Prof. Dr. Alexander Roßnagel

Dr. Christoph Schnabel, LL.M.

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
im Forschungszentrum für Informationstechnikgestaltung (ITeG)
der Universität Kassel

Datenschutzkonforme Nutzung von E-Learning-Verfahren an hessischen Hochschulen

– Abschlussbericht –

Kassel, den 31. März 2009

Inhalt

1. Einleitung

E-Learning-Verfahren stellen einen wichtigen Bestandteil eines auf die Zukunft ausgerichteten Lehrbetriebs dar. E-Learning-Verfahren ermöglichen und unterstützen das selbstständige und -tätige Lernen der Studierenden und helfen, sie als selbständige, eigenverantwortliche Lernende anzusprechen und herauszufordern. E-Learning ersetzt nicht die Präsenzlehre, sondern ist als zusätzliches Angebot von Lernchancen zu verstehen, das Lernenden ermöglicht, ein breiteres Angebot von Lernwegen zu nutzen und flexibel die individuell angemessene Mischung von Lernmöglichkeit zu wählen. E-Learning kann so als Mittel und Medium genutzt werden, mit dessen Hilfe medienunterstützte Lehre das eigenständige, selbstverantwortete Lernen der Studierenden fordert und fördert, indem sie Lernanlässe schafft, Lernanreize setzt, Erprobungen des Neugelernten ermöglicht, Rückmeldungen zu Lernfortschritten gibt und Betreuung bei der Aufgabenerfüllung anbietet. Außerdem bietet E-Learning Studierenden neue Möglichkeiten, sich im Umgang mit Informations- und Kommunikationstechnologien zu üben.

Gleichzeitig kann E-Learning die Hochschulen unterstützen, ihre Aufgaben wahrzunehmen, indem sie auch mit beschränkten Ressourcen noch eine angemessene Lehre durchführen können. So können zum Beispiel räumliche Kapazitätsprobleme verringert werden, indem eine Vorlesung gleichzeitig den Veranstaltungsteilnehmern nach Hause oder in einen benachbarten Hörsaal übertragen wird oder indem Klausuren elektronisch angeboten und korrigiert werden.

Durch E-Learning-Verfahren entstehen aber auch Risiken für die informationelle Selbstbestimmung der betroffenen Studierenden und der Lehrenden.[1] Im Gegensatz zu Präsenzveranstaltungen im Hörsaal entstehen bei E-Learning-Verfahren sowohl von Lehrenden als auch von Studierenden bei jedem Lehr- und Lernschritt Datenspuren, die hinsichtlich Inhalt, Ort, Zeit und Person zusammengeführt und sogar zu mittel- oder langfristigen Profilen aggregiert werden können. Diese könnten zu Leistungsbewertungen sowohl bei Lehrenden als auch bei Lernenden oder zu anderen Zwecken genutzt werden. Da alle diese Datenspuren personenbezogene Daten darstellen, sind ihre Erhebung, Verarbeitung und Nutzung Eingriffe in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen, die einer rechtlichen Rechtfertigung bedürfen. Inzwischen werden auch vermehrt Beschwerden über die Verletzung des Persönlichkeitsrechts beim Angebot von E-Learning-Verfahren von Seiten der Studierenden vorgetragen.

Durch den Erlass die „Satzung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren an der Universität Kassel“ vom 20.Oktober 2008[2] hat sich die Universität Kassel diesen Problemen gestellt. Die Satzung vereinheitlicht die Bedingungen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, unter denen E-Learning-Verfahren angeboten werden. Sie schafft die datenschutzrechtlichen Voraussetzungen, die den technischen und organisatorischen Grundlagen des E-Learning angemessen sind und die einen Ausgleich zwischen der Nutzung der neuen Verfahren und dem Schutz der informationellen Selbstbestimmung der Betroffenen gewährleisten sollen.

Bei der „Satzung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren an der Universität Kassel“ handelt es sich wohl um die erste Satzung ei-

---

1 Allgemein zum Schutz von Studierenden-Daten Wettern, RDV 2006, 14 ff.; zum Datenschutz im E-Learning s. Flisek, CR 2004, 62 ff.

2 http://cms.uni-kassel.de/unicms/fileadmin/groups/w_430000/Download/satzung_elearning.pdf.

ner Universität, die sich ausschließlich mit den Problemen des Datenschutzes beim Einsatz vom E-Learning-Verfahren beschäftigt. Sie behandelt noch nicht alle wesentlichen Punkte, sondern muss in der Praxis erprobt und dann weiterentwickelt werden. Sie ist bewusst als eine erste Fassung mit allgemeinen Regelungen konzipiert worden, die die E-Learning-Verfahren der Universität Kassel erst einmal auf die erforderliche rechtliche Grundlage stellen sollte.

Dabei war von Anfang an geplant, spezifische Fragestellungen von E-Learning-Verfahren gezielt zu untersuchen und nach der Erarbeitung der Antworten die Datenschutz-Satzung zu ergänzen und zu überarbeiten. Die Erstellung der folgenden Untersuchung wurde durch eine Förderung des Hessischen Ministeriums für Wissenschaft und Kunst ermöglicht und erfolgte von September 2008 bis März 2009. Sie beruht auf einer schriftlichen Befragung der Datenschutzbeauftragten und der E-Learning-Koordinationsstellen aller zwölf Hessischen Hochschulen sowie einer Diskussionsveranstaltung mit diesen zu den drängenden Datenschutzproblemen des E-Learning am 24. November 2008 in der Technischen Universität Darmstadt.

Auf diese Weise wurden ergänzend zur bestehenden „Muster-Satzung“ der Universität Kassel weitere datenschutzrechtliche Fragen identifiziert, die im Folgenden untersucht werden. Die Antworten auf diese Fragen zeigen entweder eine geltende Rechtslage auf, die befriedigende normative Lösungen enthält, oder führen zu einem bestehenden Regelungsbedarf.

Für den festgestellten Regelungsbedarf werden Vorschläge zur Lösung entwickelt, die Empfehlungen enthalten, die bestehende Satzung fortzuentwickeln. Im Anhang zu dem vorliegenden Bericht findet sich daher

- ein Vorschlag zu einer neugefassten Datenschutz-Satzung und
- eine Erläuterung dieses Vorschlags für E-Learning-Nutzer.

Die auf diese Art und Weise überarbeitete und aktualisierte Fassung der „Satzung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren an der Universität Kassel“ kann als Muster für sämtliche Hochschulen herangezogen werden, die vor ähnlichen Herausforderungen stehen.

Im Folgenden werden die zusammen mit den Datenschutzbeauftragten und der E-Learning-Koordinationsstellen der Hessischen Hochschulen erarbeiteten Datenschutzfragen zu E-Learning-Verfahren untersucht und beantwortet:

2. Personenbezogene Daten externer Nutzer

Die Satzung erfasst die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ihrer Mitglieder. Viele Hochschulen haben aber zum Beispiel Weiterbildungsangebote, deren Teilnehmer keine Mitglieder der Hochschule sind, oder Lehrkooperationen mit anderen Universitäten im In- und Ausland (auch in Übersee). Dies erfordert einerseits die Verarbeitung personenbezogener Daten von Nichtmitgliedern der Hochschule und andererseits die Übermittlung von Studierenden-Daten an andere Hochschulen, möglicherweise außerhalb des Geltungsbereichs der Europäischen Datenschutzrichtlinie.

Die Satzungsbefugnis der Hochschulen ist begrenzt. Bei Körperschaften des öffentlichen Rechts ist die Satzungsbefugnis personell auf die Mitglieder der Körperschaft beschränkt.[3] Darunter fallen alle Studierende und Hochschullehrende der eigenen Hochschule, aber nicht externe Studierende oder Lehrende oder Personen, die an einem Weiterbildungsangebot der Hochschule teilnehmen.

