Rechtsfragen zu Cloud-Angeboten für Hochschulen

Johannes Nehlsen
Stabsstelle IT-Recht
der bayerischen staatlichen Universitäten und Hochschulen
c/o Rechenzentrum Universität Würzburg
Am Hubland
97074 Würzburg
johannes.nehlsen@uni-wuerzburg.de

Abstract: Staatliche Hochschulen sind nicht auf eine Auftragsdatenverarbeitung durch Anbieter mit Sitz im Europäischen Wirtschaftraum (EWR) beschränkt. Auch auf die Anbieter aus Drittstaaten kann zurückgegriffen werden, wenn die Auftragsdatenverarbeitung den gesetzlichen Anforderungen genügt und ein angemessenes Datenschutzniveau gewährleistet ist. Die restriktiven Normen aus den deutschen Datenschutzgesetzen sind europarechtskonform auszulegen. Der bloße Abschluss einer Auftragsdatenverarbeitung allein ist aber noch keine Grundlage zur Datenerhebung, sodass es daneben immer auch einer Einwilligung oder anderen rechtlichen Grundlage bedarf. Hochschulintern sind zudem der datenschutzrechtliche Freigabeprozess, die Mitbestimmung durch den Personalrat und gesetzliche wie vertragliche Pflichten zur Geheimhaltung bei der Dienstnutzung zu beachten.

1 Hintergrund

Die Digitalisierung stellt die Hochschulen und Forschungseinrichtungen vor die große Herausforderung ihre IT im Idealfall ohne zu große zusätzliche finanzielle Belastungen zu modernisieren und weiter zu professionalisieren.

Zum einen sind die Ansprüche der Lehrenden und Studierenden gestiegen. Sie erwarten von den Hochschulen, dass sie ihnen sämtliche notwendige Software und Services komfortabel und jederzeit an jedem Ort zur Verfügung stellen. Fragen zum Studium werden als Videoantworten gewünscht und Lehre und Prüfungen sollen ortsunabhängig jederzeit online, multimedial und in ansprechender Form möglich sein.

Zum anderen werden Verwaltungsvorgänge digitalisiert, während mehr und mehr rechtliche Vorgaben es erfordern, IT-Sicherheit auf hohem Niveau zu gewährleisten.

Bei so vielen Wünschen und Anforderungen sind schnell die personellen Ressourcen und Kapazitäten der Serverräume wie auch der technischen Infrastruktur universitärer Rechenzentren erschöpft.

Um auch der politisch gewollten Digitalisierung der Hochschulen gerecht zu werden, liegt es eigentlich nahe, geeignete Dienste an Drittanbieter auszulagern. Doch genau hier stoßen Hochschulen und Forschungseinrichtungen an rechtliche Grenzen. Denn bei dem Versuch Antworten auf die Frage nach der rechtlichen Zulässigkeit bei der "Cloud" aus Drittstaaten zu erhalten, heißt es schnell: „Schwierig bis unmöglich“. Das mag der sicherste Weg sein, doch auch der Schritt in diese Cloudangebote kann rechtssicher gelingen.[1] Dafür leistet dieser Beitrag eine Hilfe.

[1] In diese Sinne auch von dem Bussche in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 4b BDSG, Rn. 18.

2 Grundvoraussetzungen

Die Datenschutzgesetze sollen verhindern, dass der Umgang mit personenbezogenen Daten zu einer Beeinträchtigung des Persönlichkeitsrechtes von Betroffenen führt.[2]

Im Anwendungsbereich liegen damit nur personenbezogene Daten Betroffener.[3] Dies sind alle Daten, die einen Personenbezug ermöglichen können, d.h. eine Person identifizierbar machen könnten. Dafür ist auch Zusatzwissen Dritter relevant, das vernünftiger Weise herangezogen werden kann, insbesondere öffentlich zugängliche Informationen und gesetzlich oder vertraglich rechtmäßig zustehende Auskunftsrechte.[4] Daher empfiehlt es sich in Zweifelsfällen einen Personenbezug anzunehmen.

Die deutschen Datenschutzgesetze verlangen bei jedem Umgang mit personenbezogenen Daten entweder eine gesetzliche Erlaubnis oder eine Einwilligung.[5] Fehlt es an einer dieser alternativen Voraussetzungen, ist der Umgang mit personenbezogenen Daten unzulässig.[6]

Darüber hinaus ist neben dem Gebot der Datensparsamkeit[7] insbesondere der Zweckbindungsgrundsatz von entscheidender Bedeutung. Dieser besagt: Bereits mit der Erhebung von personenbezogenen Daten ist im Regelfall der Zweck der Datenverarbeitung festzulegen.[8]

Betroffene haben um den Umgang mit Ihren Daten kontrollieren zu können, besondere Rechte gegenüber den Stellen, die für den Umgang mit den Daten verantwortlich sind.

Diese Rechte umfassen Auskunft, Berichtigung, Löschung oder Sperrung der Daten,[9] deren Ausübung die Datenschutzbehörden für Betroffene im Konfliktfall durchsetzen können.[10] Insbesondere vor diesem Hintergrund sind die Gesetze so ausgestaltet, dass die verantwortliche Stelle grundsätzlich nicht die Hoheit über die Daten verlieren soll. Soweit die verantwortliche Stelle im Rahmen ihrer Tätigkeit Dritte einspannt, diese aber in Kontakt mit personenbezogenen Daten kommen, bedarf es einer vertraglichen Absicherung für den Umgang mit den Daten. Diese vertragliche Absicherung ist in den Gesetzen als Auftragsdatenverarbeitung ausgestaltet.[11] Eben dieser Vertragstyp ermöglicht es in vielen Fällen auch Dienste aus der Cloud zu nutzen. Gleichzeitig bleibt die Art des Einsatzes in der Verantwortung des Auftraggebers, denn die Verarbeitung und Nutzung von Daten erfolgt durch Weisungen.

Die Alternative zur Auftragsdatenverarbeitung, die Funktionsübertragung, bringt nur dann eine Erleichterung, wenn die Daten nicht mehr von der ursprünglich verantwortlichen Stelle verarbeitet oder genutzt werden müssen, da anderenfalls jeder weitere Daten(rück)fluss einer erneuten Legitimation bedürfte,[12] und somit kaum einen Anwendungsbereich für Dienstleistungen aus einer Public-Cloud schaffen kann.

---

[2] § 1 BDSG, Art. 1 BayDSG.
[3] § 2 Abs.1 BDSG, Art. 4 Abs. 1 BayDSG.
[4] EuGH, Urteil vom 19.10.2016 - C-582/14.
[5] §. 4 Abs. 1 BDSG, Art. 15 Abs. 1 BayDSG.
[6] Statt aller BeckOK DatenSR/Bäcker BDSG § 4 Rn. 21.
[7] § 3a BDSG.
[8] Allgemeiner Grundsatz, spätestens seit BVerfGE 65, 1-71.
[9] § 6 BDSG, Art. 10 – 13 BayDSG.
[10] § 38 BDSG, Art. 31 BayDSG.
[11] § 11 BDSG, Art. 6 BayDSG.
[12] Gola/Schomerus/Gola/Klug/Körffer BDSG § 11 Rn. 9, beck-online; Ehman in Wilde/Ehmann/Niese/Knoblauch Datenschutz in Bayern Art. 6 BayDSG Rn. 10.

