

Datenschutzrechtliche Vorgaben für eine E-Learning-Videoplattform

Anne Lauber-Rönsberg*

*TU Dresden

Abstract

Der Beitrag fasst die datenschutzrechtlichen Rahmenbedingungen zusammen, die bei der Auswahl einer konkreten Videoportallösung und während ihres Einsatzes im Rahmen der Hochschullehre zu berücksichtigen sind. Dabei geht er insbesondere auf die Zulässigkeit von Datenverarbeitungen im Rahmen von Lernmanagementsystemen (LMS) auf Grundlage gesetzlicher Erlaubnisnormen oder mit Einwilligung des Betroffenen ein. Zudem werden weitere datenschutzrechtliche Anforderungen an die technische und organisatorische Ausgestaltung einer Videoplattform erörtert. Der Beitrag kommt zu dem Ergebnis, dass der Aufbau einer Videoplattform speziell für die Hochschullehre zwar im Vergleich zu der Nutzung bestehender unentgeltlicher Angebote wie bspw. YouTube aufwändiger, aus datenschutzrechtlichen Gründen aber geboten ist.¹

1 Eigener Videocampus oder bestehende Videoplattformen?

Ob Hochschulen im Rahmen ihrer Lernmanagementsysteme (LMS) einen hohen datenschutzrechtlichen Standard gewährleisten, wird mittlerweile von der Öffentlichkeit genau beobachtet. Dies zeigt die Verleihung des Negativ-Preises *Big Brother Award* an die LMU München und die TU München im Mai 2017 als Kritik an ihrer Kooperation mit dem US-amerikanischen MOOC-Anbieter Coursera, der nicht nur umfangreiche Daten über die Teilnehmer der Onlinekurse erhob, sondern diese auch an Arbeitgeber oder Recruiting-Unternehmen übermittelt [1] [2].

Im Rahmen von E-Learning-Angeboten werden regelmäßig personenbezogene Daten von Studierenden, Dozentinnen und Dozenten erhoben, bspw. Bestandsdaten wie Namen und E-Mail-Adressen, oder Nutzungsdaten, bspw. Informationen über den Abruf von zur Verfügung gestellten Dateien. Der rechtliche Rahmen für die Erhebung und Verarbeitung personenbezogener Daten durch die Hochschulen ergibt sich grundsätzlich aus dem jeweiligen Landesdatenschutzgesetz, d.h. hier dem Gesetz zum Schutz der informationellen Selbstbestimmung im Freistaat Sachsen (SächsDSG), soweit nicht speziellere Regelungen – wie bspw. das Telemediengesetz (TMG) – eingreifen. Ab dem 25.05.2018 wird das nationale Datenschutzrecht weitgehend durch die Datenschutz-Grundverordnung (DSGVO)² der Europäischen Union

-
- 1 Für Informationen zu den urheberrechtlichen Rahmenbedingungen siehe Lauber-Rönsberg/Bergert/Hartlaub „Der Videocampus Sachsen – Strategische Potenziale und juristische Rahmenbedingungen“, abrufbar unter <http://nbn-resolving.de/urn:nbn:de:bsz:105-qucosa-208267> (Stand: 9.01.2018).
 - 2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum

verdrängt. Der Bundesgesetzgeber hat bereits die erforderliche Reform des BDSG beschlossen; die geänderten Regelungen werden ebenfalls ab dem 25.05.2018 anwendbar sein. Die Anpassungen der landesrechtlichen Regelungen befinden sich noch im Gesetzgebungsverfahren.³

Die datenschutzrechtlichen Regelungen verpflichten die Hochschulen dazu, angemessene personelle, technische und organisatorische Maßnahmen zu treffen, um die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten. Wenn Hochschulen eine E-Learning-Plattform nicht selbst betreiben, sondern hierzu auf externe Anbieter im Rahmen einer sogenannten *Datenverarbeitung im Auftrag* zurückgreifen (§ 7 SächsDSG; zukünftig Art. 28 DSGVO), ist dies grundsätzlich zulässig. Allerdings bleiben die Hochschulen auch bei einer solchen Auslagerung für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich und sind u.a. dazu verpflichtet, den Auftragnehmer sorgfältig und unter besonderer Berücksichtigung der Eignung der von diesem getroffenen personellen, technischen und organisatorischen Maßnahmen auszuwählen, die einzuhaltenden datenschutzrechtlichen Standards durch vertragliche Vereinbarungen festzulegen sowie zu kontrollieren.

Rechtlich problematisch wird es jedoch dann, wenn Hochschulen ihre Lehrangebote über für den Nutzer unentgeltliche Videoplattformen zur Verfügung zu stellen, deren Geschäftsmodell darin besteht, Informationen über Nutzer zu sammeln, bspw. IP-Adressen, Nutzungsdaten oder gerätebezogene Informationen, die potenziell zu Persönlichkeitsprofilen zusammengeführt werden oder sogar eine Identifizierbarkeit des konkreten Nutzers ermöglichen können. Gemäß § 9 SächsDSG (zukünftig Art. 24 DSGVO) müssen die Hochschulen die Einhaltung der datenschutzrechtlichen Vorgaben durch technische und organisatorische Maßnahmen sicherstellen. In diesem Rahmen muss auch gewährleistet werden, dass nur Befugte personenbezogene Daten zur Kenntnis nehmen können. Es spricht vieles dafür, dass diese Pflicht verletzt würde, wenn die Zugänglichmachung prüfungsrelevanter Lehrveranstaltungen für die Studierenden über solche datenverarbeitenden Plattformen erfolgt, ohne dass eine gleichwertige Alternative zur Verfügung gestellt wird, so dass Studierende diese Lehrangebote nur um den Preis der Verarbeitung ihrer personenbezogenen Daten durch den Plattformbetreiber wahrnehmen könnten.

Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. EU L 119, 4.5.2016, http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=OJ:JOL_2016_119_R_0001.

3 Der Bundestag hat 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) am 27.04.2017 beschlossen, der Bundesrat hat ihm am 12.05.2017 zugestimmt. Die Sächsische Staatsregierung hat einen Gesetzesentwurf vom 29.09.2017 zur Anpassung der landesrechtlichen Vorschriften an die DSGVO vorgelegt (Sächsischer Landtag, Drucksache 6/10918).

Noch problematischer wäre es, wenn eine Hochschule bspw. eine Vorlesungsaufzeichnung, bei der einzelne Studierende erkennbar sind, über eine solche Videoplattform zugänglich macht. Wenn keine Vereinbarung mit dem Plattformbetreiber über eine „Datenverarbeitung im Auftrag“ geschlossen wurde, so stellt dies rechtlich eine Übermittlung der Daten an einen Dritten dar (§ 3 Abs. 2 Nr. 5 SächsDSG). Eine Übermittlung von Daten an externe nicht-öffentliche Stellen ist nur unter engen Voraussetzungen möglich. Sie ist nur dann zulässig, wenn die Daten rechtmäßig erhoben wurden [3] und dies zur Erfüllung der Aufgabe der Hochschule in Lehre und Forschung erforderlich ist, was in der Regel nicht der Fall ist.

Daher ist der Aufbau einer eigenen Plattform im Vergleich zu der Nutzung bestehender unentgeltlicher Angebote wie bspw. YouTube zwar aufwändiger, aus datenschutzrechtlichen Gründen aber geboten. Dies bedeutet jedoch nicht, dass jegliche Nutzung von Anbietern wie YouTube untersagt wäre. So ist es etwa zulässig, optionale Zusatzangebote außerhalb regulärer Lehrveranstaltungen, bspw. Aufzeichnungen wissenschaftlicher Vorträge oder an externe Teilnehmer gerichtete MOOCs, über solche Plattformen öffentlich zugänglich zu machen, wenn ihre Nutzung auf freiwilliger Basis erfolgt. Insofern hängt die Zulässigkeit der Nutzung vom jeweiligen Kontext ab. Jedoch stehen die gesetzlichen Vorgaben einer generellen Auslagerung der E-Learning-Aktivitäten durch eine Hochschule auf einen Videoplattformanbieter entgegen, der bei für die Studierenden obligatorischen Angeboten Daten der Studierenden erhebt und verarbeitet, um diese zu eigenen kommerziellen Zwecken zu verwerten. Wenn technische Möglichkeiten wie Vorlesungsaufzeichnungen auch im Rahmen obligatorischer Lehrveranstaltungen genutzt werden sollen, müssen Hochschulen daher auch aus datenschutzrechtlichen Gründen entweder eine eigene Infrastruktur aufbauen oder datenschutzkonforme Dienstleistungen gegen Entgelt in Anspruch nehmen.

2 Zulässigkeit von Datenverarbeitungen im Rahmen von LMS

Die Erhebung und Verarbeitung personenbezogener Daten stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen dar und ist nur dann zulässig, wenn entweder der Betroffene rechtswirksam eingewilligt hat oder wenn eine Rechtsvorschrift die Datenverarbeitung erlaubt (vgl. § 4 Abs. 1 SächsDSG; zukünftig Art. 6 DSGVO). Ohne eine solche Rechtfertigung ist die Erhebung und Verwendung personenbezogener Daten rechtswidrig und stellt eine Ordnungswidrigkeit dar (§ 38 Abs. 1 Nr. 1 SächsDSG). Die datenschutzrechtliche Verantwortung für Datenverarbeitungen im Rahmen von E-Learning-Verfahren tragen die jeweiligen Hochschulleitungen [4].

2.1 Datenverarbeitung mit Einwilligung der Betroffenen

Wenn die Datenverarbeitung im Rahmen von E-Learning-Plattformen nicht durch eine Rechtsvorschrift erlaubt wird (dazu s.u. 2.2), ist sie nur zulässig, wenn der Betroffene einwilligt.

Die Anforderungen an eine wirksame Einwilligung ergeben sich aus § 4 Abs. 3-5 SächsDSG bzw. § 12 Abs. 1 TMG. Die Einwilligung muss zum Ersten den jeweiligen formellen Anforderungen entsprechen, d.h. nach § 4 Abs. 4 und 5 SächsDSG schriftlich erfolgen, soweit nicht im Einzelfall wegen besonderer Umstände eine andere Form angemessen ist, oder durch die mit einer qualifizierten elektronischen Signatur verbundene elektronische Form bzw. nach § 13 Abs. 2 TMG durch elektronische Erklärung. Es spricht vieles dafür, dass bei E-Learning-Verfahren zur Vermeidung eines Medienbruchs eine Ausnahme von dem Schriftformerfordernis gemacht werden kann. Dies ist jedoch bislang nicht abschließend geklärt und wird im Schrifttum z.T. anders beurteilt [5].