Solche Personen müssen die Benutzungsordnung des Hochschulrechenzentrums der Universität Kassel anerkennen, wenn sie an E-Learning-Verfahren der Universität teilnehmen wollen. Da diese Benutzungsordnung auch auf die Satzung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren an der Universität Kassel verweist, gilt die Satzung aufgrund dieser Anerkennung auch für externe Nutzer, die ansonsten nicht der personellen Satzungsgewalt der Universität unterfallen.

Problematischer ist die Antwort auf die Frage, wie mit der Übermittlung von Daten in das Ausland umzugehen ist. In zwei verschiedenen Konstellationen könnte dies relevant sein: Wenn ein Lehrender im Ausland weilt (auf einer Dienstreise oder aufgrund eines Forschungsaufenthalts) und von dort aus ein E-Learning-Verfahren betreut oder wenn eine Kooperation mit einer Hochschule oder einer Forschungseinrichtung im Ausland durchgeführt wird. Nach § 17 Abs. 2 Satz 1 HDSG ist die Übermittlung von Daten außerhalb des Geltungsbereichs der Datenschutzrichtlinie nur zulässig, wenn die Datenübermittlung ausschließlich im Interesse des Betroffenen liegt oder beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist. Mit dieser Regelung setzt das HDSG Art. 25 Abs. 1 DSRL um.

Innerhalb des Anwendungsbereichs der Datenschutzrichtlinie (also in der Europäischen Union und im Europäischen Wirtschaftsraum) ist von der Gewährleistung eines angemessenen Schutzniveaus im Sinn des Art. 25 Abs. 1 DSRL auszugehen und ein Zugriff auf die Daten von dort aus oder eine Übermittlung der Daten dort hin möglich. Außerhalb des Europäischen Wirtschaftsraums wird die Gewährleistung eines angemessenen Schutzniveaus von der Europäischen Kommission überprüft und für einzelne Staaten verbindlich festgestellt.[4] Zum jetzigen Zeitpunkt hat die Kommission ein angemessenes Schutzniveau für Argentinien, Schweiz, Kanada, Guernsey, Jersey und Isle of Man angenommen. Es fehlen die USA und alle asiatischen und afrikanischen Länder.

Es bestehen Kooperationen mit Universitäten in Ländern, die kein angemessenes Datenschutzniveau gewährleisten, und es ist auch davon auszugehen, dass Lehrende bei Auslandsreisen in diese Länder reisen und von dort auf Daten aus den E-Learning-Verfahren zugreifen werden. Hier ist zunächst zu untersuchen, ob es sich bei diesen Arten des Zugriffs um Datenübermittlungen nach § 17 Abs. HDSG handelt. Wenn dies der Fall ist, müssen Lösungen gefunden werden.

Zunächst ist der Fall des Lehrenden zu untersuchen, der in einem Staat, der kein angemessenes Datenschutzniveau gewährleistet, weilt und von dort aus auf die Daten des von ihm angebotenen E-Learning-Verfahrens zugreift. Physikalisch sind die Daten im Moment des Zugriffs auf dem Computer des Lehrenden und damit in einem Staat, der kein angemessenes Schutzni-

---

[3] S. Maurer 2006, § 4, Rn. 23. Die Universität Kassel ist als Körperschaft öffentlichen Rechts organisiert. Einige Universitätskliniken sind als Anstalten öffentlichen Rechts organisiert. In einem solchen Fall umfasst die Satzungsbefugnis personell die Benutzer der Anstalt, s. Maurer, § 4, Rn. 23.

[4] Die Liste ist abrufbar unter http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm.

veau gewährleistet. Fraglich ist, ob hierin auch eine Übermittlung von Daten zu sehen ist.[5] Nach § 2 Abs. 2 Nr. 3 HDSG ist Übermitteln das

> *„…Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder dass der Dritte zum Abruf bereitgehaltene Daten abruft."*

Der „Dritte" ist in § 2 Abs. 5 HDSG definiert als jede Person oder Stelle „außerhalb der datenverarbeitenden Stelle". Beim Lehrenden, der im Rahmen einer Auslandsreise auf die Daten zugreift, handelt es sich nicht um einen Dritten, da er Mitglied der Universität Kassel ist. Es findet daher kein Wechsel der verantwortlichen Stelle im Sinn des § 2 Abs. 3 in Verbindung mit § 3 Abs. 1 Satz 1 HDSG statt. Die Ausnahme, die im Rahmen der Auftragsdatenverarbeitung greift, ist auf Fälle des § 4 HDSG beschränkt.[6] Mangels Übermittlung besteht daher auch kein datenschutzrechtliches Problem. Technisch befinden sich die Daten bei einem Zugriff durch einen Lehrenden zwar im Ausland und unterliegen dann auch dem dort geltenden Recht, so dass gegebenenfalls kein angemessenes Datenschutzniveau gewährleistet ist, zum Beispiel beim Zugriff durch Sicherheitsbehörden. Dennoch behandeln das europäische und das hessische Datenschutzrecht den Zugriff der berechtigten Lehrenden nicht als Übermittlung und verhindern sie nicht. Wegen des faktisch verminderten Schutzniveaus sollten derartige Datenverarbeitungen aber vermieden werden.

Fraglich ist, was bei einer Kooperation mit ausländischen Universitäten und Forschungseinrichtungen gilt. Bei einer solchen Kooperation werden die Mitglieder der ausländischen Einrichtung auf Daten zugreifen, die im Rahmen des E-Learning verarbeitet werden. Schon der Zugriff auf personenbezogene Daten, die auf Servern der Universität Kassel gespeichert werden, könnte eine Übermittlung darstellen.

Der Europäische Gerichtshof hat im Lindqvist-Fall erklärt,[7]

> *„…dass keine Übermittlung von Daten in ein Drittland im Sinne von Artikel 25 der Richtlinie 95/46 vorliegt, wenn eine sich in einem Mitgliedstaat aufhaltende Person in eine Internetseite, die bei ihrem in demselben oder einem anderen Mitgliedstaat ansässigen Host-Service-Provider gespeichert ist, personenbezogene Daten aufnimmt und diese damit jeder Person, die eine Verbindung zum Internet herstellt, einschließlich Personen in Drittländern, zugänglich macht."*

Diese Erkenntnisse sind aber nicht unmittelbar auf die hier zu untersuchende Konstellation übertragbar. Der Europäische Gerichtshof hatte einen Fall zu beurteilen, bei dem es um frei abrufbare Internetseiten ging. Das Gericht hat sich dabei unter anderem von dem Gedanken leiten lassen, dass eine anders lautende Entscheidung das Ende des World Wide Web (WWW) bedeutet hätte.[8] Ferner hatte der Europäische Gerichtshof das Verhältnis zwischen

---

5 Zur Problematik des Begriffs „Übermitteln" („data transfer") im Sinn der DSRL s. Kuner 2007, Rn. 2.42 ff.

6 S. Nungesser 2001, Erl. § 17, Rn. 6.

7 EuGH, Urteil v. 6.11.2003, Rs C-101/01, Abs. 71; die andere Ansicht von Nungesser 2001, Erl. § 2, Rn. 53 dürfte sich damit erledigt haben.

8 S. Roßnagel, MMR 2004, 99: „Wäre das Angebot zum Abruf von Seiten aus dem WWW als eine Übermittlung zu klassifizieren, würde der Vollzug der Regelung des Art. 25 DSRL für Europa weitgehend zum Erliegen des WWW führen."

Anbieter und Host-Provider zu beurteilen. In der Konstellation der E-Learning-Kooperation mit einer ausländischen Universität geht es aber um die Frage, ob der Abruf der Daten vom Host-Provider eine Datenübermittlung darstellt.

Durch den Datenabruf gelangen die Daten in den Verfügungsbereich der ausländischen Hochschule und damit an einen Dritten im Sinn des § 2 Abs. 5 HDSG. Somit liegt eine Datenübermittlung nach § 2 Abs. 2 Nr. 3 HDSG vor. Folglich müssen die Voraussetzungen einer Datenübermittlung nach § 17 Abs. 2 HDSG und Art. 25, 26 DSRL erfüllt sein.