Damit wird auch deutlich, dass ein Transfer von Daten in Staaten, die Betroffenen keinen gleichartigen Datenschutz gewähren wie das Land mit dem Sitz der verantwortlichen Stelle es bietet, nur unter besonderen Vorrausetzungen zulässig sein kann.[13]

Aufgebrochen wird dieses Konzept durch die Verträge zur Europäischen Union und die darauf aufsetzende europäische Regulierung, die auch den Handel mit Daten deutlich in den Vordergrund rückt.[14] Die zukünftige Datenschutzgrundverordnung räumt zwar dem Datenschutz mehr Gewicht ein,[15] bleibt aber dem Grundsatz treu, dass durch die Regulierung Datenhandel ermöglicht und aufrechterhalten werden soll.[16] Die Mitgliedschaft in der europäischen Union hat für die Rechtsanwendung zur Folge, dass diese die bestmögliche Zur-Geltung-Bringung von Unionsrecht erzielen muss.[17]

Vor diesem Hintergrund ergibt sich in letzter Konsequenz, dass, soweit unionsrechtlich eine Verarbeitung von personenbezogen Daten in Auftrag zulässig ist, diese auch im deutschen Recht zu ermöglichen ist; gegebenenfalls unter zu Hilfenahme aller zulässigen Auslegungsmethoden.[18] Einzig, wenn das Unionsrecht den Mitgliedsstaaten eine Abweichung zubilligt oder außerhalb seines Anwendungsbereiches liegt, greift dieser Mechanismus bei der Umsetzung der Datenschutzrichtlinie nicht ein.[19]

3 Europarechtliche Betrachtung

3.1 Richtlinienbeeinflusster Bereich der Regelung

Zunächst ist festzuhalten, dass die Richtlinie 95/46/EG (künftig bezeichnet als „Datenschutzrichtlinie“) keine ausdrückliche Regelung zu der Frage hat, ob mit ihr nur ein Mindeststandard im Datenschutz sichergestellt werden soll oder eine Vollharmonisierung angestrebt ist. Mit Blick auf die häufige Verwendung von Worten wie „zumindest“ bei Informations-[20], Auskunfts-[21] und Widerspruchsrechte[22] liegt eher eine Mindestharmonisierung nahe. Ebenso ist für die Mitgliedsstaaten ein Spielraum vorgesehen.[23] Andererseits legt der Erwägungsgrund 7 der Datenschutzrichtlinie eher nahe, dass unterschiedlich hohe Schutzniveau der Zielerreichung der Richtlinie, nämlich den Handel mit Daten zu erleichtern, entgegenstehen würde.

Die Rechtsprechung des EuGH hat sich diesbezüglich seit 2003[24] hin zu einer durch die Richtlinie verfolgten umfassenden Harmonisierung positioniert.

[13] Art. 4c BDSG, Art. 21 BayBSG.
[14] Art. 16 Abs. 2 AEUV; Erwägungsgrund 56 Richtlinie 95/46/EG.
[15] Erwägungsgrund 1 Verordnung (EU) 2016/679.
[16] Erwägungsgrund 101, Art. 1 Abs. 3 Verordnung (EU) 2016/679.
[17] Art. 4 Abs. 3 EUV; Groeben, von der /Schwarze/Walter Obwexer EUV Art. 4 Rn. 116-119.
[18] Calliess/Ruffert/Ruffert, 5. Aufl. 2016, AEUV Art. 1 Rn. 24; Herresthal EuZW 2007, 396 (400).
[19] Grabitz/Hilf, Das Recht der EU, Vorbemerkung: Datenschutz und die Europäische Gemeinschaft Rn. 45 - 52, beck-online.
[20] Art. 11 Datenschutzrichtlinie.
[21] Art. 12 Datenschutzrichtlinie.
[22] Art. 14 Datenschutzrichtlinie.
[23] Erwägungsgrund 9 der Datenschutzrichtlinie.
[24] EuGH Urteil vom 6. November 2003 – Rs. C-101/01; EuGH Urteil vom 24. November 2011 – Rs. C‑468/10 und C‑469/10.

Damit geht einher, dass sich der den Mitgliedstaaten zur Verfügung stehende Spielraum nur auf die Ausgestaltung bezieht, jedoch nicht den Umfang einer zulässigen Datenverarbeitung begrenzen darf.[25] Die Begriffsdefinitionen der Datenschutzrichtlinie sind erst recht bindet, da anderenfalls die angestrebte Rechtsangleichung hinfällig wäre.

3.2 Datenschutzrichtlinie

Die Datenschutzrichtlinie definiert den Dritten in Art. 2:

> *„"Dritter" die natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten;“*

Nach dieser Definition ist ein Auftragsverarbeiter im Rahmen der Auftragstätigkeit niemals Dritter. Der Sitz des Auftragnehmers ist relevant für die Frage, ob eine Übermittlung in Drittstaaten erfolgt. Aus Art. 4 Abs. 2 wird ersichtlich, dass es für Anbieter aus Drittstaaten nur erforderlich ist, einen in einem Mitgliedstaat der Europäischen Union ansässigen Vertreter zu benennen, falls Daten im Hoheitsgebiet vorgehalten werden.

Wann welche nationalen Datenschutzgesetze Anwendungen finden, ist in seinen Feinheiten komplex ausgestaltet und die Auswirkungen aus der Rechtsprechung des EuGH[26] wohl noch nicht gänzlich durchdrungen. Im Grundprinzip entscheidet sich das „ob“ nach dem anwendbaren Recht für die Behörde, das „wie“ nach dem Datenschutzrecht der europäischen Niederlassung des Cloud-Anbieters.[27]

Die Richtlinie enthält keine Definition für den Begriff der Übermittelung.[28] Für die Frage, ob eine Übermittlung vorliegt, spielt es keine Rolle, ob Daten zu einem „Dritten“ transferiert werden.[29] Der Begriff ist somit im Kontext der Definition des Verarbeitens aus Art. 2 lit. b vielmehr eher technisch zu verstehen, jedoch bedarf es Eingrenzungen, um einen uferlosen Anwendungsbereich der Richtlinie zu verhindern.[30]

Art. 25 ermöglicht die Übermittlung personenbezogener Daten in Drittstaaten, wenn dort ein angemessenes Schutzniveau gewährleistet ist.

Auch ohne dass dieses vorliegt, können Daten bei Vorliegen geeigneter Garantien in Drittstaaten übermittelt werden gemäß Art. 26 Abs. 2. Als eine solche Garantie werden auch die von der EU-

[25] Grabitz/Hilf, Das Recht der EU, Vorbemerkung: Datenschutz und die Europäische Gemeinschaft Rn. 45 - 52; Hören, RDV 2009, 89 (94f).
[26] Z.B. EuGH, Urteil v. 13.05.2014, Az. C-131/12.
[27] Art. 3 Abs. 1 b) Datenschutzrichtlinie.
[28] EuGH Urteil vom 6. November 2003 - Rechtssache C-101/01 Rn. 56.
[29] Grabitz/Hilf, Das Recht der EU, Art. 2 Rn. 24, beck-online.
[30] EuGH Urteil vom 6. November 2003 - Rechtssache C-101/01 Rn. 56.

Kommission beschlossen Standardvertragsklauseln angesehen.[31] Diese liegen in drei verschiedenen Fassungen vor,[32] wobei im Bereich Cloud Computing die 2010 verabschiedeten Klauseln am weitesten verbreitet sind.[33]

Eine Alternative für die Praxis zu den Standardvertragsklauseln den Datentransfer in die USA zu ermöglichen, ist das EU-U.S. Privacy Shield.[34] Ist ein Unternehmen auf der Datenschutzschild-Liste gemäß Art. 1 Abs. 3 Durchführungsbeschluss (EU) 2016/1250 aufgeführt, bedarf es zwar immer auch noch des Abschlusses einer Vereinbarung über eine Datenverarbeitung im Auftrag,[35] die Standardvertragsklauseln müssen aber dafür nicht zwingend verwendet werden.

