel, E. (2017). HEAT 1.2 - Handbuch zur Evaluation der Anti-Terror-Gesetze in Österreich . Verfügbar unter: https://epicenter.works/sites/default/files/heat_v1.2.pdf [24.04.2018]

Warren, S.D. Brandeis, (1890). "The Right to Privacy". Harvard Law Review IV, 1890, S.193 ff. Verfügbar unter: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [10.04.2018]

Welan, M. (2002). Über die Grundrechte und ihre Entwicklung in Österreich. Österreich in Geschichte und Literatur, Heft 4-5, 2002

Wimmer, B. (2018). Überwachungskapitalismus: Wie unser Online-Verhalten ausgewertet wird. Futurezone, 20.02.2018. Verfügbar unter: https://futurezone.at/netzpolitik/ueberwachungskapitalismus-wie-unser-online-verhalten-ausgewertet-wird [20.02.2018]

WKO (2017). EU-Datenschutz-Grundverordnung (DSGVO): Das Datenschutz-Anpassungsgesetz 2018. wko.at, 26.09.2017. Verfügbar unter: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-datenschutz-anpassungsgesetz-2018.html [24.04.2018)

9. Abbildungsverzeichnis

Abbildung 1 Auswirkung unterschiedlicher Kennwortkomplexität 35
Abbildung 2: Beispiel für eine App mit vernünftigen Appberechtigungen 41
Abbildung 3: Wie sich jede erfasste Tätigkeit auswirkt. (Cracked Labs CC-BY-SA 4.0) 51

10. Anhang

10.1. Experteninterviews

10.1.1. Interview mit MinR Dr. Thomas Menzel

Halbstrukturiertes Interview mit MinR Dr. Thomas Menzel, IT und Datenschutzbeauftragter des Bildungsministerium am 3. November 2017 im Bildungsministerium.

MinR. Dr. Thomas Menzel:

Wir sind im Datenschutz im öffentlichen Bereich schon relativ gut aufgestellt. Die DSGVO ist nichts allzu Neues. Wir können mit Datenschutz schon seit Jahrzehnten gut umgehen. Es ist so, dass wir die meisten der Umstellungsarbeiten die zu machen sind schon erledigt haben. Des Weiteren wird es noch einige technische Umstellungen geben wie Verschlüsselung einführen, „Privacy by Design“, Pseudonymisierung. Das sind so die Schlagworte die das alte Datenschutzgesetz nicht kannte die Grundverordnung aber kennt, die wir jetzt umsetzen müssen. Vor allem gibt es nun auch umfangreiche Dokumentationspflichten. Es fallen die Meldepflichten und Genehmigungspflichten im Datenverarbeitungsregister fallen weg. Dafür muss aber jeder seine eigenen Anwendungen dokumentieren. Und da ist unsere Philosophie die Schulen weitestgehend wenig zu belasten. Alles was als Standardanwendungen und Schulen ausgerollt wird und wurde, alle Anwendungen die das Ministerium oder ein Landesschulrat den Schulen vorgibt, also Sokrates Web an den Pflichtschulen oder Sokrates an den Bundesschulen, WebUntis als elektronisches Klassenbuch, Lernplattformen wie Moodle oder lms.at oder andere, dann sind das Anwendungen. die vom Ministerium ausgehen. Da wird sich das Ministerium auch darum kümmern alles was für die Datenschutzgrundverordnung notwendig ist auch vom Ministerium erfüllt wird. Da brauchen sich die Schulen nicht viel darum kümmern.

Wichtige Neuerung ist, dass jede Behörde einen Datenschutzbeauftragten nennen muss. Das werden die Schulen nicht brauchen. Es wird einen Datenschutzbeauftragten im Ministerium geben, das bin ich, und einen Datenschutzbeauftragten in jedem Landesschulrat. Und der Landesschulrat wird auch zumindest für den Bereich der

Bundesschulen, für die Pflichtschulen müssen wir noch schauen, auch die Datenschutzaspekte an den Schulen übernehmen. Wir brauchen also keinen Datenschutzbeauftragten an den Schulen.

Daniel Lohninger:

Wie kommen Sie da der Informationspflicht des Datenschutzbeauftragten an den Schulen nach?

MinR. Dr. Thomas Menzel:

Für den einzelnen Lehrer ist datenschutzrechtlich wichtig was er im Unterricht einsetzt. Dass er hier eine Sensibilität hat. Man kann einmal davon ausgehen, dass alle Anwendungen die vom Bund, vom Land oder vom Ministerium zur Verfügung gestellt werden datenschutzrechtlich sauber sind. Da achten wir auf ein hohes Niveau damit Schülerdaten eben nicht in die Privatwirtschaft gelangen, für irgendwelchen Werbeangeboten verwendet werden oder sonst was. Aber nichts desto trotz gibt es viele pädagogische Apps und Anwendungen die aus Amerika, aus Weißrussland, ich weiß nicht woher kommen und da muss man den Lehrer sensibilisieren. Das müssen ja nicht nur per se böse Anwendungen sein die Daten rauben, das können durchaus pädagogisch sinnvolle Anwendungen sein bei denen man aber nicht sagen kann wo der Server steht und was mit den Daten passiert. Es ist vielleicht ein ganz sinnvolles Sprachlaboratorium oder was auch immer. Da muss man den Lehrer soweit sensibilisieren, dass er weiß das er diese Webseiten oder was auch immer das ist durchaus verwenden kann aber möglichst nur Pseudonyme einsetzt und keine personenbezogenen Schülerdaten dorthin übermittelt.