Es besteht die Möglichkeit, über den in Art. 26 Abs. 2 DSRL vorgesehenen Weg ein angemessenes Datenschutzniveau zu gewährleisten. Art. 26 Abs. 2 DSRL lautet:

> *„...ein Mitgliedstaat* [kann] *eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland genehmigen, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet; diese Garantien können sich insbesondere aus entsprechenden Vertragsklauseln ergeben."*

Es existieren verschiedene Möglichkeiten, den Anforderungen aus Art. 26 Abs. 2 DSRL gerecht zu werden.[9] Hierzu zählen das Safe-Harbor-Abkommen,[10] Standardvertragsklauseln[11] und verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer.[12]

Für die Kooperation mit anderen Universitäten oder Forschungseinrichtungen eignen sich verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer am besten. Universitäten und Forschungseinrichtungen sind keine Unternehmen und haben insbesondere im Regelfall keine Zweigstellen im Ausland. Trotzdem kann die Idee, die hinter verbindlichen unternehmensinternen Vorschriften für den internationalen Datentransfer steht, auch beim Datentransfer an ausländische Universitäten hilfreich sein. Eine ausländische Universität kann sich, ebenso wie ein Unternehmen, einem bestimmten Verhaltenskodex unterwerfen und diesen für sich als verbindlich anerkennen. Bieten diese Vorschriften ein angemessenes Schutzniveau, sind sie für die Universität verbindlich und hat der Betroffene im Zweifel die Möglichkeit, die Einhaltung der Regeln zu erzwingen, so kann die Universität Kassel die Daten an die kooperierende Universität genauso übermitteln, wie wenn sich diese im EU-Ausland befände.

Die Artikel-29-Datenschutzgruppe hat sich zu den Voraussetzungen, die verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer erfüllen müssen, ausführ-

---

9 § 17 Abs. 2 Satz 1 2. Alt. HDSG fordert, dass „...beim Empfänger ein angemessener Datenschutz gewährleistet ist." Diese Voraussetzung dürfte durch die im folgenden genannten Vorgehensweisen zu erfüllen sein.

10 S. dazu Holzhausen 2002, 28 ff.

11 S. die Entscheidung der Kommission 2001/497/EC vom 15.7.2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, L 181, 19 ff. via http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:181:0019:0031 :DE:PDF.

12 S. dazu Artikel-29-Datenschutzgruppe 2003, 1 ff.

lich geäußert.[13] Die wichtigsten Voraussetzungen werden im Folgenden kurz zusammengefasst:

Der Empfänger der Daten muss sich Regeln unterwerfen, die grundsätzlich ein angemessenes Schutzniveau gewährleisten. Dies muss nicht bedeuten, dass der Datenempfänger nach exakt den gleichen Regeln verfährt, die in der Datenschutz-Satzung festgelegt sind. Er muss sich aber einem Regelungsregime unterwerfen, das die anerkannten Grundsätze des Datenschutzes enthält. Diese Grundsätze werden im Wesentlichen in Art. 6 DSRL wiedergegeben: Treu und Glauben, Zweckbindung, Erforderlichkeitsgrundsatz und die sachliche Richtigkeit der Daten.[14] Hinzu kommen unabdingbare Rechte des Betroffenen der Datenverarbeitung.[15]

Der Empfänger der Daten muss gewährleisten, dass diese Vorschriften von seinen Mitarbeitern auch eingehalten werden. Möglichkeiten dies zu erreichen, sind zum Beispiel individuelle und ausführliche Information der Mitarbeiter etwa durch Schulungsprogramme, Disziplinarmaßnahmen bei Verstößen gegen die Vorschriften und ähnliche Umsetzungsmaßnahmen.[16]

Trotzdem kann es vorkommen, dass Mitarbeiter des Empfängers der Daten die datenschutzrechtlichen Vorgaben bewusst oder versehentlich verletzen. In einem solchen Fall muss der Betroffene die Möglichkeit haben, die Einhaltung der Regeln zu erzwingen.

> *„Von einem angemessenen und wirksamen Datenschutzsystem ist zu fordern, dass der Einzelne bei einem Problem im Zusammenhang mit den eigenen personenbezogenen Daten nicht allein gelassen wird, sondern institutionelle Hilfe erhält, um die Schwierigkeiten zu beheben.“*[17]

Dies kann erreicht werden, indem der Empfänger seine Mitarbeiter verpflichtet, mit nationalen Datenschutzbehörden zusammenzuarbeiten, wenn eine entsprechende Verpflichtung nicht ohnehin existiert. Sind im Rechtssystem des entsprechenden Landes überhaupt keine Datenschutzbehörden vorgesehen, kann der Empfänger gehalten sein, einen eigenen betrieblichen Datenschutzbeauftragten zu bestimmen und ihn mit ausreichenden unternehmensinternen Rechten auszustatten, so dass er in völliger Unabhängigkeit den vorgetragenen Beschwerden nachgehen kann. Betroffene dürfen keine Sanktionen in Aussicht gestellt werden, wenn sie Rechtsmittel gegen den Empfänger wegen der Verletzung des Datenschutzes ergreifen.

Die Einhaltung der nationalen gesetzlichen Bestimmungen für den Datenschutz durch den ausländischen Empfänger ist selbstverständlich eine unabdingbare Voraussetzung.[18] Auch wenn diese Vorschriften kein angemessenes Datenschutzniveau gewährleisten, müssen sie trotzdem befolgt werden. Hält sich der Datenempfänger nicht an die eigenen nationalen Regeln, so kommt eine Datenübermittlung an ihn nicht in Betracht.

Darüber hinaus fordert § 17 Abs. 2 Satz 2 HDSG:

---

13 Artikel-29-Datenschutzgruppe 2003, 7 ff.

14 S. Ehmann/Helfrich 1999, Art. 6, Rn. 2 ff.

15 S. dazu Wedde, in: Roßnagel 2003, 4.4, Rn. 1 ff.

16 Artikel-29-Datenschutzgruppe 2003, 10.

17 Artikel-29-Datenschutzgruppe 1998, 14.

18 Artikel-29-Datenschutzgruppe 2003, 7.

„Vor der Entscheidung über die Angemessenheit ist der Hessische Datenschutzbeauftragte zu hören."

Diese Anforderung muss ebenfalls erfüllt werden. Der Hessische Datenschutzbeauftragte wird abschließend entscheiden, ob die einseitigen Garantien der ausländischen Hochschule oder Forschungseinrichtung den Anforderungen der Datenschutzrichtlinie genügen und ein Transfer von Daten daher zulässig ist oder nicht.

Im Ergebnis ist eine Änderung der Datenschutz-Satzung der Universität Kassel nicht erforderlich. Das Erfordernis, vor der Entscheidung über die Angemessenheit, den Hessischen Datenschutzbeauftragten zu hören, ergibt sich unmittelbar aus § 17 Abs. 2 Satz 2 HDSG und muss nicht zusätzlich in die Satzung aufgenommen werden. Bei der Wahl des Mittels, wie die Universität einen angemessenen Schutz der personenbezogenen Daten bei der Kooperationseinrichtung erreichen will, sollte die Hochschule nicht durch starre Vorgaben in der Satzung in ihren Wahlmöglichkeiten beschränkt werden. Entscheidend ist lediglich, dass ein angemessenes Datenschutzniveau gewährleistet ist, bevor die Daten übermittelt werden.