Soweit Daten unternehmensintern auch in Drittstaaten übertragen werden, können auch sogenannte Binding Corporate Rules einen angemessenen Datenschutz gewährleisten. Die Anzahl an Unter-nehmen mit von den Datenschutzbehörden genehmigten Binding Corporate Rules ist überschau-bar.[36]

Für die Auftragsdatenverarbeitung sieht die Datenschutzrichtlinie vor, dass diese durch Dienstleister auf der ganzen Welt erfolgen kann. Außerhalb des EWR sind aber die genannten zusätzlichen Schutzmechanismen, [37] z.B. der Einsatz von Standardvertragsklauseln, notwendig. Ein Unternehmen mit weltweiten Niederlassungen kann seinen internen Datentransfer mittels Binding Corporate Rules absichern.

3.3 Standardvertragsklauseln

Soweit der Einsatz von Standardvertragsklauseln nach dem EU-Kommissions-Beschluss 2010/87/EU beabsichtigt ist, bedürfen zwei Punkte einer besonderen Berücksichtigung.

Der Mustervertrag darf gemäß Klausel 10 Standardvertragsklauseln (Auftragsverarbeiter) grundsätzlich nicht verändert werden. Deshalb ist es hilfreich, wenn zum Beispiel im Vertrag sichergestellt ist, dass die Standardvertragsklauseln in Zweifelsfällen stets vorrangig sind.

Eine Möglichkeit sich vor unzulässigen Abänderungen der Standardvertragsklauseln zu schützen, kann ähnlich den Mustern der „bitkom“ zur Auftragsdatenverarbeitung nach BDSG gelingen mit Formulierungen im Vertrag wie:

[31] Grabitz/Hilf, Das Recht der EU, Art. 26 Rn. 21, beck-online; BeckOK DatenSR/Schantz BDSG § 4c Rn. 42-46, beck-online.
[32] EU-Kommission, Entscheidung v. 15.6.2001 (K(2001) 1539); EU-Kommission, Entscheidung v. 27.12.2004 (K(2004) 5271) und EU-Kommissions-Beschluss 2010/87/EU.
[33] So nutzen z.B. Amazon http://www.cnpd.public.lu/en/actualites/international/2015/03/AWS/index.html , Dropbox https://www.dropbox.com/privacy#business_agreement und Microsoft https://www.microsoft.com/en-us/TrustCenter/Compliance/EU-Model-Clauses diese Klauseln.
[34] Durchführungsbeschluss (EU) 2016/1250 der Kommission.
[35] So auch explizit unter 10. a. i. Anhang II „Grundsätze des EU-US-Datenschutzschilds vorgelegt vom amerikanischen Handelsministerium“ Durchführungsbeschluss (EU) 2016/1250 der Kommission.
[36] Eine Liste der Unternehmen ist abrufbar unter: http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm .
[37] Art. 26 Datenschutzrichtlinie; Grabitz/Hilf, Das Recht der EU, Vorbemerkung zu Art. 26, beck-online.

Deutsch: Bei etwaigen Widersprüchen gehen Regelungen der vereinbarten EU-Standardvertragsklauseln den Regelungen des geschäftlichen Vertrages vor.

English: In case of any conflict, the regulations of the EU-Model Clauses as contractually agreed shall take precedence over the regulations of the Business Agreement.

Der zweite kritische Punkt sind die Anhänge, die für eine wirksame Auftragsdatenverarbeitung für den jeweiligen Vertrag passend und vollständig auszufüllen sind. Nicht jeder Cloud-Anbieter bietet sie bereits vollständig vorausgefüllt an. Sie können jedoch nur mit Kenntnis der technischen Infrastruktur und Sicherheitsfeatures des Anbieters vervollständigt werden.

3.4 Artikel 29-Gruppe

In der Stellungnahme[38] der Artikel 29-Gruppe, deren Aufgabe es ist, öffentliche Stellungnahmen zu Datenschutzfragen aus unionsrechtlicher Sicht abzugeben, werden nur Anforderung für Cloud Computing festgelegt. Von einer grundsätzlichen Zulässigkeit kann damit ausgegangen werden.

3.5 Datenschutzgrundverordnung

Auch die DSGVO ändert diese Systematik nicht. Im Unterschied zum bisherigen Recht, ist jedoch nicht der jeweils nationale Gesetzgeber gehalten, Auftragsdatenverarbeitung (nach dem Termini der DSGVO Verarbeitung im Auftrag) zu ermöglichen, sondern die Verarbeitung im Auftrag ist durch Unionrecht unmittelbar vorgesehen.[39]

Neu ist, dass nun die Anforderungen an die Sicherheit der Verarbeitung einheitlich vorgegeben sind[40] und zur Prüfung der Einhaltung dieser Anforderung auch Zertifizierungen als Faktor mitherangezogen werden können.[41]

Die bisherigen Entscheidungen der Kommission, wie z.B. zur Angemessenheit des Datenschutzes in Drittstaaten, zum EU-US Privacy Shield oder zu den Standardvertragsklauseln, gelten bis zum Erlass neuer Durchführungsrechtsakte fort.[42]

Auch das Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU) baut auf den Definition der DSGVO auf.

---

[38] Abrufbar z.B. unter: https://www.lda.bayern.de/media/wp196_de.pdf .

[39] Hier hat die DSGVO eine dogmatische Schwäche. So kann die Verarbeitung im Auftrag gemäß Art. 28 DSGVO als unionsrechtliche Rechtsgrundlage gemäß Art. 6 Abs. 3 lit. a DSGVO für Art. 6 Abs. 1 lit. c DSGVO angesehen werden (so wohl Ehmann in: Datenschutz in Bayern, Kommentar Art. 28 DSGVO S. 1f) oder auch das jeder Form der Verarbeitung nach Art. DSGVO auch als Verarbeitung im Auftrag möglich ist (so z.B. Plath in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 28 DSGVO, Rn. 3). Dass wegen der der fehlenden rechtlichen Eindeutig, die Verarbeitung im Auftrag nicht möglich sei, wird nicht ernsthaft vertreten. Dies zeigt sich auch bei der Auslegung von Schmidt/Freund ZD 2017, 14 (14-16).

[40] Art. 32 DSGVO; Eine Abweichung von diesen Anforderungen sieht auch die Öffnungsklausel in Art. 6 Abs. 2, 3 DSGVO nicht vor. Siehe auch Plath in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 6 DSGVO, Rn. 25.

[41] Art. 28 Abs. 5, 6 DSGVO; siehe auch Plath in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 28 DSGVO, Rn. 15.

[42] Art. 45 Abs. 9; 46 Abs. 5 DSGVO.

4 Betrachtung der Auftragsdatenverarbeitung nach BDSG

4.1 Auslegung am Gesetzestext BDSG

Das BDSG folgt einer anderen Systematik als die Datenschutzrichtlinie und enthält eigene Begriffsdefinitionen.

Ausgangspunkt sind die im Gesetz angelegten Definitionen sowie die Gesetzessystematik. Jeder Umgang mit Daten bedarf einer gesetzlichen Grundlage (Rechtsvorschrift) oder einer Einwilligung.[43] Das Gesetzt unterscheidet die Phasen des Umgangs mit personenbezogenen Daten in Erhebung, Verarbeitung und Nutzen.[44]

Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten, § 3 Abs. 4 Nr. 1 BDSG.