Daniel Lohninger:

Und diese Informationen, diese Schulungen gehen vom Ministerium aus?

MinR. Dr. Thomas Menzel:

Was wir brauchen ist eine gute Schulung in der Schulverwaltung. Die Schulleiterinnen, die Administratoren und IT-Kustoden brauchen eine vierstündige bis eintägige Schulung. Das wird einerseits in der zukünftigen Schulleiterausbildung verankert.

Dafür macht das Ministerium ja ein genaues Curriculum und da wird der Datenschutz fest verankert. Wir werden in der Fort und Weiterbildung sowohl für Verwaltungsbedienstete als auch den pädagogischen Hochschulen Datenschutzkurse bzw. Schulungen anbieten. Da wir in der verbleibenden Zeit nicht genügend Lehrpersonal organisieren können um das im Frontalunterricht abzuhandeln bis Mai machen wir MOOC, einen Massive Open Online Course. Wir werden einen MOOC zum Datenschutz planen und den an den PHs zur Verfügung stellen.

Dann gibt es schon Folien zum Selbststudium. Es gibt ein Skript zur digitalen Schülerverwaltung für Schulleiter. Dieses gibt es in einer alten Version und bezieht sich nur auf die DSG und wird gerade überarbeitet. Es wird vermutlich im Dezember fertig und dann fürs Selbststudium zur Verfügung gestellt.

Das sind die Schulungsangebote die wir haben. Ich weiß auch schon von einigen PHs die auch schon selbst überlegen Unterlagen oder Schulungen zu gestalten. Konkret weiß ich, dass es an der PH Wien, PH Burgenland und PH Salzburg eigenständige Überlegungen gibt etwas zum Datenschutz zu umzusetzen.

Daniel Lohninger:

An den PHs erreichen Sie ja vor allem Lehrkräfte in der Ausbildung. Was ist mit den schon Ausgebildeten Lehrkräften?

MinR. Dr. Thomas Menzel:

Die Maßnahmen sollen auch die Fortbildung umfassen.

In den Folien haben Sie einige Sachen. Das sind im Prinzip alle Punkte die umgesetzt werden müssen damit wir die DSGVO Umstellung gut hinbringen. Sie sehen dann das sind eher die Zuständigkeiten des Ministeriums und des Landesschulrats und dann gibt es vor allem im Punkt Betroffenenrechte wahren die Zuständigkeit des Schulen. Wenn der Vater vom Maxi kommt und wissen will was vom Maxi, der in die 3C geht ,alles an der Schule so gespeichert ist, ist das sein gutes Recht, das sogenannte Auskunftsrecht. Er wird das nicht im Ministerium oder im Landesschulrat erfragen sondern am besten weiß der jeweilige Schulleiter was er von seinen Schülern gespeichert hat. Und dort kann man nachfragen und wird eine Information bekommen was verarbeitet ist.

Daniel Lohninger:

Das heißt Sie können mir da vermutlich auch keine Information geben wie oft Auskunftsbegehren an Schulen gestellt werden?

MinR. Dr. Thomas Menzel:

Nein, das kann ich nicht. Erstens ich darf gar nicht reinschauen. Wir haben gesetzlich festgelegt, dass alle Schülerbezogenen Daten Benotung, Klassenbucheinträge oder sonstiges nur lokal an der Schule bleibt und dass es nicht vom Landesschulrat oder vom Ministerium eingesehen werden kann. Nur der jeweilige Schulleiter kann die Daten im Sokrates einsehen und das nur für die Kinder an seiner Schule.

Daniel Lohninger:

Das heißt die Daten liegen zentral können aber dort nicht eingesehen werden?

MinR. Dr. Thomas Menzel:

Genau sie liegen zwar zentral sind aber verschlüsselt. Wir nennen das mandantenfähige Datenbank. Das heißt nur das jeweilige Personal an einer Schule kann die Daten der Schule einsehen nicht aber die von anderen Schulen. Zumindest was Sokrates im Bund betrifft, da kenne ich mich aus. Die anderen Schulverwaltungen kenne ich nicht genau, es sollte dort aber genauso funktionieren.