3. Umgang mit Daten besonderer Art

§ 7 Abs. 4 HDSG beschränkt den Umgang besonderer Kategorien von Daten. Zu diesen Daten gehören Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.[19] Dies entspricht zwar den europäischen Vorgaben in Art. 8 DSRL, es steht jedoch in einem klaren Widerspruch zum bisherigen deutschen Verständnis, nach dem alle personenbezogenen Daten gleich schutzwürdig sind, da sich ihre soziale Bedeutung aus dem Kontext der Datenverwendung ergibt.[20]

Streng genommen handelt es sich bereits bei der Information, dass jemand eine Brille trägt, um ein Gesundheitsdatum. Würde man jede Information dieser Art, die nur Hinweise auf Daten besonderer Art enthält, bereits dem besonderen Schutz des § 7 Abs. 4 HDSG unterstellen, so würde dies zu einer ausufernden und nicht mehr praktikablen Anwendung der Sonderregelungen führen. Für die besonderen Kategorien von Daten ist daher zu fordern, dass sich ihre besondere Schutzbedürftigkeit aus dem Verwendungszusammenhang ergeben muss. Ausschlaggebend für die Anwendung der Regeln über diese besonderen Arten von Daten ist also der Zusammenhang, in dem die Daten, sofern sie überhaupt in die in Art. 8 DSRL und § 7 Abs. 4 HDSG genannten Kategorien fallen, verwendet werden.[21] Grunddaten, die nur Rückschlüsse auf derartige Informationen zulassen, unterfallen nicht dem besonderen Schutz für die besonderen Kategorien von Daten, wenn nicht gerade die Absicht besteht, die Informationen als solche zu speichern.[22] Ansonsten unterfielen fast alle überhaupt gespeicherten und verarbeiteten Daten unter die Sonderregelungen, da sich Rückschlüsse und Zusammenhänge fast immer herstellen lassen und es auf die Korrektheit der Rückschlüsse nicht ankommt. Entscheidend ist auch nicht die Frage, ob das Datum der besonderen Kategorie selbst (zum Bei-

---

19 Zur Kritik an der fragwürdigen Wortwahl bei dem Begriff „rassische Herkunft" s. Cremer 2008, 1 ff. Der Gesetzgeber hat hier die Wortwahl der DSRL übernommen, um Auslegungsschwierigkeiten zu vermeiden, vgl. Nungesser 2001, Erl. § 7, Rn. 29.

20 S. dazu Ehmann/Helfrich 1999, Art. 8, Rn. 9. Zur Kritik an dieser Regelung s. Roßnagel/Pfitzmann/Garstka 2001, 81; Simitis 2006, § 3, Rn. 250 ff.

21 Simitis 2006, § 3, Rn. 254.

22 S. dazu Gola/Schomerus 2007, § 3, Rn. 56a mit anschaulichen Beispielen.

spiel die Religionszugehörigkeit als solche) oder nur Daten gespeichert werden, aus denen sich das Datum ergibt, sondern ob die Daten gespeichert werden, weil eine Kategorisierung der Betroffenen in verschiedene Religionszugehörigkeiten vorgenommen werden soll. In einem solchen Verwendungszusammenhang sind die Vorschriften über den Umgang mit besonderen Kategorien von Daten anwendbar, weil sie die Betroffenen gerade vor den Gefahren einer Kategorisierung schützen sollen.

Eine zielgerichtete Auswertung von Daten, die Studierende nach ethnischer Herkunft, religiöser Überzeugung, Sexualleben oder ähnlichem kategorisiert, sollte soweit irgend möglich vermieden werden. Es ist auf Anhieb nicht ersichtlich, inwiefern eine derartige Datenverarbeitung im Rahmen des E-Learning erforderlich sein könnte. Es kann aber nicht ausgeschlossen werden, dass auch im E-Learning Konstellationen existieren oder entstehen, die eine Verarbeitung der genannten Kategorien von Daten in einem Verwendungszusammenhang vorsehen, der die Anwendbarkeit der besonderen Regeln erfordert. In diesem Fall existieren zwei Rechtsgrundlagen, die eine Verarbeitung erlauben.

Eine Verarbeitung kann auf eine Einwilligung nach § 7 HDSG gestützt werden.[23] In einem solchen Fall muss sich die Einwilligung gemäß § 7 Abs. 2 Satz 2 HDSG ausdrücklich auf die in § 7 Abs. 4 HDSG genannten Daten beziehen.[24] Dies bedeutet, dass über die Anforderungen hinaus, die an eine informierte Einwilligung ohnehin zu stellen sind, die besonderen Kategorien von Daten und ihr spezifischer Verwendungszweck in der Einwilligung ausdrücklich genannt werden müssen. Auf die Einwilligung kann gemäß § 7 Abs. 4 Satz 2 HDSG verzichtet werden, wenn die Verarbeitung der Daten, die in die besonderen Kategorien fallen, ausschließlich im Interesse des Betroffenen liegt und der Hessische Datenschutzbeauftragte vor der Verarbeitung gehört wurde.[25] Diese Verarbeitungsgrundlage sollte jedoch nicht gewählt werden, da es hier an der Transparenz fehlt und eine solche Vorgehensweise bei Studierenden auf Unverständnis und Skepsis stoßen könnte.

Denkbar ist eine Verarbeitung von Daten, die den besonderen Schutz des § 7 Abs. 4 HDSG erfordert, vor allem im Bereich der Forschung. Bei Forschungsvorhaben im Rahmen des E-Learning ist § 8 der Satzung einschlägig. Diese Vorschrift bezieht sich aber nicht ausdrücklich auf besondere Kategorien von Daten. Sie kann daher die Verarbeitung von personenbezogenen Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben nicht rechtfertigen. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten dieser Art bleibt es daher bei der Einwilligung.

Die aus Sicht des Datenschutzes vorzugswürdigste Möglichkeit ist die Anonymisierung der Daten. In diesem Fall besteht kein Risiko für die Persönlichkeitsrechte der betroffenen Nutzer. Eine ausreichende Pseudonymisierung liegt nur dann vor, wenn die Möglichkeit der Re-

---

23 Zwar sieht § 7 Abs. 4 HDSG, der die besonderen Kategorien von Daten benennet dies nicht vor, aber Abs. 2 Satz 2 verlangt, dass eine Einwilligung, die diese Verarbeitung ermöglichen soll, die Datenkategorie aus Abs. 4 ausdrücklich benennen muss. Hieraus lässt sich folgern, dass auch die Einwilligung die Verarbeitung legitimieren können muss – im Ergebnis ebenso Nungesser 2001, Erl. § 7, Rn. 22. Dieses Ergebnis steht auch im Einklang mit den europarechtlichen Vorgaben, s. Art. 8 Abs. 2 a) DSRL. Die Formulierung ist aber nicht glücklich.

24 S. dazu auch Nungesser 2001, Erl. § 7, Rn. 22.

25 Hiermit wird der Annahme Rechnung getragen, dass Betroffene kein Verständnis dafür hätten, jedes Mal eine ausdrückliche Einwilligung erteilen zu müssen, so Nungesser 2001, Erl. § 7, Rn. 33 a.E.

Personifizierung so gering ist, dass die Daten wie anonyme Daten zu behandeln sind. Ist dies geschehen, so ist die Verarbeitung dieser Daten ohne Einschränkungen möglich.

In die Satzung sollte daher folgende Regelung zusätzlich aufgenommen werden:

> *„Die Verarbeitung von Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben von Nutzern zu Zwecken des E-Learning ist nur auf Grundlage einer ausdrücklichen Einwilligung des Nutzers zulässig."*

4. Umgang mit Videodaten

Lehrveranstaltungen werden aus verschiedenen Gründen als Videodatei übertragen oder aufgezeichnet, so zum Beispiel, um einer größeren Gruppe die Teilnahme an der Veranstaltung zu ermöglichen, obgleich die räumlichen Kapazitäten erschöpft sind oder sich die Teilnehmer an einem anderen Ort befinden, um eine zeitversetzte Teilnahme an der Veranstaltung zu ermöglichen oder um mit der Veranstaltung über die Universität als Ganzes oder einen bestimmten Fachbereich oder eine Studienrichtung zu informieren. Vom Grund der Videoaufzeichnung hängt ab, was genau mit den Videodaten geschieht, ob und wie sie weiterverwendet werden sollen.