Nach § 3 Abs. 6 S. 2 BDSG sind Dritte nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

Cloudcomputing ist somit möglich, wenn die Tätigkeit des Cloudanbieters im Rahmen einer Auftragsdatenverarbeitung im EWR erfolgt. Eine Privilegierung der Auftragsdatenverarbeitung in Drittstaaten ist nicht vorgesehen. Vielmehr ist die Übermittlung nur in den engen Ausnahmen der §§ 4b, 4c BDSG möglich.[45]

Neben der Frage, ob überhaupt übermittelt werden darf, muss zudem die Übermittlung auf Basis der Einwilligung der Betroffenen oder einer Rechtsvorschrift erfolgen.[46]

Da bei einer Einwilligung aber das Risiko besteht, dass diese nicht wirksam erklärt worden ist und sie zudem jederzeit widerrufen werden kann, eignet sich eine Einwilligung nur selten als taugliche Grundlage für einen Datentransfer im Rahmen einer Auftragsdatenverarbeitung.[47]

Und für Behörden gibt es, anders als für nicht öffentliche Stellen, keine Generalklausel ähnlich dem § 28 Abs. 1 S. 1 Nr. 2 BDSG, über die ein Datentransfer ohne Einwilligung möglich wäre.[48]

Im Ergebnis ist öffentlichen Stellen (soweit nur nach Wortlaut und Systematik betrachtet) die Wahl eines Cloudanbieters aus Drittstaaten verwehrt. Einzig günstig an dieser Betrachtung ist, dass der Serverstandort des Anbieters in keiner Weise maßgeblich wäre, denn innerhalb einer verantwortlichen Stelle kann nicht „übermittelt“ werden.

[43] § 4 Abs. 1 BDSG; statt aller Gola/Schomerus/Körffer/Gola/Klug BDSG § 4 Rn. 3 beck-online.
[44] § 3 Abs. 3-5 BDSG.
[45] Von dem Bussche in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 4b BDSG, Rn. 16f.
[46] § 4 Abs. 1 BDSG; statt aller Gola/Schomerus/Körffer/Gola/Klug BDSG § 4 Rn. 3 beck-online.
[47] Simitis in: Simitis Bundesdatenschutzgesetz (2014), § 4a Rn. 94; Borges, Borges/Meents Cloud Computing (2016), S. 287 Rn. 35.
[48] § 28 BDSG steht im dritten Abschnitt „Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen“. Der Umgang mit personenbezogen Daten soll für Unternehmen flexibler sein als für Behörden; vgl. Simitis in: Simitis Bundesdatenschutzgesetz, § 27 Rn. 2.

4.2 Auffassung der Datenschutzbehörden

Die Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben eine „Orientierungshilfe – Cloud Computing“[49] erstellt.

Diese Position bleibt nahe an Wortlaut und Systematik, ermöglicht allerdings für **nicht öffentliche Stellen** die Datenübermittlungen außerhalb des EWR über § 28 Abs. 1 S. 1 Nr. 2 BDSG,[50] sofern die Anforderung des § 4c BSDG erfüllt sind; d.h., unter anderem nur mit Einwilligung oder Garantien wie nach den Standardvertragsklauseln. Als Alternative kann nach § 4b Abs. 2 BDSG ein angemessenes Datenschutzniveaus festgestellt werden, in der Regel durch Entscheidung der EU Kommission.[51]

Bezogen auf die Landesdatenschutzgesetze heißt es dort:

> „Soweit öffentliche Stellen Cloud Services in Drittstaaten anwenden, ist hier eine besonders sorgfältige Prüfung geboten, denn ein dem § 28 Abs. 1 Satz 1 Nr. 2 BDSG entsprechender Erlaubnistatbestand dürfte es in den Landesdatenschutzgesetzen nicht geben, soweit ersichtlich. Die Verfasser dieser Orientierungshilfe haben allerdings keine Prüfung aller Landesdatenschutzgesetze vorgenommen.“

Somit trifft die Orientierungshilfe keine Aussage darüber, ob Cloud-Computing für Behörden außerhalb des Europäischen Wirtschaftsraumes möglich ist.

4.3 Weitere Auffassungen

4.3.1 Restriktive Auslegungen

Einige Auffassungen bleiben beim Wortlaut und sind dabei teilweise noch einschränkender bei der Interpretation berechtigter Interessen im Rahmen von § 28 Abs. 1 S. Nr. 2 BDSG.

So sieht Simitis[52], dass § 28 Abs. 1 S. 1 Nr. 2 BDSG nur in Ausnahmenfällen eine Auftragsdatenverarbeitung rechtfertigt. Dammann[53] sieht eine europarechtliche Interpretation des Begriffes „Übermittlung“ nicht veranlasst, und lehnt eine analoge Anwendung von Art. 3 Abs. 8 BDSG ab.

Nach Weber und Voigt[54] sei Durchführung einer Verarbeitung im Auftrag von der Datenschutzrichtlinie auf den EWR beschränkt.

4.3.2 Rechtfertigung nach § 28 Abs. 1 S. 1 Nr. 2 BDSG

Ein großer Anteil der Stimmen wie die Landesdatenschutzbehörden (siehe 4.2), aber auch in der Literatur sieht die Möglichkeit der Rechtfertigung über § 28 Abs. 1 S. 1 Nr. 2 BDSG bei Cloudanbietern aus Drittstaaten. Erforderlich sind also Einwilligungen, alternativ ein angemessenes Datenschutzniveau oder ausreichenden Garantien vorliegen (siehe 3.2 und 3.5).[55]

---

[49] Abrufbar z.B. unter: https://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf .
[50] Orientierungshilfe – Cloud Computing, S. 16.
[51] Vgl. z.B. BeckOK DatenSR/Schantz BDSG § 4b Rn. 25-35, beck-online.
[52] Simitis in: Simitis Bundesdatenschutzgesetz (2014), § 28 Rn. 101.
[53] Dammann in: Simitis Bundesdatenschutzgesetz (2014), § 3 Rn. 246.
[54] Weber/Voigt, ZD 2011, 74 (77). Die sich jedoch Grundsätzlich die Möglichkeit einer internationalen Auftragsdatenverarbeitung bejahen über eine Analogie zu § 3 Abs. 8 BDSG (a.a.O. 78).
[55] Nachweise finden sich z.B. bei Borges, Borges/Meents Cloud Computing (2016), S. 232f Rn. 10.

4.3.3 Richtlinienkonforme Anwendung § 3 Abs. 8 BDSG

Neben einer unmittelbaren Anwendung der Richtlinie[56] wird im Hinblick auf die europarechtlichen Vorgaben entweder eine teleologische Reduktion vertreten oder eine analoge Anwendung der Norm bei der Verarbeitung personenbezogener Daten im Auftrag mit Sitz des Anbieters in Drittstaaten vorgeschlagen.[57]

Diese Autoren erblicken eine planwidrige oder überschießende Regelung in § 3 Abs. 8 BDSG, sowie eine vergleichbare Interessenlage, insbesondere wenn die Standardvertragsklauseln die Diensterbringung zu Grunde liegen. Diese Auslegung sei auch unionsrechtlich geboten.[58]

5 Betrachtung nach BayDSG

Die Begriffsdefinitionen entsprechen – soweit hier relevant – dem BDSG, jedoch sind die Übermittlungsmöglichkeit von Daten auch an nicht öffentliche Stellen im Art. 21 Abs. 2 S. 4 Nr. 3 BayDSG weitergefasst als im BDSG. Allerdings findet sich kein passender Anknüpfungspunkt für eine Übermittlung von Daten im Rahmen von Cloud Computing mit Bezügen zu Drittstaaten, denn mit dieser Norm sollte im Wesentlichen nur die Datenschutzrichtlinie umgesetzt werden[59], die primär für den Fall internationaler Überweisungen gedacht ist[60].