Natürlich gibt es jetzt gesetzliche Grundlagen, dass man etwas an den Landesschulrat übermitteln muss. Der Landesschulrat muss planen wieviel Turnlehrer schickt er an welche Schulen, wie viele Religionslehrer schickt er an welche Schulen. Da gibt es umfangreiche Berichtspflichten die eine gesetzliche Grundlage haben. Aber auch hier ist es wieder so, dass der Landesschulrat nicht direkt in die Schuldatenbank zugreifen kann sondern der jeweilige Schulleiter muss aufgrund der gesetzlichen Anforderungen die er hat die Berichte erstellen die der Landesschulrat braucht. Und der Schulleiter drückt auf den Knopf damit diese Berichte abgesandt werden. Das heißt der Schulleiter ist auch verantwortlich dass diese richtig und datenschutzrechtlich sauber sind.

Daniel Lohninger:

Diese Berichte werden also auch anonymisiert?

MinR. Dr. Thomas Menzel:

Je nachdem wie es notwendig ist. Wenn es z.B. nur darum geht wie viele Lehrer schicke ich an welche Schule damit alle genügend Turnunterricht oder Religionsunterricht dann werden die Schülerzahlen ausreichen.

Daniel Lohninger:

Werden Daten von Schüler/innen abseits der im BilDokG genannten Fälle erfasst?

MinR. Dr. Thomas Menzel:

Nein, von Schülern nicht. Von Lehrern ist die ganze Lehrerbesoldung, Überstundenabrechnung und ähnliches zu erfassen was aber im Dienstrecht geregelt ist. Also die übliche Personalverwaltung die ich überall als Arbeitgeber habe. Diese ist natürlich auch mit massiv personenbezogenen Daten vorhanden. Wer arbeitet wann wieviel, Krankenstände und ähnliches. Das sind aber keine Anwendungen die wir im Unterrichtsministerium erschaffen haben sondern die werden zentral vom Finanzministerium für den gesamten Bundesbereich für alle 400.000 Bediensteten vorgegeben. Das PMSAB, das ist die Personalverwaltung des Bundes. Da kümmert sich natürlich das Finanzministerium darum, aber ich gehe einmal davon aus, dass die DSGVO konform sein wird.

Daniel Lohninger:

Wie hat sich die Praxis an den Schulen in Österreich seit dem Wegfallen des Safe Harbour Abkommens geändert und welche Schritte wurden von Seiten des Ministeriums in dieser Hinsicht unternommen?

MinR. Dr. Thomas Menzel:

Das Safe Harbour Abkommen interessiert uns insofern nicht besonders stark weil alle Server die wir betreiben sowohl die Verwaltungsserver, so wie die pädagogischen Server sprich Digi4school wo die elektronischen Schulbücher der Kinder, die beiden Lernplattformen wie auch das elektronische Klassenbuch liegen auf österreichischen Servern.

Die einzige Ausnahme ist Microsoft. Mit denen haben wir eine Vereinbarung, dass Schulen auch Office365 nutzen können. Und Microsoft Office365 E-Mail-Adressen

nutzen können. Hierfür gibt es mit Microsoft eine Datenschutzvereinbarung die besagt, dass alle personenbezogenen Daten dieser Postfächer auf europäischen Servern liegen. Die liegen in Amsterdam bzw. in Dublin. Die DSGVO macht keinen Unterschied ob das ein österreichischer Server ist oder nicht. Es muss ein Server im EWR-Raum sein.

Daniel Lohninger:

Wie sehen Sie die Nutzung von unsicheren Lernplattformen wie Edmodo (bei der Leistungsbeurteilungen auf US-Servern liegen)?

MinR. Dr. Thomas Menzel:

Also prinzipiell gilt generell ist es so dass nach der alten Rechtslage der Schulleiter der Datenschutzverantwortliche ist; d.h. die Beurteilung über die datenschutzrechtliche Einordnung von E-Learningplattformen oder sonstige Tools die Lehrer an seiner Schule im Unterricht verwenden obliegt ihm. In der Praxis wird er sich dabei oft an der Expertise des IT-Kustoden orientieren, respektive gibt es auch Ansprechpartner für ihn bei mir oder beim Landesschulrat.

Generell gilt sowohl für die alte wie für die neue Rechtslage bei Servern die nicht von der Schule selber betrieben werden aber sich im EU-Raum befinden sollten die Schulen eine Dienstleistungsvereinbarung mit dem Dienstleister abschließen.

Wenn man das nicht hat weil es einfach nur ein tolles Webangebot ist bei dem man entdeckt und entscheidet das möchte ich für die nächsten Wochen oder fürs nächste halbe Jahr für meine Schüler nutzen im Unterricht dann sollte man auf jeden Fall Pseudonyme verwenden. Das sollte kein Problem sein da hier keine Leistungsbeurteilungen oder umfangreiche Profilingdaten gespeichert werden. Es geht hier meistens nur darum, dass den Schülern Content zur Verfügung gestellt wird, dass der Schüler mit diesem Content arbeitet und vielleicht gibt es einen kurzen Multiplechoicetest nachher und hier reicht es völlig wenn man mit Pseudonymen arbeitet.