Grundsätzlich bestehen drei unterschiedliche Umgangsweisen mit Videodaten:

- Die direkte Übertragung in einen anderen Hörsaal oder an Teilnehmer der Lehrveranstaltung an einem anderen Ort ohne Aufzeichnung (Live-Streaming),

- Aufzeichnung und Speicherung für einen späteren Zugriff durch Teilnehmer der Veranstaltung,

- Live-Streaming oder Aufzeichnung und Speicherung für einen externen Zugriff durch die Öffentlichkeit,[26] zum Beispiel über das Internet.

An der Universität Kassel wurden im Wintersemester 2008/09 rund 30 Videoprojekte durchgeführt. Im überwiegenden Teil der Projekte wurde die Lehrveranstaltung nur aufgezeichnet oder aufgezeichnet und gleichzeitig in benachbarte Hörsäle oder an die Teilnehmer an anderen Orten übertragen. Die reine Übertragung von Hörsaal zu Hörsaal und das Aufzeichnen zum Bereitstellen für die Öffentlichkeit stellen Ausnahmefälle dar.

Bei datenschutzadäquaten Lösungen für Videoaufzeichnungen und -übertragungen zu Zwecken des E-Learning ist zwischen Eingriffen in die Rechte der Lehrenden und der Studierenden zu unterscheiden. Im Gegensatz zur Aufnahme der Lehrenden ist es nicht immer notwendig, für die genannten Zwecke Studierende auf Video zu erfassen, manchmal lässt es sich aber auch nicht vermeiden. Wenn Hörsäle so geschnitten sind, dass Studierende regelmäßig ins Bild geraten oder der Lehrende sich im Hörsaal bewegt und dabei auch durch die Reihen der Studierenden geht, dann muss die Kamera ihm folgen und wird dabei zwangsläufig auch Studierende aufnehmen.

---

[26] Mitglieder der Hochschule, die nicht an einer Veranstaltung teilnehmen, fallen unter den Begriff der Öffentlichkeit.

Durch Videoaufzeichnungen wird in das Persönlichkeitsrecht der Betroffenen eingegriffen. Das Recht am eigenen Bild ist als besonderes Persönlichkeitsrecht auch verfassungsrechtlich geschützt.[27] Dieses Recht gewährleistet dem Abgebildeten, selbst darüber zu bestimmen, „wie er sich gegenüber Dritten oder der Öffentlichkeit darstellen will, was seinen sozialen Geltungsanspruch ausmachen soll".[28] Soweit in den Aufnahmen und Übertragungen von Lehrveranstaltungen von Lehrenden oder Studierenden Bilder verwendet werden, in denen einzelne Personen als Individuen im Mittelpunkt stehen, ist deren Recht am eigenen Bild betroffen. Dies ist jedoch dann nicht der Fall, wenn Bildaufnahmen eine Gruppe betreffen und der Einzelne quasi zufällig durch das Bild erfasst ist.[29] Lehrende werden bei der Aufnahme und Übertragung von Lehrveranstaltungen wohl immer in ihrem Recht am eigenen Bild betroffen sein. Bei Studierenden ist genau zu prüfen, ob sie als Individuen oder nur als Teil der großen Gruppe der Lehrveranstaltungsteilnehmer erfasst werden. Ersteres dürfte zum Beispiel bei der Aufnahme eines individualisierten Beitrags, letzteres bei einem Kameraschwenk über einen großen Hörsaal der Fall sein.

Der einfachgesetzliche Schutz richtet sich nach den §§ 22, 23 KunstUrhG.[30] Diese Vorschriften verdrängen das ansonsten einschlägige Datenschutzrecht nach § 3 Abs. 3 HDSG.[31] Grundlage für die Verarbeitung von Bilddaten ist nach § 22 Satz 1 KunstUrhG die Einwilligung des Abgebildeten. Keine Einwilligung der Studierenden ist nach § 23 Abs. 1 Nr. 3 KunstUrhG notwendig, wenn nur eine Aufnahme einer größeren Vorlesung erstellt wird, ohne dass eine bestimmte Person herausgehoben wird.

Nach der gefestigten Rechtsprechung ist, im Gegensatz zum Datenschutz, die Einwilligung formlos und auch durch konkludentes Verhalten möglich.[32] Für Studierenden bedeutet dies, dass ihre Einwilligung als erteilt gelten kann, wenn sie wussten, dass die Veranstaltung als Video aufgezeichnet wird, und sie die Veranstaltung trotzdem besucht haben. Diese konkludente Einwilligung kann in vielfältiger Weise erteilt werden. Dies ist einmal anzunehmen, wenn bereits im Vorlesungsverzeichnis angekündigt wurde, dass Veranstaltungen auf Video aufgezeichnet werden. Zusätzlich ist von einer solchen Einwilligung auszugehen, wenn in der ersten Veranstaltung im Semester auf die Aufzeichnung oder Übertragung hingewiesen wird. Außerdem muss bei einer Übertragung in einen anderen Hörsaal oder an einen anderen Ort darauf hingewiesen werden, dass eine Teilnahme an der Lehrveranstaltung auch an dem anderen Ort möglich ist. Bei einer gemeinsamen Lehrveranstaltung mit einer anderen Hochschule sind die Teilnehmer durch die gegenseitige Übertragung im Hörsaal informiert. Schließlich wird zum Beispiel in der Universität Kassel eine portable Übertragungs- und Aufzeichnungstechnik benutzt, die den an der Lehrveranstaltung Teilnehmenden nicht verborgen bleiben kann.

---

27 BGH, GRUR 2005, 74, 75.

28 BVerfGE 35, 202 (220).

29 S. hierzu die verfassungsrechtlich zulässige Wertung des § 23 Abs. 1 Nr 3 KunstUrhG.

30 Ausführlich zum Recht am eigenen Bild und Datenschutz Schnabel, ZUM 2008, 657 ff.

31 Schnabel, ZUM 2008, 661f. zum Verhältnis §§ 22, 23 KunstUrhG und BDSG.

32 Vgl. dazu nur BGHZ 49, 288, 295; zusammenfassend Libertus, ZUM 2007, 621 ff. Werden durch das Bild auch besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG, § 7 Abs. 4 HDSG verarbeitet, so ist eine konkludente Einwilligung aufgrund europarechtlicher Einflüsse nicht möglich, s. dazu Schnabel, ZUM 2008, 662. Allgemein zu besonderen Arten personenbezogener Daten im Rahmen des E-Learning s. oben unter 3.

Ebenso wie die datenschutzrechtliche Einwilligung soll auch die Einwilligung nach dem Kunsturhebergesetz dem Abgebildeten ermöglichen, grundsätzlich selbst zu entscheiden, in welcher Weise er der Öffentlichkeit vorgestellt wird.[33] Dieses Ziel kann nur erreicht werden, wenn die Betroffenen zuvor über die Aufnahme und die Übertragung informiert wurden. Hierfür müssen insbesondere die Studierende beim Besuch der Veranstaltung erfahren, dass die Veranstaltung aufgezeichnet wird und auch wie mit dem Video weiter verfahren werden soll, also ob es sich nur um eine Direktübertragung in den nächsten Hörsaal handelt oder ob das Video gespeichert und anderen Veranstaltungsteilnehmern oder vielleicht sogar der Öffentlichkeit zur Verfügung gestellt werden soll. Diese Informationen müssen den Studierenden zur Verfügung stehen, bevor sie aufgezeichnet werden. Entscheiden sie sich dann für einen Besuch der Veranstaltung (anstatt die Veranstaltung im benachbarten Hörsaal oder zu Hause per Video-Stream zu verfolgen), dann gilt die Einwilligung als erteilt.