Zukünftig wird das Schriftformgebot durch Art. 7 DSGVO gelockert. Hiernach ist es lediglich erforderlich, dass der Verantwortliche nachweisen können muss, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat. Für sensible Daten – bzgl. der rassistischen oder ethnischen Herkunft, politischer Meinungen, religiöser oder philosophischer Überzeugungen oder der Gewerkschaftszugehörigkeit – gelten gemäß § 4 Abs. 2 SächsDSG (Art. 9 DSGVO) jedoch erhöhte Anforderungen.

Eine wirksame Einwilligung setzt zum Zweiten die vorherige Information über Umfang und Zweck der Datenverarbeitung voraus. Der Nutzer muss daher darüber informiert werden, welche seiner Daten bspw. gespeichert werden und wer darauf Zugriff hat (§ 4 Abs. 3 SächsDSG, § 13 Abs. 1 TMG, Art. 4 Nr. 11, Art. 7 und Erwägungsgrund 32 DSGVO).

Zum Dritten ist eine Einwilligung nur dann wirksam, wenn sie freiwillig erfolgt. Dies ist bspw. bei der Teilnahme Externer an MOOCs grundsätzlich zu bejahen, hingegen bei Pflichtveranstaltungen, die immatrikulierte Studierende belegen müssen, nicht der Fall. Hier liegt nur dann Freiwilligkeit vor, wenn eine gleichwertige Alternative zu dem Angebot besteht [6] [7] [8], also bspw. online zur Verfügung gestellte Materialien auch als analoge Kopiervorlage angeboten werden oder die Studierenden die Wahl haben, ob sie eine Videoaufzeichnung einer Lehrveranstaltung ansehen oder stattdessen eine (ggf. andere) Präsenzveranstaltung besuchen. Diese Grundsätze gelten auch unter der DSGVO, die für eine datenschutzrechtliche Einwilligung ebenfalls Freiwilligkeit voraussetzt (Art. 4 Nr. 11 DSGVO). Wenn keine gleichwertige Alternative angeboten wird, scheidet eine einwilligungsbasierte Datenverarbeitung im Rahmen der regulären Studienangebote grundsätzlich aus. Eine Datenverarbeitung wäre in diesem Fall nur dann rechtmäßig, wenn sie durch eine gesetzliche Er-

laubnisnorm gestattet wird (dazu s.u. 2.2.2). Im Gegensatz zu der Verarbeitung von Daten von Hochschulangehörigen ist in Bezug auf Externe, bspw. im Rahmen von MOOCs, eine einwilligungsbasierte Lösung unproblematischer möglich, da Freiwilligkeit in der Regel gegeben ist.

2.2 Datenverarbeitung auf gesetzlicher Grundlage

Die Verarbeitung personenbezogener Daten im Rahmen verpflichtender Studienangebote kann, wie soeben dargestellt, nicht durch eine Einwilligung der Betroffenen gerechtfertigt werden, sofern es keine gleichwertige Alternative zu dem E-Learning-Angebot gibt und die Einwilligung daher nicht freiwillig erfolgt. In diesen Fällen ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie gesetzlich erlaubt wird.

2.2.1 Datenverarbeitung für Studien- und Prüfungszwecke nach § 14 Abs. 1 SächsHSFG
Das Sächsische Hochschulfreiheitsgesetz enthält in § 14 Abs. 1 Nr. 1 und 2 SächsHSFG einen speziellen Erlaubnistatbestand für die Verarbeitung personenbezogener Daten durch die Hochschulen für Studien- und Prüfungszwecke.

Bislang war allerdings unklar, ob § 14 SächsHSFG eine ausreichend qualifizierte Erlaubnisnorm darstellt. Dies hängt davon ab, ob hier die Regelung des § 12 Abs. 2 TMG einschlägig ist, die bei Datenverarbeitungen zur Bereitstellung von Telemedien erhöhte Anforderungen an eine gesetzliche Erlaubnisnorm stellt. Nach § 12 Abs. 2 TMG ist die Verarbeitung personenbezogener Daten hier nur dann gestattet, wenn sie entweder durch das TMG selbst oder eine andere Norm, die sich ausdrücklich auf Telemedien⁴ bezieht, erlaubt wird. Da § 14 SächsHSFG nicht ausdrücklich auf Telemedien Bezug nimmt, ist diese Regelung nach diesen Maßstäben keine qualifizierte Erlaubnisnorm i.S. von § 12 Abs. 2 TMG.

Es ist allerdings streitig, ob die Regelungen des TMG auf den Einsatz von E-Learning-Systemen an Hochschulen anwendbar sind. Dies verneint der nordrhein-westfälische Datenschutzbeauftragte hinsichtlich der Verarbeitung personenbezogener Daten von Studierenden, Lehrenden und sonstigen Beschäftigten im Rahmen von E-Learning-Angeboten, bejaht dies allerdings für externe Dritte, die nicht in einer Sonderbeziehung zu der Hochschule stehen [6]. Ein Beispiel hierfür sind die nicht an einer Hochschule eingeschriebenen Teilnehmer eines frei zugänglichen MOOCs. Zumindest auf diesen Personenkreis finden daher die Vorschriften des TMG Anwendung mit der Folge, dass § 14 SächsHSFG als Erlaubnisnorm nicht ausreicht. In diesen Fällen bedarf es vielmehr einer wirksamen Einwilligung der Betroffenen (dazu oben 2.1), da die erforderliche Datenverarbeitung über die begrenzten Erlaub-