Daniel Lohninger:

Wie sehen Sie die Nutzung von datenschutzrechtlich fragwürdigen SocialMedia Plattformen wie Facebook zur Aufgabenverteilung und Kommunikation?

MinR. Dr. Thomas Menzel:

Das sehen wir anders. Das haben wir auch in den Folien unter „Einsatz von Medien". Generell gibt es den Grundsatz: „Facebook und WhatsApp sind fürs Wohnzimmer die Lernplattform ist fürs Klassenzimmer".

Es gibt professionelle Tools mit denen man das meiste das man mit Facebook oder WhatsApp machen will erledigen kann. Bitte diese zu verwenden.

Wenn eine Klasse auf Skikurs fährt und beschließt, dass es für sie viel leichter ist in der Kommunikation wenn sie eine WhatsApp-Gruppe einrichten dann habe ich damit insofern kein Problem da hier keine Daten wie Leistungsbeurteilungen kommuniziert werden sondern Inhalte wie welche Skibrille nehme ich mit oder wieviel Unterhosen.

In diesem Bereich tue ich mir allgemein leichter in der Sekundarstufe 2 wenn die Schüler zugestimmt haben. Da habe ich kein Problem wenn sie sozial adäquate Medien verwenden, und sie chatten auch mit ihren Freunden über WhatsApp. Facebook ist eh schon tot. Die Schüler nutzen hauptsächlich WhatsApp, dann sollen sie es auch im Klassenzimmer nutzen. Nur muss sich auch der Lehrer bewusst sein worauf er sich einlässt, eine höhere Erreichbarkeit geht damit einher und auch viele WhatsApp-Nachrichten und meistens erwarten die Schüler wenn der Lehrer in der Gruppe ist auch, dass dieser rasch antwortet. Die Frage ist ob der Lehrer das will oder nicht.

Daniel Lohninger:

Es geht nicht nur um Inhalte sondern auch um Metadaten. In dem Moment in dem ich WhatsApp installiere gebe ich Zugriff auf mein Adressbuch. Wenn ich also WhatsApp für den Unterricht vorgebe zwinge ich die Schüler ihre Daten und die von andern WhatsApp zur Verfügung zu stellen.

MinR. Dr. Thomas Menzel:

Das kann ich sicher nicht. Ich kann als Lehrperson nicht sagen liebe Schüler ihr müsst WhatsApp verwenden. Das geht definitiv nicht. Was mit ein bisschen Augenzudrücken geht ist wenn die Initiative gemeinsam entwickelt wird. Ich kenne das so: Wenn WhatsApp-Gruppen für den Unterricht genutzt werden, dann nicht weil der Lehrer sagt ihr müsst WhatsApp nutzen sondern, dass die Klasse selbst schon eine WhatsApp-Gruppe hat und der Lehrer gefragt wird ob er nicht beitreten wollte, könnte oder dürfte damit er da auch sinnvoll mitkommunizieren kann.

Also der Lehrer ist sicher geschäftsfähig genug um zu erkennen ob er ein datenschutzrechtliches Problem hat oder nicht wenn er sein Handy in eine WhatsApp-Gruppe der Schüler einbindet. Das überlassen wir dem Lehrer. Es gibt sicher keine Verpflichtung dazu, dass ein Lehrer WhatsApp verwenden muss und es kann auch kein Direktor festlegen, dass für die dienstspezifische Kommunikation WhatsApp genutzt werden muss.

Das wird's nicht spielen. Es ist wahrscheinlich nicht so sinnvoll das massiv für pädagogische Zwecke im Klassenverband zu verwenden. Wenn es in der Sekundarstufe 2 einen Konsens darüber gibt, dass WhatsApp für dieses oder jenes genutzt wird sehe ich das nicht so tragisch.

In der Unterstufe ist das anders. Wir haben in der Novellierung des DSG jetzt endlich die Klarstellung erreichen können, dass man mit 14 Jahren hinreichend geschäftsfähig ist um eine datenschutzrechtliche Zustimmung bzw. Einwilligungserklärung zu geben. Und davor sind es die Eltern. Das heißt wenn ich in der Sekundarstufe 1 bin muss ich die Eltern fragen. Das ist so.

Daniel Lohninger:

Als Lehrer hätte ich, auch aus pädagogischen Gründen heraus, die Möglichkeit einen sicheren Messenger zu verwenden, oder nicht? Vor allem da ja auch die europäische Datenschutzbehörde Article 29 Working Party große Bedenke bezüglich der Datenübertragung zwischen WhatsApp und dem Mutterkonzern Facebook geäußert hat.