Hier ist aber das Gleiche zu berücksichtigen wie allgemein bei Datenverarbeitungsvorgängen im Rahmen der Datenschutz-Satzung, die auf Einwilligungen Studierender beruhen.[34] Um die Freiwilligkeit der Einwilligung zu wahren, darf die Einwilligung nicht zur Grundlage einer Datenverarbeitung gemacht werden, wenn sie Voraussetzung für ein Pflichtfach ist und die Studierenden keine Alternative haben, an ihr teilzunehmen. Solche Alternativen wären aber gegeben, wenn die Studierenden an der Veranstaltung in einem nicht von den Kameras erfassten Bereich des Hörsaals, in einem anderen Hörsaal oder von einem anderen Ort aus teilnehmen können. Auf die Möglichkeit, die Vorlesung im benachbarten Hörsaal zu verfolgen oder sich die Veranstaltung von zu Hause aus anzusehen, darf der Studierende nur verwiesen werden, wenn dadurch seine Möglichkeiten im Rahmen der Veranstaltung nicht eingeschränkt werden. Dies wäre aber zum Beispiel der Fall, wenn die mündliche Beteiligung eine wichtige Rolle bei der Notenvergabe spielt.

Bei Aufnahmen sollte Studierenden ermöglicht werden, „das Rampenlicht“ zu meiden. Dies gilt auch dann, wenn es rechtlich zulässig wäre, die Studierenden zu filmen. Die Aufzeichnung vorher informierter Studierender sollte nur erfolgen, wenn es aufgrund der Gegebenheiten unvermeidbar ist, Studierende aufzuzeichnen oder der Aufwand, der betrieben werden müsste, um Studierende nicht zu filmen, unzumutbar wäre. Die Anonymisierung einzelner gefilmter Studierender zum Beispiel durch Verpixelung des Gesichts ist ein nach § 4 Abs. 2 der Satzung unzumutbarer Aufwand, der im Normalfall nicht vom Verantwortlichen verlangt werden kann.

Für Lehrende ist die Rechtslage hinsichtlich des Rechts am eigenen Bild vergleichbar. Zusätzlich können sich Lehrende an Hochschulen, die Erkenntnisse der Forschung in wissenschaftlich fundierter Weise vermitteln, aber auf das Grundrecht auf Freiheit der Lehre nach Art. 5 Abs. 3 Satz 1 GG berufen.[35] Dieses Grundrecht ist ohne Schranken gewährleistet. Staatliche Eingriffe sind nicht zulässig. Soweit die Freiheit reicht, tragen allein die Grundrechtsträger die Verantwortung für ihre Ausübung. Die Lehrfreiheit beinhaltet das Recht des Hochschullehrers, selbst über Inhalt und Ablauf der Lehrveranstaltung bestimmen zu können.[36] Der Lehrende kann die Methoden der Darstellung und der Didaktik, nach denen er lehrt, frei wählen.[37] Dazu gehören auch Fragen der Organisation der Veranstaltung und deren

---

33 St. Rspr., s. nur BGH, ZUM 1996, 405, 406.

34 S. dazu später unter 7.

35 S. dazu Dreier 2004, Art 5 III, Rn. 32 ff.; Starck 2005, Art 5 III, Rn. 375 ff.

36 BVerfGE 55, 37, 68..

37 BVerwG, NVwZ 1991, 1082f.

Abhaltung, worunter auch die Aufzeichnung Lehrveranstaltung und deren spätere Verwendung fallen.

Kein Eingriff in die Freiheit der Lehre ist jedoch die Organisation und die Ausgestaltung der Lehre im Rahmen eines abgestimmten Lehrbetriebs. Freiheit benötigt nämlich geeignete Bedingungen zu ihrer Verwirklichung. Unter den Bedingungen heutiger Wissenschaft erfordert die Freiheit der Lehre in der Regel einen organisierten und finanzierten Lehrbetrieb. Diesen zu gewährleisten, ist Aufgabe des Staats. Die wichtigste Organisationsform zur Ausübung der Lehrfreiheit ist die Universität. Sie kann sich deshalb selbst auf die Lehrfreiheit berufen.[38]

Ein Lehrbetrieb in akademischer Selbstverwaltung ist somit Voraussetzung und nicht Einschränkung der Lehrfreiheit. Doch auch dieser muss die individuelle Lehrfreiheit beachten und sich auf die Organisation der Rahmenbedingungen beschränken. Hochschulen können allerdings zum Beispiel Räume und Zeiten an Lehrende zuweisen. Diese Ressourcenverteilung ermöglicht Lehre und schränkt sie nicht ein. Das gleiche gilt, wenn der Einsatz bestimmter technischer Hilfsmittel notwendig ist, um das Recht der Studierenden an der Teilnahme an der Lehrveranstaltung zu gewährleisten oder andere lehrbezogene Aufgaben der Hochschulen zu erfüllen.

Nach § 4 Abs. 1 HHG obliegt der Hochschule die „Aufgabe … der Vermittlung einer wissenschaftlichen Ausbildung“. Sie hat nach § 27 Abs. 1 HHG für jeden Studiengang ein Studienangebot sicherzustellen. Bei der Frage, ob der Ausbildungszweck der Hochschule Videoaufzeichnungen und -übertragungen rechtfertigt, ist nach den dargestellten verschiedenen Arten der Videoaufzeichnung- und -übertragung zu unterscheiden.

Kein Zweifel an der Notwendigkeit der Maßnahme kann bestehen, wenn nur durch die Hörsaalübertragung der berechtigte Anspruch der Studierenden auf Teilnahme an der Lehrveranstaltung bei den gegebenen Ressourcen befriedigt werden kann.

Das Gleiche muss aber auch gelten, wenn das Videosignal als Live-Stream an einen anderen Ort der Teilnehmer (z.B. nach Hause) oder in eine kooperierende Lehrveranstaltung einer anderen Hochschule in Deutschland oder im Ausland[39] direkt übertragen wird. Auch in diesem Fall kann diese Vorgehensweise eine ressourcenschonende Möglichkeit darstellen, um zum Beispiel räumliche Kapazitätsprobleme zu beheben oder mit einer anderen Hochschule in der Ausbildung zusammenzuarbeiten.

Aber auch die Aufnahme und Speicherung des Videos, um Studierenden eine zeitversetzte Teilnahme an den Veranstaltungen zu ermöglichen, dienen unmittelbar dem Ausbildungsauftrag. Sie sind zum einen eine Fortentwicklung der Lehre, die Studierenden eine zusätzliche, selbstbestimmte Art des Lernens ermöglicht, indem diese zum Beispiel in die Lage versetzt werden, selbst zu entscheiden, wann sie eine Vorlesung hören oder etwa zur Vorbereitung auf die Prüfung wiederholen möchten. Die Übertragung von Lehrveranstaltungen bedeutet jedoch nicht nur eine zusätzliche Erleichterung für Studierende, sondern ist für viele – wie bereits dargestellt – sogar die einzige Möglichkeit, regelmäßig an der Lehrveranstaltung teilzunehmen. Das gilt nicht nur für eine gelegentliche Erkrankung oder sonstige Verhinderung eines Studierenden (z.B. Arztbesuch). Nicht wenige Studierende betreuen neben ihrem Studium

---

38 BVerfGE 15, 256 (262); 35, 79 ff.; Pernice, in: Dreier, Art. 5 III (Wissenschaft), Rn. 17..

39 S. hierzu oben 2.

eine pflegebedürftige Person. Rund 30% der Studierenden müssen oder wollen selbst während der Vorlesungszeit einer (teilweisen) Beschäftigung nachgehen.[40]