4 Siehe zum Begriff der Telemedien die Legaldefinition des § 1 Abs. 1 TMG.

nistatbestände des TMG⁵ hinausgeht. Nach der von beachtlichen Stimmen vertretenen Gegenansicht soll dagegen auch bei Studierenden und Hochschulangehörigen das TMG anwendbar sein⁶ mit der Folge, dass § 14 SächsHSFG mangels expliziter Bezugnahme auf Telemedien nicht als Erlaubnisnorm für eine Datenverarbeitung ausreichen würde. Folgt man dieser Rechtsansicht, so wäre die Erhebung und Verarbeitung personenbezogener Daten – bspw. die Speicherung von Bestandsdaten wie dem Namen oder der E-Mail-Adresse – im Rahmen von E-Learning-Angeboten grundsätzlich unzulässig, soweit mangels Freiwilligkeit keine wirksame Einwilligung erfolgen kann, also bspw. bei Pflichtveranstaltungen, soweit keine gleichwertigen Alternativen angeboten werden.

Aufgrund der unsicheren Rechtslage haben eine Reihe von Hochschulen Regelungen in Form von Hochschulsatzungen erlassen, die explizit auf Datenverarbeitungen durch Lernmanagementsysteme Bezug nehmen⁷, auch vor dem Hintergrund, dass in anderen Bundesländern zum Teil keine mit § 14 SächsHSFG vergleichbare Erlaubnisnorm existiert. Jedoch ist bislang unklar, inwieweit das Fehlen einer qualifizierten Erlaubnisnorm durch den Erlass untergesetzlicher Normen, die den Anforderungen des § 12 Abs. 2 TMG genügen, tatsächlich geheilt wird, und ob dieses Vorgehen dem Wesentlichkeitsgrundsatz genügt, nach dem wesentliche Grundrechtseingriffe nur durch ein formelles Gesetz gerechtfertigt werden können.⁸

Es spricht vieles dafür, dass sich diese Problematik jedoch im Zuge der Anpassungen des nationalen Rechts an die DSGVO durch eine zu erwartende Aufhebung der

5 Dazu im Einzelnen: Forschungsstelle Recht im DFN: Datenschutz bei E-Learning-Plattformen, Stand Juli 2014, https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Datenschutz_bei_E-Learning-Plattformen.pdf, S. 4 f.

6 So Forschungsstelle Recht im DFN: Datenschutz bei E-Learning-Plattformen (s.o. Fußnote 5), S. 2 ff.; Roßnagel/Schnabel: Datenschutzkonforme Nutzung von E-Learning-Verfahren an hessischen Hochschulen (s.u. Endnote 7), S. 22; Bischoff: E-Learning und Datenschutz an Hochschulen (s.u. Endnote 5), S. 57.

7 Soweit ersichtlich gilt dies u.a. für die Universität Kassel (Satzung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren vom 1.6.2009, https://www.uni-kassel.de/einrichtungen/fileadmin/datas/einrichtungen/scl/LLukas/E-Learning-Satzung_2009.pdf); die Universität Marburg (Satzung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren vom 13.09.2010, <https://www.uni-marburg.de/de/universitaet/administration/recht/satzung/e-learning-datenschutzsatzung.pdf>); die RWTH Aachen (Ordnung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren vom 30.09.2015, https://www.rwth-aachen.de/global/show_document.asp?id=aaaaaaaaaoolwek) und die Bergische Universität Wuppertal (Ordnung zum Schutz personenbezogener Daten beim Einsatz von E-Learning-Verfahren vom 10.10.2012, <http://www.zim.uni-wuppertal.de/wirueber-uns/ordnungen/datenschutz-e-learning.html>).

8 Vgl. auch Forschungsstelle Recht im DFN: Datenschutz bei E-Learning-Plattformen (siehe Fußnote 5), S. 6.

Regelungen der §§ 11 ff. TMG – einschließlich des § 12 Abs. 2 TMG – erledigt wird.⁹ Maßgebliche Erlaubnistatbestände für Datenverarbeitungen durch Hochschulen im Rahmen der Lehre sind zukünftig Art. 6 Abs. 1 lit. c) und lit. e) DSGVO, die gemäß der Öffnungsklausel des Art. 6 Abs. 2 DSGVO durch die Mitgliedstaaten weiter spezifiziert werden können. Der von der Sächsischen Staatsregierung vorgelegte Gesetzesentwurf vom 29.09.2017 zur Anpassung der landesrechtlichen Vorschriften an die DSGVO sieht dementsprechend vor, § 14 SächsHSFG im Wesentlichen unverändert beizubehalten. Sollte dies so kommen, so entfielen die Problematik, dass § 14 SächsHSFG den erhöhten Anforderungen des § 12 Abs. 2 TMG nicht genügt. Falls sich der Bundesgesetzgeber jedoch anders entscheiden und § 12 Abs. 2 TMG aufrecht erhalten sollte, so wäre kurzfristig der Erlass einer an die Erfordernisse des E-Learning angepassten Rechtsverordnung durch das Staatsministerium für Wissenschaft und Kunst (SMWK) auf Grundlage von § 14 Abs. 3 S. 1 und 2 SächsHSFG und mittelfristig eine Anpassung des § 14 SächsHSFG empfehlenswert.