MinR. Dr. Thomas Menzel:

WhatsApp ist wie gesagt fürs Wohnzimmer und nicht fürs Klassenzimmer. Dafür haben wir WebUntis. Das gibt es als HandyApp. Ich kenne das von meinem eigenen

Sohn. Der Lehrer trägt dort die Hausübungen, den Teststoff und anderes ein. Das funktioniert auch als Webanwendung. An vielen Schulen sind die Schüler für WebUntis freigeschalten. Und da kann ich davon ausgehen, dass es die Datenschutzanforderungen erfüllt und der Server steht in Österreich und ist vom BMB beauftragt. Das macht Sinn. Für Lernplattformen weiß ich nicht genau ob es da ein Handy Frontend gibt oder nicht. Ich vermute aber dass es zumindest auf den größeren Handys oder Tabletts ganz gut funktionieren wird.

Ich sehe die Verwendung von Messenger auch nicht als unbedingt notwendig. Es gibt genügend professionelle Tools. Zwei gibt es, ein drittes prüfen wir gerade, dass das Mitteilungsheft ersetzen bzw. auf eine elektronische Form bringen kann. Das ist die klassische Eltern Lehrer Kommunikation. Dafür werde ich sicher kein WhatsApp verwenden. Damit hätte ich auch keine Nachweismöglichkeit, dass die Eltern es gelesen haben oder die die Nachweismöglichkeit, dass wirklich die Eltern geantwortet haben und nicht irgendwer der gerade Zugriff auf den WhatsApp-Account hat. Da gibt es geeignetere Tools.

Daniel Lohninger:

Sehen sie Auswirkungen der geänderten Gesetzeslage auf Lehrer/innen? Z.B. ein gesteigertes Bewusstsein für Datenschutz?

MinR. Dr. Thomas Menzel:

Wir haben derzeit einen medialen Hype. Die Datenschutzgrundverordnung ist in allen Zeitungen. Es wird von ein paar Anwälten ein bisschen gezündelt. Die verdienen gut daran und sagen so grauslich, fürchterlich und es wird alles schlimm werden mit den zu erwartenden Strafen. So ist das nicht. Aber natürlich es ist einiges zu tun vor allem sehr viel zu dokumentieren. Wir müssen uns alle Systeme anschauen. Und ich finde es auch nicht schlecht, dass der Datenschutz durch die Grundverordnung medial in den Vordergrund bringt und dass ich deswegen mehr Lehrer mit dem Thema erreiche.

Daniel Lohninger:

Auch die höheren Strafen sind durchaus sinnvoll.

MinR. Dr. Thomas Menzel:

Ja, aber die treffen uns im Unterricht nicht. Das ist kein Problem.

Klassische Beispiele wo uns was passiert sind währen: Wir hatten eine Schule die wollte es ihren Schülern die eine Nachprüfung bei der Matura hatten leichter machen und hat eine Excel Tabelle geschrieben wer in welchem Raum seine Nachprüfung hatte. Diese Excel Tabelle haben sie blöderweise nicht ins Schulintranet gestellt sondern sie ist im Internet gelandet. Einer der betroffenen Schüler hat sich dann ein halbes Jahr nach bestandener Matura um einen Job bei der Piratenpartei beworben. Der Personalchef hat den Jobbewerber dann wie es üblich ist einmal gegoogelt und das erste was er gefunden hat ist, dass der eine Nachprüfung bei der Matura hatte weil er die Liste gefunden hat. Berechtigterweise hat dieser dann gemeint das ist schon eine komische Auffassung von Datenschutz wenn ich öffentlich nachlesen kann welcher Schüler wann eine Nachprüfung hatte. Das sind die Fehler die uns passieren.

Dann gab es eine Gruppe von Lehrern die haben eine Fortbildung zum Thema „Richtig Bewerben gemacht“. Sie haben dann viele Lebensläufe von sich geschrieben, untereinander ausgetauscht und bewertet. Und irgendwann sind sie draufgekommen, dass so riesige PDFs schlecht über Mail auszutauschen sind weil das Postfach sehr schnell voll ist und haben einen Moodlekurs dafür angelegt. Sie haben also diesen Moodlekurs als Dokumentenspeicher genutzt um ihre Lebensläufe schnell und einfach auszutauschen. Was sie nicht beachtet haben ist, dass sie keinen neuen Moodlekurs angelegt haben sondern einen alten der vor eineinhalb Jahren angelegt wurde kopiert? Default mäßig sind Moodlekurse auf Lernplattform.at nicht von Google durchsuchbar. Ich kann allerdings beim Anlegen des Kurses einen Schalter umlegen und sagen den Moodlekurs will ich öffentlich stellen. Und das war eben genau der mit den Lebensläufen. Damit ist Google über alle Lebensläufe drübergefahren, hat diese Lebensläufe in den Cash von Google genommen und die Lebensläufe waren mit ziemlich erst mit viel Mühe wieder aus Google raus zu löschen.

Das sind genau die Fehler die uns passieren.