5.1 Auffassung des Bayerischen Landesbeauftragte für den Datenschutz

Im 25. (2012) Tätigkeitsbericht des Bayerischen Landesbeauftragten für den Datenschutz wird bei der Inanspruchnahme von Cloud Diensten äußerste Zurückhaltung angemahnt.[61] Diese Einschätzung wurde im 26. (2014) und 27. (2016) Tätigkeitsbericht aufrechterhalten.[62]

5.2 Weitere Auffassung

Für die Landesdatenschutzgesetze ist die Literaturlage überschaubar. Im Kommentar „Datenschutz in Bayern“ heißt es lapidar: „Gerade ein Cloud Computing unter Einschaltung von Drittstaaten ist für öffentliche Stellen in aller Regel keine realistische Option.“[63]

Die Meinungen und Argumentationen, die für das BDSG vorgebracht werden, sind aber übertragbar, da die Begriffsdefinitionen des BayDSG, soweit hier relevant, denen des BDSG entsprechen.

[56] Kahler, RDV, 2012, 167 ff.
[57] Nachweise bei Borges, Borges/Meents Cloud Computing (2016), S. 233 Rn. 11.
[58] Borges, Borges/Meents Cloud Computing (2016), S. 234f Rn. 12.
[59] Bayerischer Landtag, Drucksache 14/3327, S. 14.
[60] Grabitz/Hilf, Das Recht der EU, Art. 26 Rn. 8.
[61] Punkt 2.3.3. abrufbar unter https://www.datenschutz-bayern.de/ .
[62] 26. Tätigkeitsbericht 2014 Punkt 13.1. https://www.datenschutz-bayern.de/tbs/tb26/k13.html#13.1 und 27. Tätigkeitsbericht 2016 Punkt 13.3, abrufbar unter https://www.datenschutz-bayern.de/tbs/tb27/k13.html#13.3 .
[63] Ehmann in: Wilde/Ehemann/Niese/Knoblauch Datenschutz in Bayern, 26. EL – Stand Oktober 2016, Art. 6 BayDSG Rn. 3g.

6 Eigene Stellungnahme

Folgt man den restriktiven Ansichten, steht Behörden oft keine praxistaugliche Möglichkeit zur Verfügung, auf Cloud-Computing von Anbietern außerhalb des EWR zurückzugreifen. Da auch in Unteraufträgen der Schutz des Hauptvertrages nicht unterschritten werden darf, kann nicht auf Leistungen von Konzernen mit Töchtern eigener Rechtspersönlichkeiten zurückgegriffen werden, denn der Datenschutz kennt (noch) kein Konzernprivileg.

Ein Verzicht auf eine Korrektur des Begriffs des Dritten, verbunden mit einer großzügigeren Auslegung des § 28 BDSG, verändert die datenschutzrechtliche Ausgangssituation für Behörden nicht, da es für den öffentlichen Bereich an einer dem § 28 BDSG entsprechenden Vorschrift fehlt.

Ein Verharren auf dem deutschen Begriff der „Übermittlung“ führt aber zu der perplexen Situation, dass innerhalb einer jeweils zuständigen Stelle der Speicherort der Daten nicht relevant wäre, da innerhalb einer Stelle nicht übermittelt werden kann. Somit könnte eine Hochschule Server in Pjöngjang oder Minsk mieten, aber keinen Updateservice und Remotesupportvertrag mit Netzwerkausrüstern aus Drittstaaten, wie HPE oder Cisco, oder mit Softwareanbietern aus Drittstaaten, wie Microsoft oder VMWare, abschließen. Der von der Richtlinie gewollte sicherere Rechtsrahmen, dass, überall dort wo die Daten mit den Daten umgegangen werden, auch ein angemessener Datenschutz gewährleistet wäre, könnte unterlaufen werden.[64]

Um das Schutzniveau der Datenschutzrichtlinie im nationalen Datenschutzrecht umzusetzen, bleibt einzig der Weg die Definition des Dritten unionsrechtlich bedingt zu modifizieren und wie folgt anzuwenden: „Dritte sind nicht der Betroffene sowie Personen und Stellen, ~~die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum~~ personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.“

Gleichzeitig muss der Begriff der Übermittlung in § 4b und § 4c BDSG, bzw. z.B. Art. 21 BayDSG europarechtlich ohne Bezug auf die Definition im BDSG bzw. BayDSG verstanden werden. Das bedeutet, dass auch z.B. die Miete eines Servers außerhalb des EWR als Übermittlung aufgefasst wird.

Die Begründung für diese beiden Begriffskorrekturen liegt in der Pflicht, das Unionsrecht durch Auslegung des nationalen Rechts bestmöglich zur Geltung zu bringen.[65] Schon mit der Datenschutzrichtlinie wurde in Europa ein gleichwertiges Schutzniveau geschaffen, und die in der Richtlinie vorgesehenen Begriffe stehen im Rahmen der Umsetzung einer Richtlinie dem nationalen Gesetzgeber nicht zur Disposition.[66]

Das Ergebnis der unionsrechtskonformen Auslegung des deutschen Datenschutzrechts ist: Auch öffentliche Behörden sind nicht auf eine Auftragsdatenverarbeitung durch Anbieter mit Sitz im EWR beschränkt. Auch auf die Dienste aus Drittstaaten kann zurückgegriffen werden.

[64] Dies verdeutlicht auch Erwägungsgrund 10 Datenschutzrichtlinie.
[65] Siehe dazu bereits die Ausführungen unter 2.
[66] Gebot effektiver Umsetzung: Herdegen, Europarecht (2016), § 8 Rn. 41-45.

7 Umsetzung

Allein aus der Tatsache, dass es sich juristisch gut vertreten lässt, dass Clouddienste auch bei einem Bezug zu Drittstaaten für Behörden genutzt werden können, bleibt die Herausforderung bestehen die gesetzlichen Anforderungen der Auftragsdatenverarbeitung vollständig umzusetzen. **Ohne und ohne korrekte Auftragsdatenverarbeitung liegt stets eine unzulässige Datenübermittlung vor.**[67]

Im Allgemeinen gelten z.B. für bayerische staatliche Hochschulen und die Akademie der bayrischen Wissenschaften die Anforderungen aus Art. 6 BayDSG, für Universitäten des Bundes und Vereinigungen des Privatrechts die Anforderungen aus § 11 BDSG. Für Religionsgesellschaften finden, insbesondere wenn für sie als Körperschaften des öffentlichen Rechts agieren, weder Bundes- noch Landesdatenschutzgesetze Anwendung, da diese keine des Bundes oder der Länder sind.[68] In Deutschland haben sich die Bistümer der katholischen Kirche, wie auch die evangelischen Landeskirchen Datenschutzordnungen gegeben, die im Wesentlichen Regelungen des BDSG aufgreifen.[69] Im katholischen Datenschutz lassen sich Strafvorschriften bei Datenschutzverstößen wenigstens für gravierende Verstöße im Zusammenspiel von Can. 1399[70] und Can. 220 konstruieren.[71] Ein Vergleich der Landesdatenschutzgesetze zeigt eine Skepsis des Gesetzgebers, sofern die Auftragsdatenverarbeitung bei nicht-öffentlichen Stellen stattfindet.[72]

Zwar findet bereits durch die Datenschutzrichtlinie für den Auftragsdatenverarbeiter im Grundsatz nur das Datenschutzrecht an seiner Niederlassung Anwendung. Aber durch die Wahl der Standardvertragsklauseln wird vertraglich die (eingeschränkte) Anwendung des Datenschutzrechts des Auftraggebers vereinbart. Dies führt für internationale Anbieter zu allein in Deutschland mindestens 19 unterschiedlichen anwendbaren Datenschutzgesetzen.