Die Benachteiligung gilt in besonderem Maß für Studierende mit Kindern und für Studierende mit Behinderungen. Für diese fordert § 3 Abs. 4 Satz 2 HHG ausdrücklich, „die besonderen Bedürfnisse von Studierenden mit Kindern (zu berücksichtigen) und darauf hin (zu wirken), dass behinderte Studierende in ihrem Studium nicht benachteiligt werden und sie Angebote der Hochschule möglichst ohne fremde Hilfe in Anspruch nehmen können". Für diese beiden Gruppen sind Aufzeichnungen und Übertragungen der Lehrveranstaltungen ein Gebot der Chancengleichheit. Nach einer Schätzung der Hochschulrektorenkonferenz ist davon auszugehen, dass durchschnittlich 8% der Studierenden durch Krankheit behindert sind, ohne Einschränkung an Lehrveranstaltungen teilzunehmen.[41] Etwa 10% der Studierenden sind zusätzlich durch Kindererziehung beansprucht.[42]

Das Gleiche kann aber nicht uneingeschränkt für Aufzeichnungen gelten, die Lehrveranstaltungen über den Kreis der Teilnehmer hinaus der Öffentlichkeit zur Verfügung stellen sollen. Sie sind daher nicht mehr vom Ausbildungsauftrag und vom Auftrag chancengleicher Möglichkeiten der Teilnahme an Lehrveranstaltungen gedeckt. Diese Maßnahmen könnten allenfalls durch die Aufgabe der Hochschule nach § 3 Abs. 8 HHG gerechtfertigt sein, die Öffentlichkeit über die Bewertungen der Lehre zu informieren. Hierzu gehört auch die Information der Öffentlichkeit über Lehrformen und Lehrinhalte.[43]

Aufnahmen und Übertragungen von Lehrveranstaltungen sind nach den zuvor genannten Bedingungen rechtlich möglich. Insoweit wäre eine ausdrückliche Regelung nicht erforderlich. Die Rechtslage ist jedoch sehr kompliziert. Sie wird im Einzelfall immer wieder zu Streitigkeiten führen. Zur Verdeutlichung und Klarstellung der Verfassungsrechtslage könnte es sich daher anbieten, die gesetzlichen Regelungen für die spezifische Situation der Hochschule zu konkretisieren. Außerdem ist dann die Videoaufzeichnung und -übertragung unmittelbar durch die Satzung gerechtfertigt, Unsicherheiten insbesondere hinsichtlich der konkludenten Einwilligung der Studierenden bestehen nicht mehr. Diese Erhöhung der Rechtssicherheit erscheint erst recht geboten, wenn ohnehin eine Satzung zum Datenschutz in E-Learning-Verfahren erlassen wird.

Soweit Aufzeichnungen und Übertragungen rechtlich geregelt werden, sind diese Regelungen, die Eingriffe in das Recht am eigenen Bild darstellen, gerechtfertigt, wenn sie zur Verfolgung eines öffentlichen Interesses auf gesetzlicher Grundlage und in verhältnismäßiger Weise erfolgen.[44] Auch für verfassungsrechtlich akzeptable Bedingungen der Ausübung der Lehrfreiheit der Hochschullehrenden ist es erforderlich, dass sie für diesen Zweck geeignet, erforderlich und verhältnismäßig sind.

Werden Bilder von Studierenden aufgenommen oder übertragen, kann dies grundsätzlich durch den Ausbildungsauftrag der Hochschule gerechtfertigt sein. Allerdings ist fraglich, ob hierfür individuelle Aufnahmen von Studierenden erforderlich sind. Dies dürfte allenfalls in

---

40 Studentenwerk Kassel 2006, 10.

41 HRK, Pressemitteilung v. 22.4.2009, http://www.hrk.de/de/presse/95_4894.php

42 Studentenwerk Kassel 2006, 13.

43 S. zur vollständigen Abwägungen näher in Folgenden.

44 S. allg. zu den Voraussetzungen an Grundrechtseingriffe Jarass/Pieroth, GG, 10. Aufl. 2009, Art. 2, Rn. 59 ff .

bestimmten Situationen der Fall sein, etwa wenn der Lernstoff durch Referate der Studierenden vermittelt oder in kommunikativen Passagen mit den Studierenden entwickelt wird. In der üblichen Vorlesungssituation dürfte dies nicht erforderlich sein. Manchmal lässt es sich aber auch in diesen Fällen nicht vermeiden, Studierende auf Video zu erfassen. Wenn Hörsäle so geschnitten sind, dass Studierende regelmäßig ins Bild geraten oder der Lehrende sich im Hörsaal bewegt und dabei auch durch die Reihen der Studierenden geht, dann muss die Kamera ihm folgen und wird dabei zwangsläufig auch Studierende aufnehmen. Jedenfalls kann festgehalten werden, dass die Aufnahme und Übertragung von Studierenden zu Ausbildungszwecken – also bei Videoaufnahmen und -übertragungen an Teilnehmer der Lehrveranstaltung – zulässig sein kann, aus Gründen der Verhältnismäßigkeit aber auf das Unvermeidbare zu begrenzen ist.

Für die Öffentlichkeitsarbeit der Hochschule ist es zwar sinnvoll und auch notwendig, dass in im Videomaterial Studierende vorkommen, doch ist es nicht erforderlich, hierfür einzelne Studierende zu individualisieren. Sollte dies aus „dramaturgischen" Gründen notwendig sein, kann auf freiwillige Teilnehmer zurückgegriffen werden.

Für Lehrende stellt sich die Situation etwas anders dar. Für sie ergeben sich aus dem Lehrauftrag Bindungen in Form dienstlicher Pflichten.[45] Diese Bindungen sind insoweit gerechtfertigt, als sie durch den Ausbildungszweck und andere gesetzliche Aufgaben der Hochschule gedeckt sind.[46] Soweit Aufzeichnungen und Übertragungen von Lehrveranstaltungen vom Ausbildungszweck der Hochschule gefordert werden, müssen Lehrende diese akzeptieren.

Diese Maßnahmen verändern die Möglichkeiten freier Lehre nur gering. Der Kreis derer, die die übertragene Lehrveranstaltung zur Kenntnis nehmen können, ist der gleiche wie in einem ausreichend großen Hörsaal. Bei der Übertragung in einen anderen Hörsaal wird das Bild der Lehrperson etwas vergrößert dargestellt – ähnlich wie die Stimme durch ein Mikrofon verstärkt wird. Bei der Übertragung an Teilnehmer an anderen Orten über das Internet nimmt bei der Normaleinstellung der gängigen Softwareprogramme das Bild der Lehrperson nur ca. 10% des Bildschirms ein. In der Art und Weise des Lehrens und ich ihrer Bewegungsfreiheit im Hörsaal wird die Lehrperson in keiner Weise eingeschränkt.

Grundsätzlich bringt auch der Informationsauftrag der Hochschule gegenüber der Öffentlichkeit nach § 3 Abs. 8 HHG Bindungen für die Lehrenden mit sich. Jedoch muss die Information der Öffentlichkeit nicht in der Form erfolgen, dass vollständige Lehrveranstaltungen aufgezeichnet und der Öffentlichkeit zugänglich gemacht werden. Zu beachten ist hier, dass das Bereitstellen von Aufzeichnungen einer bestimmten Lehrveranstaltung zum weltweiten Zugriff über das Internet für beliebige Personen keine Voraussetzung zur Umsetzung der Lehrfreiheit ist und einen wesentlich stärkeren Eingriff in die Persönlichkeitsrechte der abgebildeten Lehrenden darstellt als die Zugangseröffnung allein für die Teilnehmer an der Lehrveranstaltung. Diesem verstärkten Eingriff in das Recht am eigenen Bild der Lehrenden steht keine Notwendigkeit gegenüber, den Auftrag zur Information der Öffentlichkeit ausgerechnet durch die Bereitstellung von vollständigen Aufzeichnungen von Lehrveranstaltungen zu erfüllen. Im Gegenteil ist die allgemeine Öffentlichkeit eher an Zusammenfassungen oder beispielhaften Ausschnitten interessiert. Daher kann nicht davon ausgegangen werden, dass die öffentliche Bereitstellung der Aufzeichnungen bestimmter Lehrveranstaltungen ohne weiteres vom In-

---

45 Starck 2005, Art 5 III, Rn. 377.

46 BVerfGE 55, 37, 68; Dreier 2004, Art 5 III, Rn. 33.

formationsauftrag der Hochschule gefordert ist. Der Lehrende muss eine Aufzeichnung und Bereitstellung seiner Lehrveranstaltung für die Öffentlichkeit daher nicht einfach hinnehmen.