Oder irgendein Hauptschullehrer der seinen Verwaltungs-PC am Schreibtisch stehen hat. Auf diesem PC hatte ein paar Briefe an den Bürgermeister der Gemeinde geschrieben, in denen er bittet einige Kollegen disziplinarrechtlich abzumahnen, weil sie Laufend 10 Minuten zu spät in den Unterricht kommen. Und dann hat dieser Kollege irgendwie sein WindowsKennwort im Internet gespeichert. Damals hat sich Anonymous gerade darauf spezialisiert irgendwelche Lücken im Unterricht Bereich zu finden. Hat dann dieses Kennwort des Direktors gefunden und die komplette Festplatte des Lehrers heruntergeladen und ins Internet gestellt. Es haben zwar nur einige wenige Insider mitbekommen dass diese Briefe online standen, aber das ist nur passiert weil das Kennwort nicht sicher verwahrt wurde. Daran müssen wir arbeiten.

Dann gibt es einen Abteilungsvorstand an einer HTL. Die HTL hatte zwei WLANs, Ein schnelles da nur wenige Lehrer drin waren. Und ein langsameres das für die Schüler angelegt werden. Er wollte seinen Schülern etwas Gutes tun und hat an die Tafel sein Kennwort geschrieben damit die Schüler in das schnellere WLAN konnten. Was er nicht bedacht hat, dass ist gleichzeitig auch sein SokratesKennwort war.

Bei diesen Dingen müssen wir Aufklärung betreiben den Lehrern auf die Finger klopfen und den Lehrern sagen bitte passt auf eure Kennwörter auf. Wenn Kennwörter durch Fahrlässigkeit öffentlich werden sind das disziplinarrechtliches Vergehen und keine Kavaliersdelikte. Es ist wichtig, dass mehr in die Köpfe der Lehrer zubringen.

Ich kenne keinen Fall in dem jemand vorsätzlich Schülerdaten missbraucht hat um Irgendeinen Blödsinn damit zu machen, zu verkaufen oder sonst etwas. Aber der Umgang mit Kennwörtern ist ein fahrlässiger. Dann passieren genau solche Dinge wie gerade beschrieben und dann stehen wir wieder in der Kronen Zeitung und das ist dann ein Image Problem.

Der zweite Bereich in dem wir immer wieder Probleme haben ist jetzt nicht Datenschutz sondern Urheberrecht. Wir haben mehr als 6.000 Schulen in Österreich und damit mehr als 6.000 Schulwebseiten. Sehr viele Lehrer sind motiviert Webseiten zu schreiben und zu gestalten. Worin sie dann auf nicht unterscheiden Ist das man zwar sehr wohl urheberrechtliche ist Material im Unterricht einsetzen kann, nicht

aber auf der Schulwebseite. Gerne werden hier Comics benutzt und die Seite aufzupeppen. Und die Lehrer mögen hier anscheinend besonders die Comics von Ulli Stein. Diese landen regelmäßig auf Schulwebseiten und dann meldet sich regelmäßig der Anwalt von Uli Stein bei uns. Der sagt dann liebe schule erwischt, € 3.000 Mahngebühr und € 2.000 Anwaltskosten. Das zahlen wir ungefähr 10-mal im Jahr. Das geht ins Geld und ist auch nicht sehr sinnvoll.

Was wird jetzt gemacht haben sowohl für den Datenschutz wie genau für diese Urheberrechtsthematik ist ein nettes Plakat zu gestalten. Dieses Plakat kann man in jedem Lehrerzimmer aufhängen. Um das durchzulesen braucht man nur eine halbe Minute Und so können wir diese Inhalte auch dem fortbildungsresistentesten Lehrer klarmachen. Aufpassen was ich im Internet publiziere, Aufpassen was ich mit meinem Kennwörtern machen. Brauch ich dann mal 4 stündige Schulungen in denen diskutiert wird ob ich jetzt WhatsApp verwenden darf oder nicht, mit welchen Einstellungen und so weiter. Ich muss einfach nur mal klar machen pass auf dein Kennwort auf. Damit kann man schon viele Probleme ausräumen. Dafür reicht es schon wenn ich im Lehrerzimmer ein Plakat aufhänge.

Es ist auch nicht Aufgabe des Lehrers sich mit Urheberrecht auszukennen, aber es ist Aufgabe des Schulleiters sicherzustellen dass die Lehrer die auf der Schulwebseite arbeiten wissen was sie dürfen und was nicht.

Daniel Lohninger:

Etwaige Strafen werden Vom Ministerium getragen?

MinR. Dr. Thomas Menzel:

Die Strafen werden vom Schulerhalter getragen. Bei einer Bundesschule sind dass wir. Bei einer Pflichtschule ist es die Gemeinde. Diee Gemeinden sehen es oft nicht ein und versuchen, dass wir die Rechnung zahlen. Es ist aber klar der Schulerhalter verantwortlich. Wie oft das bei den Gemeinden passiert kann ich gar nicht sagen weil ich es oft nicht mitbekomme. Bei den Bundesschulen schon weil wir verantwortlich sind im Ministerium und die dann rechtsfreundlich vertreten.