7.1 Absicherung internationaler Datentransfers

Die Rechtsprechung des Europäischen Gerichtshofs erfordert, dass Beschlüsse für die Angemessenheit des Datenschutzniveaus in Drittstaaten regelmäßig zu überprüfen sind.[73] Da die politischen Voraussetzungen nicht immer berechenbar sind, ist es nicht ratsam einen internationalen Datentransfer nur minimalistisch abzusichern. Zudem sind nicht alle Entwicklungen der Rechtsprechung vorhersehbar.

Sollten also Datentransfers nur auf Basis der Standardvertragsklausen oder einer Auftragsdatenverarbeitung mit EU-US Privacy Shield abgesichert sein, könnte es durch ein einziges Urteil des EUGH veranlasst sein, den Datentransfer zu stoppen. Dies ist auch mit ein Grund dafür, trotz der Verwendung von Standardvertragsklauseln zusätzlich noch eine Auftragsdatenverarbeitung in Verträge aufzunehmen.

---

[67] Dies bezüglich, ergingen auch bereits Urteile: z.B. VG Wiesbaden, DuD 2015, 262-265; auch haben Datenschutzbehörden erste Bußgelder für Verträge mit Inhaltlichen Mängeln festgesetzt. https://www.lda.bayern.de/media/pm2015_11.pdf .

[68] Diese Frage ist umstritten. Vgl. Gola/Schomerus/Körffer/Gola/Klug BDSG § 2 Rn. 14a m.w.N., sowie Preuß ZD 2015, 217 (218 ff.).

[69] Preuß ZD 2015, 217 (223).

[70] Ausführlich dazu Max Ortner, Die Entwertung des Gesetzlichkeitsprinzips und des Analogieverbotes durch die Generalnorm des Kanon 1399 des CIC/1983 (2017).

[71] Diese Besonderheit des kirchlichen Strafrechts wird häufig übersehen, so wohl z.B. Preuß ZD 2015, 217 (223).

[72] Vgl. z.B. § 11 Abs. 3 DSGNRW oder § 4 Abs. 4 RLP LDSG.

[73] EuGH, Urteil vom 06.10.2015, C-362/14 (Schrems) Rn. 76.

7.2 Mindestinhalte der Verträge bei internationalen Datentransfers

Durch die Standardvertragsklauseln, die auch kompatibel zu den in Deutschland anwendbaren Datenschutzgesetzen ausgestaltet werden können, hat sich ein auch bei den Auftragsdatenverarbeitern akzeptiertes Vertragsmuster etabliert. Besonderheiten der deutschen Landesdatenschutzgesetze und des BDSG können in der Anlage 1 unter dem Punkt Datenverarbeitung mit Gegenstand, Dauer, Umfang, Ort und Zweck, Unteraufträgen, Weisungsbefugnissen und Rückgabe überlassene Datenträger und Löschung von Daten abgebildet werden.[74] Durch die Integration dieser Anforderungen wird im Regelfall auch den Anforderungen der Landesdatenschutzgesetze genügt.

Eine Besonderheit für Behörden, sofern auf die Kontrollen aus der Anlage zu § 9 BDSG zurückgegriffen wird, ergibt sich mit Blick auf die Datenschutzgesetze aus dem Erfordernis einer zusätzlichen Kontrolle hinsichtlich der Organisation des Datenschutzes, so z.B. Art. 7 Abs. 2 Nr. 10 BayDSG. Auftragsdatenverarbeiter, die diese zusätzlich zu den Kontrollen, wie sie das BDSG kennt, aufnehmen, erleichtern den behördlichen Datenschutzbeauftragten so ihre Prüfung, hinsichtlich der Übereinstimmung mit den jeweils anzuwendenden Landesdatenschutzgesetzen.

Auch wenn viele Landesdatenschutzgesetze, wie auch das Standarddatenschutzmodell, sich nun an Zielen statt an allgemeinen Maßnahmenkatalogen orientieren, dürfte in vielen Fällen ein Vertrag, in dem die Kontrollen des BDSG gewissenhaft umgesetzt sind, für viele Anwendungsfälle ausreichen.

Bis es genehmigte Verhaltensregeln und Datenschutzzertifizierungen nach der DSGVO geben wird, liegt es nahe, sich ab Geltung der DSGVO an Kontrollen aus ISO 27002 zur Erfüllung der technischen und organisatorischen Maßnahmen zur Datensicherheit zu orientieren.[75]

7.3 Datenschutzbeauftragter

Für einen Auftragsdatenverarbeiter in Deutschland ist ein Datenschutzbeauftragter obligatorisch.[76] In Drittstaaten und teilweise sogar im EWR ist dieser erst mit der DSGVO für nahezu jeden Anbieter vorgeschrieben.[77] Daher ist es zu empfehlen, vertraglich gegenseitig die Datenschutzbeauftragten als Kontaktpersonen festzuhalten und über deren Wechsel und Verhinderungen zu informieren. Fehlt bei einem internationalen Auftragsdatenverarbeiter die Position des Datenschutzbeauftragten, bedarf es vor Geltung der DSGVO eines adäquaten Ersatzes durch den die Einhaltung und Durchsetzung der Pflichten gewährleistet werden kann. Ob dies dann auch den behördlichen Datenschutzbeauftragten bei seiner unabhängigen Entscheidung über die Freigabe des Verfahrens ausreicht, bleibt aber ungewiss.

[74] So von dem Bussche in: Moos, Datennutzungs-und Datenschutzverträge, 1. Aufl. 2014, III. EU-Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern.
[75] Dieses Vorgehen empfiehlt z.B. die renommierte ActiveMind AG in ihrem Mustervertrag zur Auftragsverarbeitung nach DSGVO, vgl. https://www.activemind.de/datenschutz/dokumente/av-vertrag/ .
[76] § 11 Abs. 4 Nr. 2 i.V.m. § 4 f BDSG.
[77] Art. 37 DSGVO.

7.4 Stand der Technik

Als Grundsatz aus dem deutschen Vertragsrecht gilt, dass, sofern nichts vereinbart ist, nur eine Leistung mittlerer Art und Güte geschuldet ist.[78] Wenn die datenschutzrechtlichen Anforderungen des Auftragsgebers nicht nur Mittelmaß sondern den Stand der Technik verlangen, wird dies ohne vertragliche Regelung vom Auftragnehmer nicht geschuldet. Technische und organisatorische Datenschutzmaßnahmen erfordern aber stets die Berücksichtigung des Stands der Technik.[79] Ein Abweichen nach unten – was ein höheres Risiko für die Sicherheit der Daten mit sich bringt – ist akzeptierbar, wenn die gewählte Maßnahme mit Blick auf die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen dennoch ein angemessenes Schutzniveau gewährleistet. In diese Abwägung werden auch Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung mit einbezogen. Entscheidend ist, dass es einer Begründung für ein Abweichen nach unten bedarf. Hier könnten ferner auch weitergehende Interessen wie Informationssicherheit oder der Schutz von Knowhow und Geheimnissen miteinfließen.