2.2.2 *Umfang der gesetzlichen Ermächtigung*

Selbst wenn man die Erlaubnisnorm des § 14 SächsHSFG ungeachtet dieser Fragen für anwendbar hält, erweist sich jedoch der unzureichende Umfang der gesetzlichen Erlaubnisnormen als äußerst problematisch. § 14 Abs. 1 Nr. 1 und Nr. 2 SächsHSFG gestatten u.a. die für Studien- und Prüfungszwecke erforderlichen Datenverarbeitungen. Welche Daten im Einzelnen verarbeitet werden dürfen, ist nach § 14 Abs. 3 SächsHSFG durch das SMWK zu bestimmen. Allerdings hat das SMWK von dieser Verordnungsermächtigung nur sehr begrenzt Gebrauch gemacht. Die Sächsische Hochschulpersonendatenverordnung vom 20.10.2017 (SächsHSPersDatVO) [9], die mittlerweile die Sächsische Studentendatenverordnung aus dem Jahr 2000 (Sächs-StudDatVO) [10] ersetzt¹⁰, ist ebenso wie ihre Vorgängerin sehr restriktiv gefasst.

9 So geht Marosi, Johannes: Das TMG vor und nach der DSGVO – was bleibt, was kommt, in: Specht/Lauber-Rönsberg/Becker (Hrsg.), Medienrecht im Medienumbruch, 2017, S. 225, 241 f. davon aus, dass §§ 13-16 TMG mit dem Inkrafttreten der DSGVO weitgehend aufgehoben werden müssen, äußert sich aber nicht zum Schicksal des § 12 TMG. Ebenso Sydow, in: Sydow, Gernot: Europäische Datenschutzgrundverordnung, 1. Auflage 2017, Einleitung Rn. 43.

10 Allerdings hielt der Sächsische Datenschutzbeauftragte die SächsStudDatVO für nicht mehr rechtswirksam, da die nach Art. 75 Abs. 1 SächsVerf erforderliche, in der Verordnung anzugebende gesetzliche Ermächtigungsgrundlage für den Erlass der SächsStudDatVO, § 106 Abs. 1 S. 3 des Sächsischen Hochschulgesetzes (SächsHSG) von 1999, mit der Neufassung des SächsHSFG im Jahr 2009 aufgehoben wurde, siehe 17. Tätigkeitsbericht des Sächsischen Datenschutzbeauftragten, Landtags-Drucks. 6/2562, S. 153 f. Gegen diese Ansicht spricht jedoch, dass nach herrschender Ansicht in Rechtsprechung und Schrifttum (bspw. Remmert, Barbara, in: Maunz, Theodor/Dürig, Günther: Grundgesetz-Kommentar, 78. EL September 2016, Art. 80 Rn. 51 ff. m.w.N.) eine Rechtsverordnung auch dann weiterhin in Kraft bleibt, wenn die gesetzliche Ermächtigungsgrundlage aufgehoben oder inhaltlich geändert wird, es sei denn, die Rechtsverordnung wäre

Die Verordnung regelt abschließend, welche Daten für bestimmte Zwecke erhoben und verarbeitet werden dürfen. § 7 SächsHSPersDatVO gestattet Datenerhebungen und -verarbeitungen zur Durchführung von Prüfungsverfahren gemäß § 14 Abs. 1 Satz 1 Nr. 2 SächsHSFG. Dagegen enthält die SächsHSPersDatVO keine Bestimmung über Datenerhebungen und -verarbeitungen zur Durchführung des Studiums gemäß § 14 Abs. 1 Satz 1 Nr. 1 SächsHSFG. Dies ist vor dem Hintergrund problematisch, dass es bei der Nutzung von E-Learning-Plattformen selbst bei einer datensparsamen Ausgestaltung aus technischen Gründen sowie zur Gewährleistung der Datensicherheit zu Datenerhebungen kommen kann, bspw. zu einer vorübergehenden Speicherung von IP-Adressen, die nach der Rechtsprechung des Europäischen Gerichtshofs grundsätzlich als personenbezogene Daten einzuordnen sind [11]. Eine solche Datenerhebung wird durch die SächsHSPersDatVO nicht abgedeckt, sofern sie nicht auch für die Durchführung von Prüfungsverfahren erforderlich ist, und ist daher nur mit Einwilligung des Betroffenen zulässig, die – wie oben unter 2.1 dargestellt – Freiwilligkeit voraussetzt und etwa bei obligatorischen Lehrangeboten ohne gleichwertige Alternative nicht in Betracht kommt. Damit schafft die Verordnung keine adäquaten Rahmenbedingungen für einen breiteren Einsatz moderner Lerntechnologien.

Folglich ist eine Anpassung der Rechtsverordnung wünschenswert, um die Möglichkeiten neuer Technologien auch in der Hochschullehre rechtssicher nutzen zu können und den Einsatz von Lernmanagementsystemen auch unabhängig von dem Freiwilligkeit erfordernden Einverständnis der Betroffenen zu ermöglichen. Zudem ist in diesem Rahmen auch die durch Art. 5 Abs. 3 GG grundrechtlich geschützte Lehrfreiheit zu berücksichtigen, die auch die Freiheit der Methodenwahl umfasst [12] [13]. Hierbei sollte geregelt werden, dass eine Datenverarbeitung nicht nur für Immatrikulations- und Prüfungszwecke, sondern auch im Rahmen von E-Learning-Angeboten zulässig ist, da in diesen Fällen wie ausgeführt – unabhängig von Prüfungen – Datenerhebungen und -verarbeitungen anfallen können. Alternativ wäre es auch denkbar, eine eigenständige Rechtsverordnung für den Einsatz von E-Learning an sächsischen Hochschulen zu erlassen. Falls der Bundesgesetzgeber im Rahmen der Anpassung der nationalen Regelungen an die DSGVO sich dazu entschließen sollte, die Regelung des § 12 Abs. 2 TMG beizubehalten, sollte im Rahmen