Daniel Lohninger:

Zur Informationspflicht: Wie werden die Schüler/innen über die Details der Datenverarbeitung und ihre Rechte und Pflichten informiert?

MinR. Dr. Thomas Menzel:

Erstens finde ich das ein super Thema für den Unterricht. Es gibt schon viel im Bereich der Handelsschulen und HTLs. Wir haben generell schon einmal ein E-Goverment-Skriptum gemacht mit Inhalten wie Was ist helpgv.at, was ist deine Bürgerkarte, was ist eine Handysignatur, was ist ein elektronisches Zeugnis, wie mache ich eine Arbeitnehmerveranlagung und so weiter. Das hat aber nur begrenzte Datenschutzbezug. So etwas könnte ich mir auch für den Datenschutz vorstellen.

Wir arbeiten momentan vor allem an Infomaterial für Lehrer. Dieses findet man auf pubshop.bmb.gv.at.

Daniel Lohninger:

Also die Informationspflicht ist auf jeden Fall noch ausbaufähig.

MinR. Dr. Thomas Menzel:

Um den Buchstaben des Gesetzes Genüge zu tun wird man eine 3 bis 4 seitige Info auf einer Webseite veröffentlichen; „www.bmb.gv.at/datenschutz“ zum Beispiel. Das würde den gesetzlichen Ansprüchen genügen und das werden wir auch auf jeden Fall schaffen bis Mai.

Aber dann könnt ihr mal natürlich pädagogisch mehr machen und den Datenschutz in den Unterricht bringen. Das wäre sicher interessant.

Daniel Lohninger:

Sehen Sie noch andere Auswirkungen auf die Schulen die sich durch die EU-DSGVO und die Novellierung des DSG ergeben?

MinR. Dr. Thomas Menzel:

Es fällt das Standard- und Musterverzeichnis weg. Es fällt die DVR Meldung weg. Wichtig ist Artikel 30 der DSGVO, die Verpflichtung ein Anwendungsverzeichnis zu führen. Das heißt wir machen das für alle Anwendungen die wir zentral vorgeben.

Aber Es gibt viele Anwendungen die die Schulen selbst Vorgehen beziehungsweise selbst entwickeln, da sind dann auch diese dafür verantwortlich.

Klassiker ist die Videoüberwachung. Entweder hat die Schule ein Drogenproblem und es stehen die Dealer am Schulhof oder es gehen jeden Tag 3 Tabletts verloren. Da gibt es dann auf den Wunsch nach Video Überwachung um die Dealer abzuschrecken oder herauszufinden wer die Flügel sind die den Tabletts wachsen. Wir kümmern uns zentral nicht um Video Überwachung, das muss jede Schule für sich machen.

Daniel Lohninger:

Ist Videoüberwachung an Schulen in Österreich ein Thema? Ich dachte das wäre hierzulande nicht so verbreitet.

MinR. Dr. Thomas Menzel:

Doch das ist immer wieder ein Thema aus den oben genannten Gründen oder auch Problemen mit schulfremden Personen am Schulgelände. Nicht bei irgendeiner Volksschule mit 50 Leuten da kennt jeder jeden, da fällt jede schulfremde Person am Gelände auf. Aber ein BGM oder eine pädagogische Hochschule. Die pädagogische Hochschule Wien zum Beispiel hat gemeint der Ettenreichlatz ist so weitläufig dass sie ein paar Kameras brauchen. An großen Schulen wo man keinen Überblick darüber hat ob eine Person schulfremd ist oder nicht ist das durchaus ein Thema.

Oder auch immer komplexe gestaltetes Systeme mit Kopierkarten. Hier wird oft erfasst wer lädt wann wie viel auf und wer kopiert wann wie viel. Die Kopierkarten sind meist nicht mit Pseudonymen sondern mit Klarnamen verbunden und dadurch datenschutzrechtlich relevant.

Dann elektronische Zutrittskontrolle, also Auf- und Zusperren mit Karte. Ist Gott sei Dank an den meisten Schulen kein Thema da datenschutzrechtlich sehr heikel. Hier muss man sehr aufpassen dass man keine Bewegungsprofile speichert. Das wird in der Zukunft ein schulspezifisches Thema sein.

Dann diverse Webseiten die an der Schule bzw. für die Schule gestaltet werden und Datenbanken mit personenbezogenen Daten im Hintergrund eingebunden werden.

Essensverwaltung und ähnliche. Da muss die Schule selbst so sensibel sein und das datenschutzrechtlich einwandfrei umsetzen wenn sie Anwendungen gestalten die personenbezogene Daten erfassen und nicht vom BMB zur Verfügung gestellt werden. Dann müssen die Schulen selbst schauen dass sie alle Verpflichtungen der DSGVO erfüllen und das ist im Wesentlichen der Artikel 30 nämlich das Anwendungsverzeichnis. Da wird es schon Musterformulare geben. Wir arbeiten gerade an einem. Und der Landesschulrat wird diese Musterformulare zur Verfügung stellen.