Gegenüber großen Cloudanbietern prüfen die Aufsichtsbehörden die Verträge. Bei Services sehen sie die Anforderungen des europäischen Datenschutzes hinsichtlich der Auftragsdatenverarbeitung oft als erfüllt an, sofern umfassende informationssicherheitsbezogene Zertifizierungen bestehen.[80] Bei Anbietern von Infrastructure as a Service (Iaas) sind jedoch teilweise die technischen und organisatorischen Maßnahmen nicht Gegenstand der Prüfung der Aufsichtsbehörden.

Auch der neue Standard für Bundesbehörden für die Auswahl von Cloudanbietern C5, der durch das BSI gemäß § 8 Abs. 1 S. 1 BSIG festgelegt worden ist, bietet anderen Behörden eine verlässliche Orientierung, dass bei Anbietern mit diesem Testat, die Datenverarbeitung unter der erforderlichen Berücksichtigung des Stands der Technik erfolgen kann.

8 Private Nutzung von Clouddiensten am Beispiel Office 365

Soweit Hochschulen Studierenden oder Beschäftigten zu privaten Zwecken Clouddienste von Anbieter aus Drittstaaten wie z.B. Microsoft Office 365 ohne oder gegen nur geringe Entgelte zur Verfügung stellen, bedarf es keiner Auftragsdatenverarbeitung, da in diesem Fall nur die Nutzenden die Betroffenen sind und somit eine Einwilligung gegenüber dem Anbieter ausreichend ist.[81]

Die Freiwilligkeit der Einwilligung der Studierenden steht nicht in Zweifel, sie können sowohl auf andere Anbieter als auch auf die „Offline“ Variante Microsoft Office 2016 ausweichen.[82]

Die Universität Bamberg bietet ihren Studierenden Exchange Online und Office 365 mit allen Funktionen an. Sofern jedoch Studierende dies nicht wünschen, steht ein eigenes universitäres E-Mail-Postfach zur Verfügung.[83]

---

[78] Meents, Borges/Meents Cloud Computing (2016), S. 100f Rn. 124.
[79] Erwägungsgrund 46 und Art. 17 Abs. 1 Datenschutzrichtlinie.
[80] Siehe z.B. https://www.blog.google/topics/google-cloud/eu-data-protection-authorities-confirm-compliance-google-cloud-commitments-international-data-flows/ .
[81] So auch Borges, Borges/Meents Cloud Computing (2016), S. 286 Rn. 33.
[82] Spindler/Nink in Spindler/Schuster Recht der elektronischen Medien (2015) BDSG § 4a Rn. 6, beck-online.
[83] https://www.uni-bamberg.de/rz/dienstleistungen/mail/studium/altmailstud/ .

Ferner können Hochschulen die verfügbaren Features von Office 365 begrenzen, wie auch Einfluss darauf nehmen, welche Informationen über Nutzende übertragen werden.

So kann Office 365 auf die Möglichkeit beschränkt werden, dass nur die Installationsdateien der Desktopversion und die Nutzung der Apps auf Tablets und Smartphones möglich ist. Nutzeraccounts beinhalten nur zufällige Buchstaben und Zahlen sowie die Domain; weder Vor- noch Nachname werden an Microsoft übermittelt.[84] Ähnlich datenschutzsparsam kann über diesen Ansatz auch z.B. Azure oder AWS weiterverfolgt werden.

Es zeigt sich also, dass für einzelne Anwendungsszenarien das Übermitteln von Daten sehr gut mit Einwilligungen gelingen kann und zugleich datensparsame Modifikationen möglich sind.

9 Anforderungen bei dienstlicher Nutzung von Clouddiensten

Soweit jedoch ein dienstlicher Einsatz von Office 365 beabsichtigt ist, kann, selbst wenn man unterstellt es lägen wirksame Einwilligungen der Nutzenden vor, nicht ausgeschlossen werden, dass personenbezogene Daten Dritter an den Cloudanbieter übermittelt werden (z.B. Bilder Dritter bei der Nutzung von Adobe Creative Suite, Adressdaten in Briefentwürfen zu Office Online, Kontakte zu Google- oder Appledienssten).

Die Frage, ob bei der Einführung und Nutzung eines Clouddienstes der mitbestimmungspflichtige Teil des Personals an Hochschulen betroffen ist,[85] wird im Regelfall zu bejahen sein, soweit Rechenzentren z.B. für Administration mitverantwortlich sind oder Verwaltungskräfte den Dienst mitnutzen.[86] Es bietet sich daher an, eine Dienstvereinbarung über die Einführung und Nutzung von Clouddiensten abzuschließen, da diese dann den Umgang mit den personenbezogenen Daten in der Cloud anstelle einer Einwilligung rechtfertigen kann.[87] Diese erstreckt sich jedoch nicht auf den von der Mitbestimmung ausgenommen Personenkreis. Ohne eine Einwilligung können deren personenbezogene Daten für Clouddienste nur im Rahmen des BayDSG oder anderer Rechtsvorschriften erhoben, verarbeitet und genutzt werden.

Zwar können Satzungen von Körperschaften des öffentlichen Rechts eine solche Rechtsvorschrift darstellen, jedoch muss bereits aus der Ermächtigungsgrundlage der Eingriff in die Grundrechte der Betroffenen erkennbar sein.[88] Soweit sich der Umgang mit personenbezogenen Daten für die Aufgaben z.B. eines Rechenzentrums bei der Nutzung von IT aufdrängt, dürfte z.B. die Ermächtigungsgrundlage des Bayerischen Hochschulgesetztes[89] für Satzungen tauglich sein um auch die damit verbundenen Eingriffe in Grundrechte als Erlaubnisnorm rechtfertigen. Die Eingriffsintensität wird erheblich durch die Pflichten des Diensteanbieters zu technischen und organisatorischen

[84] https://www.rz.uni-wuerzburg.de/dienste/shop/studierende/software_fuer_studierende/microsoft_office/ .
[85] Art. 4 Abs. 4 BayPVG über den Professoren und Professorinnen (Art. 2 Abs. 1 S. 1 Nr. 1 BayHSchPG), Juniorprofessoren und Juniorprofessorinnen (Art. 2 Abs. 1 S. 1 Nr. 2 BayHSchPG), Wissenschaftliche Mitarbeiter und Mitarbeiterinnen mit Weiterqualifizierungsaufgaben (Art. 22 Abs. 3 BayHSchPG).
[86] Soweit es sich nicht um (bayerische) staatliche Hochschulen handelt, kann der Kreis der mitbestimmungspflichtigen Personen auch größer sein, und wissenschaftlicher Mitarbeiter miterfassen.
[87] Ehman in WILDE/EHMANN/NIESE/ KNOBLAUCH Datenschutz in Bayern Art. 15 Rn. 12 BayDSG.
[88] So Bäcker in BeckOK DatenSR 18. Ed. 1.5.2016, BDSG § 4 Rn. 12. Vgl. auch zur ähnlichen Situation bei Informationsfreiheitssatzungen Bay VGH, Beschluss vom 27.02.2017, Az. 4 N 16.461.
[89] Art. 19 Abs. 5 S.5 BayHSchG. Eine solche Satzung oder Ordnung kann jedoch nicht dazu eingesetzt werden, die Mitbestimmungspflicht des Personalrates zu umgehen.

Datenschutzmaßnahmen[90], Datenschutzbeauftragen, Freigaben und Verfahrensverzeichnissen[91] sowie inzwischen auch Informationssicherheitskonzepten[92] abgemildert.