nach Änderung des Gesetzes inhaltlich nicht mehr mit diesem zu vereinbaren. Dies war hier aber nicht der Fall, da der restriktivere Wortlaut des § 14 Abs. 1 SächsHSFG, der auf die Erforderlichkeit der Daten abstellt, nicht zu einer gegenüber dem früheren § 106 Abs. 1 SächsHSG materiell veränderte Rechtslage führte, da eine solche Beschränkung auch schon nach alter Rechtslage nach dem allgemeinen Grundsatz der Erforderlichkeit der Datenverarbeitung sowie unter dem Gesichtspunkt der Verhältnismäßigkeit im Wege einer teleologischen Reduktion in die frühere Regelung hineinzulesen war.

dieser Anpassungen zugleich den Anforderungen des § 12 Abs. 2 TMG Rechnung getragen werden. Solange die (unter)gesetzlichen Rahmenbedingungen nicht angepasst wurden, sollte die Datenverarbeitung im Rahmen von E-Learning-Plattformen dagegen grundsätzlich nur mit Einwilligung der Betroffenen erfolgen.

Ausdrücklich festzuhalten ist an dieser Stelle auch, dass § 14 SächsHSFG und die SächsHSPersDatVO keine ausreichende Rechtsgrundlage dafür darstellen, um Studierende im Rahmen einer Vorlesungsaufzeichnung zu filmen, da die Verordnung keine Filmaufnahmen zu Unterrichtszwecken gestattet. Zudem ist eine solche Datenerhebung für Studien- und Prüfungszwecke in der Regel auch nicht notwendig und daher mit dem Grundsatz der Erforderlichkeit der Datenverarbeitung (dazu s.u. 3.2) nicht vereinbar. Insoweit ist eine Aufzeichnung grundsätzlich nur mit dem – Freiwilligkeit voraussetzenden – Einverständnis des Betroffenen zulässig.

3 Weitere rechtliche Anforderungen an die technische und organisatorische Ausgestaltung einer Videoplattform

3.1 *Kein Anbieter aus Drittstaat außerhalb der Europäischen Union*

Bei der Auswahl eines Betreibers von Videoportallösungen sollte ein in Deutschland oder zumindest in der Europäischen Union (EU) ansässiger Anbieter gewählt werden; auch die Datenverarbeitung sollte in Deutschland oder zumindest der EU erfolgen. Denn eine Übermittlung personenbezogener Daten in Drittländer ist grundsätzlich nur dann zulässig, wenn diese ein angemessenes Datenschutzniveau gewährleisten (§ 17 Abs. 1 und 2 SächsDSG). Dies gilt auch dann, wenn die Hochschulen eine andere öffentliche Stelle oder ein Unternehmen mit der Verarbeitung personenbezogener Daten im Rahmen einer Videoportallösung beauftragen. Denn gemäß § 7 Abs. 4 SächsDSG ist die Beauftragung eines Auftragnehmers, der Daten außerhalb der Europäischen Union verarbeitet, nur dann zulässig, wenn eine Übermittlung an ihn nach § 17 Abs. 1 SächsDSG gestattet wäre, d.h. wenn im Staat des Auftragnehmers ein angemessenes Datenschutzniveau besteht. Dies hat der Europäische Gerichtshof (EuGH) bspw. in seiner Safe-Harbor-Entscheidung vom 06.10.2015 für die USA verneint und die Übermittlung von Daten durch die irische Facebook-Tochter in die USA u.a. aufgrund der Überwachungspraktiken der US-amerikanischen Geheimdienste für unzulässig erklärt [14]. Offen ist derzeit, ob eine Datenübermittlung auf einer anderen rechtlichen Grundlage – bspw. mit Einwilligung des Betroffenen oder auf Grundlage der neuen Privacy Shield-Regelung – zulässig ist.

Nicht nur aufgrund der seit dieser Entscheidung bestehenden Rechtsunsicherheit, sondern auch wegen der hierdurch erhöhten Sensibilität der Thematik sollte ein Anbieter mit Sitz in Deutschland oder zumindest der EU ausgewählt werden, der auch die Datenverarbeitung in Deutschland oder der EU vornimmt.

3.2 Grundsatz der Erforderlichkeit der Datenverarbeitung

Nach dem Grundsatz der Erforderlichkeit der Datenverarbeitung (vgl. bspw. § 12 Abs. 1 SächsDSG) ist eine Verarbeitung personenbezogener Daten nur zulässig, soweit sie zur Erreichung des durch die Erlaubnisnorm vorgegebenen Zwecks notwendig ist. Steht eine datenschutzfreundlichere Alternative zur Verfügung, ist diese zu wählen [15]. Dieser Grundsatz wird in § 13 Abs. 6 TMG für Telemediendienste dahingehend konkretisiert, dass Diensteanbieter die Nutzung von Telemedien anonym oder unter Pseudonym zu ermöglichen haben, soweit dies technisch möglich und zumutbar ist.