Viele Schulen die die Microsoft Produkte nutzen stellen ihren Schülern auch E-Mail Adressen zu Verfügung. Beim Schüler muss ich dafür um Zustimmung Fragen. Beim Lehrer nicht, Da ich bei diesem als Dienstgeber das Recht haben die Kommunikationskanäle vorzugeben. Also zum Beispiel eine E-Mail Adresse die zweimal die Woche abgerufen werden muss. Wie das auch jeder andere Dienstgeber machen kann. Beim Schüler kann ich das nicht. Wenn die Eltern eines Schülers oder der Schüler die Einrichtung einer E-Mail Adresse verweigern, dann muss ich mich danach richten und ihm Informationen in konventioneller Form zukommen lassen.

Aber wenn die Schule E-Mail Adressen bereitstellt und Üblicherweise also in 99,9 Prozent der Fälle werden diese auch angenommen muss ich ein Anwendungsverzeichnis erstellen. Dadurch dass die meisten Schulen über Office 365 machen wird dieses immer gleich aussehen.

Das Anwendungsverzeichnis macht vor allem Arbeit bei Anwendungen die nur für eine bestimmte Schule geschaffen sind. Neulich hatte ich jemanden davon einer Berufsschule in Tirol. Wenn man in Tirol zum Friseur geht hatte eine Meisterschule eine Datenbank da werden alle möglichen Kundendaten eingetragen. Zum Beispiel Shampoo Unverträglichkeiten und sonstiges. Ich hab keine Ahnung was die da alles eintragen. Die Berufsschulen dort zu möchte praxisnah Unterrichten und nutzen deshalb dieselbe Datenbank auch an der Schule. Das ist die einzige Schule die eine Friseur-Kopfwasch-Datenbank verwendet. Da wird sich die Schule selber drum kümmern müssen dass das ganze datenschutzrechtlich in Ordnung ist. Ich habe jetzt Unterricht Ministerium keine Erfahrung mit Friseur Datenbanken. Da müssen die sich selbst drum kümmern.

Daniel Lohninger:

Haben die Schulen hierbei Unterstützung vom Ministerium.

MinR. Dr. Thomas Menzel:

Die Schulen haben dafür Ansprechpartner beim Landesschulrat sie soll sich also nicht direkt an mich wenden soll uns erst in den Landesschulrat. Hat sich noch nicht ganz herumgesprochen ich bekomme einige Anfragen von Schulen die Anwendungen installieren wollen Und beim Landesschulrat nicht notwendigen Informationen bekommen haben. Jetzt muss man aber sagen dass der Datenschutzbeauftragten Landesschulrat erst vor kurzem, ein bis zwei Monaten, installiert wurde.

Daniel Lohninger:

Wurden dafür neue Stellen geschaffen?

MinR. Dr. Thomas Menzel:

Nein, das sind neue Funktionen aber es sind die gleichen Leute die jetzt diese Aufgaben übernommen haben. Sie sind bis jetzt noch nicht offiziell nominiert sondern nur intern schon festgelegt. Das sind momentan die Personen die vom Landesschulrat nominiert worden sind. Sinnvollerweise sind das Techniker und Juristen.

Wasser in den Schulen auch vorkommt sind zum Beispiel Anfragen der Polizei. Aufgrund von Unterhalt Streitigkeiten oder sonstigem. Wenn hier ein Gerichtsbeschluss vorgelegt wird kein die Schule bin ich selbst feststellen das ist rechtmäßig ist. Wenn der Fall nicht klar gelagertes oder sie sich unsicher sind können sie sich immer an den Datenschutz Verantwortlichen im Landesschulrat wenden und dort erst Informationen einholen bevor irgendwelche Daten herausgegeben werden.

Was auch regelmäßig vorkommt sind Anwälte von irgendwelchen Verwertungsgesellschaften die an den Schulen anfragen, wer hinter bestimmten IP-Adressen steht. Bzw. dass sie Kenntnis haben das über eine bestimmte IP Adresse zu einem bestimmten Zeitpunkt MP3-Files getauscht wurden und man ihnen jetzt doch bitte Auskunft geben sollwer hinter dieser IP Adresse steckt. Dies blocken wir dann standardmäßig mit der Begründung dass wir solche Aufzeichnungen nicht führen ab.

Daniel Lohninger:

Ergeben sich sonst noch Änderungen durch die EU-DSGVO für die Schulen über die wir noch nicht gesprochen haben?

MinR. Dr. Thomas Menzel:

Nicht wirklich, da die Standards im öffentlichen Bereich schon bisher hoch waren. Gewisse Anpassungen werden durchgeführt. Der geänderte Modus durch die DSGVO trifft er den privaten Bereich also Firmen zu. Die gesteigerte Bedeutung des Datenschutzes durch die DSGVO sehe ich positiv.