Die Legitimationswirkung von Dienstvereinbarung und Hochschulsatzung endet im Regelfall aber stets dort, wo auch personenbezogene Daten nicht satzungsmäßiger Mitglieder der Hochschule zu einem Clouddienst verlagert werden. Der Umgang mit diesen personenbezogenen Daten bedarf einer eigenständigen Legitimation. Die Fiktion, dass an einen Auftragsdatenverarbeiter im Rahmen der Auftragsdatenverarbeitung die Daten nicht übermittelt werden, bleibt dann der einzige Weg den zusätzlichen Datenfluss zum Auftragsdatenverarbeiter zu legitimieren. Aus diesem Grund ist grundsätzlich eine Auftragsdatenverarbeitung erforderlich, es sei denn, die Nutzung z.B. bei Office 365 wird auf die Möglichkeit beschränkt, dass nur die Installationsdateien der Desktopversion verfügbar sind und die Nutzung der Apps auf Tablets und Smartphones ohne Zugriff auf OneDrive möglich ist.

10 Geheimnisschutz

10.1 Aktuelle Rechtslage

Aus dem Blick kann auch geraten, dass viele Informationen aus der Hochschule dem Dienstgeheimnis[93], dem Amtsgeheimnis[94] oder dem Geheimnisschutz für Dritte[95] unterliegen. Ein Lösungsansatz kann sein, dass Daten nur im verschlüsselten Zustand in der Cloud liegen, sofern die Verschlüsselung dem Stand der Technik entspricht und die Schlüsselverwaltung allein in der Verfügungsgewalt der Hochschule bleibt.[96] Die Alternative für die öffentliche Verwaltung ist, dass das Personal des Anbieters förmlich verpflichtet wird und die gesetzliche Pflicht zum Geheimnisschutz besteht.[97] Der teilweise vertretene großzügigere Gehilfenbegriff[98] löst die Probleme nur für Berufsgeheimnisträger, erfasst aber nicht den Bereich des Geheimnisschutzes bei Tätigkeiten für die öffentliche Verwaltung. Bei einer mutigeren Gesetzesauslegung könnte angenommen werden, dass keine unbefugte Offenbarung von Dienstgeheimnissen im Rahmen einer Auftragsdatenverarbeitung erfolgt.[99] Für eine praktikablere, rechtssichere Lösung, welche die Reichweite des Tatbestandes beschränkt, hat der Bundestag am 29. Juni 2017 eine Reform des § 203 StGB auf Grundlange des Regierungsentwurfs [100] auf den Weg gebracht. Demnächst können Vertraulichkeitsvereinbarungen mit den Anbietern Strafbarkeitsrisiken beseitigen.

[90] Art. 7 BayDSG.
[91] Art. 25-28 BayDSG.
[92] Art. 8 Abs.1 BayEGovG.
[93] § 353b StGB.
[94] Art. 30 BayVwVfG; § 30 VwVfG.
[95] § 203 Abs. 2 StGB, ggf. auch § 17 UWG.
[96] Thalhofer in Auer-Reinsdorff/Conrad, IT- und Datenschutzrecht, Teil C. Software-, Hardware- und Providerverträge § 19 Outsourcing-Verträge Rn. 227-230; Spickhoff in: Spickhoff Medizinrecht (2014) § 205 StGB Rn. 23.
[97] § 11 Abs. 1 Nr. 2 c StGB; Schünemann in Leipziger Kommentar (2009) § 203 StGB Rn. 44.
[98] Preuß, DuD 2016, 802 (806).
[99] So z.B. Pohle, Kommunikation und Recht, 2013, 34 (35).
[100] BT-Drs 18/11936.

10.2 Rechtslage unter der DSGVO

Eine explizite Vorschrift für den Umgang mit durch besondere Geheimnispflichten geschützte, personenbezogene Daten findet sich in der DSGVO abgesehen von satzungsmäßigen Berufsgeheimnisträgern[101] nicht. Allerdings werden diese erwähnt.[102] Die Mitgliedstaaten können regeln, welche Einrichtung oder Behörde Aufsicht über die Einhaltung des Datenschutzes dieser speziellen personenbezogenen Daten wahrnimmt. Für den behördlichen Bereich wird anzunehmen sein, dass § 203 Abs. 2 StGB den zulässigen Tätigkeitsbereich von Auftrags(daten)verarbeitern weiterhin einschränkt,[103] da Geheimnisschutz und Datenschutz zwar Überschneidungen aufweisen, in ihrer Zielsetzung aber unterschiedlich sind.[104]

10.3 Fazit zum Geheimnisschutz

Die Verantwortung Geheimnisschutz zu gewährleisten liegt bei der Behörde selbst und ist eine vom Datenschutz unabhängige Pflicht. Während es gesetzliche Vorgaben für die Verlagerung von personenbezogenen Daten zu Auftragsdatenverarbeitern gibt, ist zum Schutz vor dem Offenbaren von Geheimnissen im gesetzlichen Grundfall zukünftig eine Vertraulichkeitsvereinbarung vorgesehen. Sind personenbezogene Daten zugleich auch Geheimnisse, nimmt die DSGVO ferner an, dass oft ein höherer Schaden im Falle einer Verletzung des Schutzes personenbezogener Daten vorliegen wird, sodass solche Daten besonderer Schutzmaßnahmen bedürfen.[105]

11 Fazit

Auch öffentliche Behörden sind oft nicht auf eine Auftragsdatenverarbeitung durch Anbieter mit Sitz im EWR beschränkt. Es kann auch auf die Dienste aus Drittstaaten zurückgegriffen werden, wenn die Auftragsdatenverarbeitung vertraglich richtig und umfassend geregelt ist. Zertifizierte Dienstleister, die bereit sind, ihre Leistung mit für öffentliche Stellen geeigneten Auftragsdatenverarbeitungsverträge oder mit vollständigen EU-Standardvertragsklauseln anzubieten, ebnen einen rechtssichern Weg in die Cloud.

Daneben bleiben interne Herausforderungen durch Freigabe, Mitbestimmung und Geheimnisschutz. Dies zeigt, dass weder kostenfreie Dienste noch bei Verbrauchern favorisierte Produkte stets eine Lösung für den Einsatz an Hochschulen sind sobald eine dienstliche Nutzung erfolgen soll. Um einen guten Kompromiss zu finden, sind die Hochschulen gefragt ihre Anforderungen zur Auftragsdatenverarbeitung klar zu kommunizieren. Auch nach Innen ist eine Sensibilisierung nötig um Bewusstsein für Dienste zu schaffen, die der Gesetzmäßigkeit der Verwaltung genügen (Neudeutsch auch „Compliance“ genannt).

Inhalt, Form und Kontrolle der Auftragsdatenverarbeitung geben die Gesetze vor. Wirksamen Verträgen stehen jedoch oft formelle und inhaltliche Fehler in den Vertragsmustern der Diensteanbieter entgegen. Hiervor können auch Zertifizierungen nicht schützen. Ein erster Schritt zur Fehlervermeidung ist das GÉANT IaaS Vergabeverfahren, ein zweiter die Rechtsvereinheitlichung durch die DSGVO.

---

[101] Art. 14 Abs. 5 d DSGVO.
[102] Erwägungsgrund 50 DSGVO.
[103] So Preuß, DuD 2016, 802 (808).
[104] Dies wird sehr deutlich in den Erwägungsgründen 18 und 35 Richtlinie (EU) 2016/943 und 63 DSGVO.
[105] Erwägungsgrund 76 DSGVO; Plath in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Artikel 24 DSGVO Rn. 7.