Im Hinblick auf E-Learning-Angebote wird im Schrifttum die Auffassung vertreten, dass nur solche Daten von Studierenden erhoben werden dürfen, die „conditio sine qua non“, also unverzichtbar für die Durchführung der E-Learning-Anwendung sind. Hingegen soll es nicht ausreichen, dass die erhobenen Daten die E-Learning-Anwendung nur unterstützen oder fördern, indem sie bspw. Kommunikationsmöglichkeiten schneller und effektiver ausgestalten [16] [17]. Diese Auffassung erscheint jedoch angesichts der verfassungsrechtlich durch Art. 5 Abs. 3 GG geschützten Freiheit der Lehre zu restriktiv. Allerdings ist in jedem Einzelfall streng zu prüfen, inwieweit bestimmte Datenverarbeitungen tatsächlich zu einer Erleichterung oder Verbesserung der Lehre beitragen und in diesem Sinne erforderlich sind.

Auch die Erlaubnistatbestände des Art. 6 Abs. 1 lit. b)-f) DSGVO stehen unter dem Vorbehalt der Erforderlichkeit der Datenverarbeitung. Allerdings ist noch unklar, wie streng dieser Maßstab im Rahmen der DSGVO gehandhabt wird.

3.3 Grundsatz der Datenvermeidung und Datensparsamkeit

Nach dem Gebot der Datenvermeidung und Datensparsamkeit sind grundsätzlich so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen (§ 9 Abs. 1 S. 2 SächsDSG, § 3a BDSG). Soweit dies ohne unverhältnismäßigen Aufwand möglich ist, sind personenbezogene Daten zu pseudonymisieren oder zu anonymisieren. Der nordrhein-westfälische Datenschutzbeauftragte leitet in seiner Stellungnahme hieraus ab, dass Nutzerverhalten grundsätzlich nicht personenbezogen ausgewertet werden darf, insbesondere da die Erhebung von Nutzungsdaten nur in wenigen Ausnahmefällen erforderlich sei [18]. Inwieweit dies der Fall ist, hängt maßgeblich von den zur Verfügung gestellten Funktionen ab. Wenn eine E-Learning-Plattform letztlich nur als Videoplattform genutzt wird, so wäre wohl nur ein sehr eingeschränkter Funktionsumfang erforderlich. Sollen dagegen an die jeweilige Zielgruppe angepasste Informationsdienste (wie Benachrichtigungen, Informationen über Aktionen im System, Transparenz des Gruppenverhaltens) ermöglicht werden, so wären Dozentinnen und Dozenten häufig auf weitergehende Systemfunktionalitäten angewiesen [19]. Erforderlich wäre hier ein differenziertes

Rechte-Rollen-Konzept. Nach dem Grundsatz der Datensparsamkeit ist darauf zu achten, dass eine flexible, veranstaltungsbezogene Konfiguration möglich ist, um ein Nutzer-Tracking auszuschließen und entsprechende Datenerhebungen auf das im Einzelfall absolut erforderliche Minimum zu reduzieren [18] [19]. Die hierfür notwendigen Informationen sollten den Dozentinnen und Dozenten, die die Konfiguration vornehmen, in angemessener Form, bspw. durch Schulungen oder Informationsmaterial, vermittelt werden.

Um dem Grundsatz der Datensparsamkeit zu entsprechen, sind darüber hinaus angemessene Löschkonzepte zu entwickeln. Denkbar wäre bspw. das automatische Löschen von Inhaltsbereichen nach einem bestimmten *Verfallsdatum* [19].

Das Gebot der Datenminimierung gilt auch unter der DSGVO (Art. 5 Abs. 1 lit. c) DSGVO) [20]. Ausdrücklich weist die DSGVO darauf hin, dass diesem Gebot auch durch eine entsprechende Technikgestaltung und durch datenschutzfreundliche Voreinstellungen Rechnung zu tragen ist (Art. 25 DSGVO).

3.4 *Transparenz der Datenverarbeitungsvorgänge*

Zu beachten ist des Weiteren das Transparenzgebot (vgl. § 9 Abs. 2 Nr. 6 SächsDSG, § 13 Abs. 1 S. 3, Abs. 2 Nr. 3 TMG, Art. 13 DSGVO). Danach sind nach dem jeweiligen Stand der Technik geeignete Maßnahmen zu treffen, um zu gewährleisten, dass die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können. So sind die Nutzer der Videoplattform u.a. darüber zu unterrichten, welche Personen bzw. Personenkreise welche Daten einsehen oder verarbeiten können [19]. Gemäß § 13 Abs. 1 S. 3 TMG müssen diese Informationen für die Nutzer jederzeit abrufbar sein.

3.5 *Technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes*

Wie oben dargestellt, sind gemäß § 9 SächsDSG, § 13 Abs. 7 TMG alle angemessenen personellen, technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine datenschutzrechtskonforme Datenverarbeitung zu gewährleisten (zukünftig Art. 24 DSGVO). Dies beinhaltet die Verpflichtung zur Schaffung angemessener technischer und organisatorischer Rahmenbedingungen und anderer Maßnahmen nach dem jeweiligen Stand der Technik zur Sicherung der Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Revisionsfähigkeit gemäß § 9 Abs. 2 SächsDSG. Genauere Vorgaben ergeben sich aus der Anlage zu § 9 S. 1 BDSG sowie Richtlinien und Orientierungshilfen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Aufsichtsbehörden für den Datenschutz. Ein entsprechendes Konzept sollte in Abstimmung mit den Datenschutzbeauftragten

der Hochschulen entwickelt und umgesetzt werden. Eine hochschulübergreifende, standardisierte Vorgehensweise im Umgang mit videobasierten Inhalten im sächsischen Hochschulraum wird insgesamt als erstrebenswert erachtet.

Literatur

Die angegebenen Links wurden zuletzt am 09.01.2018 abgerufen.

- 1 N.N. (2015): Münchner Unis erhalten Negativpreis, in: Spiegel Online vom 5.5.2017, <http://www.spiegel.de/lebenundlernen/uni/datenschutz-tu-und-lmu-muenchen-erhalten-big-brother-award-a-1145924.html>.
- 2 Boie, J.; Grassegger, H. (2015): Der gläserne Student – Datenschutz bei Online-Kursen, in: Süddeutsche Zeitung vom 2.12.2015, <http://www.sueddeutsche.de/bildung/2.220/datenschutz-bei-online-kursen-der-glaeserne-student-1.2762465>.
- 3 Albers, M. (2017): § 16 BDSG Rn. 12. In: Wolff, H. A./Brink, S., Beck'scher Online-Kommentar Datenschutzrecht (BeckOK DatenschutzR), 22. Edition, Stand: 01.11.2017.
- 4 Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (2011): E-Learning an Hochschulen nach den Grundsätzen des Datenschutzes, https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/BildungundForschung/Inhalt/6_E-Learning-Systeme/E-Learning_an_Hochschulen.pdf, S. 1.
- 5 Bischoff, A. (2013): E-Learning und Datenschutz an Hochschulen, S. 88 ff.
- 6 Landesbeauftragter für Datenschutz und Informationsfreiheit NRW (2011): E-Learning an Hochschulen nach den Grundsätzen des Datenschutzes, https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/BildungundForschung/Inhalt/6_E-Learning-Systeme/E-Learning_an_Hochschulen.pdf, S. 3.
- 7 Roßnagel, A.; Schnabel, C. (2009): Datenschutzkonforme Nutzung von E-Learning-Verfahren an hessischen Hochschulen, Abschlussbericht vom 31.3.2009, www.uni-kassel.de/einrichtungen/fileadmin/datas/einrichtungen/scl/LLukas/Abschlussbericht_Datenschutz_im_E-Learning.pdf, S. 21;
- 8 Bischoff, A. (2013): E-Learning und Datenschutz an Hochschulen, S. 74.
- 9 Sächsisches Staatsministerium für Wissenschaft und Kunst – SMWK (2017): Verordnung des Sächsischen Staatsministeriums für Wissenschaft und Kunst über die Verarbeitung personenbezogener Daten der Mitglieder, Angehörigen, Studienbewerber, Prüfungskandidaten, Gasthörer und ehemaligen Mitglieder der staatlichen Hochschulen (Sächsische Hochschulpersonendatenverordnung – SächsHSPersDatVO) vom 20. Oktober 2017, <https://www.revosax.sachsen.de/vorschrift/17455-Saechsische-Hochschulpersonendatenverordnung>.
- 10 Sächsisches Staatsministerium für Wissenschaft und Kunst – SMWK (2000): Verordnung des Sächsischen Staatsministeriums für Wissenschaft und Kunst zur Verarbeitung personenbezogener Daten der Studienbewerber, Studenten und Prüfungskandidaten für statistische und Verwaltungszwecke der Hochschulen (Sächsische Studentendatenverordnung – SächsStud-DatVO) vom 19. Juli 2000, <https://www.revosax.sachsen.de/vorschrift/3796/33306>.

- 11 Europäischer Gerichtshof – EuGH (2016): Urteil vom 19.10.2016, Az. C-582/14, NJW 2016, 3579 – Breyer/Deutschland; BGH, Urteil vom 16.05.2017, Az.: VI ZR 135/13.
- 12 Kempen, B. (2017): Art. 5 Rn. 183. In: Epping, V.; Hillgruber, C. (Hrsg.): Beck'scher Online-Kommentar Grundgesetz, 34. Edition, Stand: 15.08.2017.
- 13 Bischoff, A. (2013): E-Learning und Datenschutz an Hochschulen, S. 76.
- 14 Europäischer Gerichtshof – EuGH (2016): Urteil vom 6.10.2015, Az. C-362/14, NJW 2015, 3151 – Schrems/Data Protection Commissioner.
- 15 Wolff, H. A (2016): Syst. A. Prinzipien des Datenschutzrechts, Rn. 23 ff. In: Wolff, H. A.; Brink, S.: Beck'scher Online-Kommentar Datenschutzrecht (BeckOK DatenschutzR), 22. Edition, Stand: 01.11.2016.
- 16 Bischoff, A. (2013): E-Learning und Datenschutz an Hochschulen, S. 64 ff.
- 17 Kalberg, N. (2013) Datenschutz an Hochschulen, S. 106.
- 18 Landesbeauftragter für Datenschutz und Informationsfreiheit NRW (2011): E-Learning an Hochschulen nach den Grundsätzen des Datenschutzes, https://www.lidi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/BildungundForschung/Inhalt/6_E-Learning-Systeme/E-Learning_an_Hochschulen.pdf, S. 4.
- 19 Loser, K.-U. (2008): Zum Stand der Entwicklung von E-Learning-Systemen zwischen informationeller Selbstbestimmung und Freiheit der Lehre, Datenschutz Nachrichten 1/2008, https://www.datenschutzverein.de/wp-content/uploads/2013/11/DANA_1-2008.pdf, S. 14, 16 f.
- 20 Barlag, C. (2017): § 3 Rn. 233. In: Roßnagel, A. (Hrsg.): Europäische Datenschutz-Grundverordnung.