Wenn immer mehr Hochschulen die Aufzeichnungen ganzer Lehrveranstaltungen im Internet zur Verfügung stellen, ist dies eine freiwillige Werbemaßnahme, die nicht von § 3 Abs. 8 HHG gefordert wird. Dementsprechend müssen die Hochschulen auch ihre Lehrenden für eine freiwillige Teilnahme an solchen Maßnahmen gewinnen. Diese Fall sollte daher nicht in der Satzung der Hochschule geregelt werden. Vielmehr sollte es bei der – aus verfassungsrechtlicher Sicht gebotenen – Erfordernis einer Einwilligung der Lehrenden bleiben.

Da sich die Einwilligung beim Recht am eigenen Bild nach den §§ 22, 23 KunstUrhG richtet, ist die Einwilligung formlos und sogar konkludent möglich. Wird sie jedoch nicht erteilt, zum Beispiel indem der Lehrende protestiert oder einer derartigen Verwendung widerspricht, so darf die Aufzeichnung nicht der allgemeinen Öffentlichkeit zur Verfügung gestellt werden. Widerruft der Lehrende seine einmal erteilte Einwilligung nachträglich, so muss das Video entfernt werden und darf nur noch zu den Zwecken verwendet werden, die keiner Einwilligung des Lehrenden bedürfen. Die bis dahin erfolgte Verwendung des Videos wird durch den Widerruf der Einwilligung jedoch nicht nachträglich rechtswidrig.

Rein rechtstechnisch gesehen, ist für die Aufzeichnung und Übertragung einer Lehrveranstaltung keine ausdrückliche Regelung erforderlich, da sich die Rechtsfolgen bereits aus der Anwendung der einschlägigen Gesetze ergeben. Zur Verdeutlichung und Klarstellung der Rechtslage könnte es sich jedoch anbieten, die gesetzlichen Regelungen für die spezifische Situation der Hochschule zu konkretisieren. Außerdem ist dann die Videoaufzeichnung und -übertragung unmittelbar durch die Satzung gerechtfertigt, Unsicherheiten insbesondere hinsichtlich der konkludenten Einwilligung der Studierenden bestehen nicht mehr. Diese Erhöhung der Rechtssicherheit erscheint erst recht geboten, wenn ohnehin eine Satzung zum Datenschutz in E-Learning-Verfahren erlassen wird.

Nach alledem könnte eine Regelung in der Datenschutzsatzung beispielsweise lauten:

> *„Die Aufzeichnung und die zeitgleiche oder zeitversetzte Übertragung einer Lehrveranstaltung ist zulässig, wenn dies durch den Ausbildungsauftrag der Hochschule geboten ist sowie technisch und organisatorisch sichergestellt ist, dass nur an der Lehrveranstaltung teilnehmende Personen die Aufzeichnung zur Kenntnis nehmen können. Über die Aufzeichnung und Übertragung einer Lehrveranstaltung sind die Teilnehmenden vor der Aufzeichnung zu informieren."*

5. E-Learning in vernetzten Systemen

E-Learning-Verfahren werden zunehmend in andere Anwendungen wie zum Beispiel ein Studierendenportal eingebunden oder mit anderen IT-Verfahren vernetzt. Ein typisches Beispiel hierfür ist eine Identitätsmanagement-Lösung mit einem Single Sign-On für viele verschiedene Anwendungen.[47] Single Sign-On-Systeme ermöglichen es, sich einmal gegenüber einem zentralen System zu authentifizieren, um danach transparent von anderen Systemen als authentifizierter Benutzer erkannt zu werden.[48] Nach einer einmaligen Authentifizierung kann

---

47 Zur Authentisierung in verteilten Systemen anhand eines Single-Sign-On-Verfahren s. Eckert 2006, 504 und 513.

48 Sams, Jaxenter 1/2008.

ein Benutzer auf alle Rechner und Dienste zugreifen, für die er Berechtigungen innehat, ohne sich jedes Mal neu anmelden zu müssen. Den Studierenden soll mit einer Single Sign-On Lösung im Universitätsnetzwerk der Zugriff auf möglichst viele Anwendungen eröffnet werden. Zu den Anwendungen gehören beispielsweise neben den E-Learning-Verfahren auch der E-Mail-Dienste, Hochschul-Informations-Systeme und Online-Vorlesungsverzeichnisse.

Durch diese Vernetzung entstehen Fragen nach dem Anwendungsbereich der Satzung. Datenverarbeitungsvorgänge in einem vernetzten System betreffen unter Umständen sowohl E-Learning-Verfahren als auch andere Anwendungen außerhalb von E-Learning-Angeboten. Für die Verarbeitung personenbezogener Daten in Bereichen, die ebenfalls vom Portal abgedeckt sind, aber nicht zum E-Learning zählen, sind andere Regeln einschlägig. Es können andere Satzungen oder Benutzungsordnungen anwendbar sein, unter Umständen existieren gar keine spezifischen Regeln und das Hessische Datenschutzgesetz ist anwendbar.

Unter Single-Sign-On ist nur der Vorgang einer einheitlichen Anmeldung zu verstehen. Im Hintergrund laufen aber, im Idealfall für den Nutzer nicht wahrnehmbar, verschiedene und separate Systeme. Jedes dieser Systeme muss so konfiguriert sein, dass es die jeweils geltenden rechtlichen Vorgaben erfüllt.

Es kann aber zu Datenverarbeitungsvorgängen kommen, die mehreren Anwendungen zuzurechnen sind. Zum Beispiel könnte der Teil des Systems, der für das Single-Sign-On zuständig ist, Zugriffe auf E-Learning-Verfahren mitloggen. Aus Sicht der Datenschutzsatzung für das E-Learning handelt es sich dann um Nutzungsdaten. Gleiches gilt für den einheitlichen Benutzernamen und das dazugehörige Passwort, die im Single-Sign-On vergeben werden und dann auch zum Zugriff auf die Daten aus den E-Learning-Verfahren des Nutzers berechtigen.

Die Tatsache, dass über Single-Sign-On auf die E-Learning-Verfahren zugegriffen wird, darf nicht zu einer Absenkung des Datenschutzniveaus führen. Für die oben beschriebenen Datenverarbeitungsvorgänge, die gleichzeitig dem E-Learning und anderen Anwendungen dienen, müssen daher Regeln gelten, die mindestens das datenschutzrechtliche Niveau der Satzung zum E-Learning gewährleisten.

Es erscheint sinnvoll, eine rechtliche Regelung zu treffen, die den Anwendungsbereich der Satzung auf alle Vorgänge der Datenverarbeitung ausdehnt, die zumindest auch das E-Learning betreffen. Nur so kann sichergestellt werden, dass vernetzte Systeme nicht dazu genutzt werden können, den Datenschutz beim E-Learning auszuhebeln.

Eine solche Regelung bezieht sich nur auf Datenverarbeitungsvorgänge, die sowohl dem E-Learning als auch anderen Anwendungen dienen. Wie oben beschrieben, dürfte eine solche Doppelnatur eines Datenverarbeitungsvorgangs nur bei einem sehr geringen Teil der Datenverarbeitung gegeben sein, da es sich zwar um vernetzte, aber doch eigenständige Systeme handelt. Handelt es sich um einen Vorgang, der eine solche Doppelnatur hat, müssen die Vorschriften der Satzung hierauf anwendbar sein. Kann der Datenverarbeitungsvorgang einer bestimmten Anwendung zugeordnet werden, sind die für diese Anwendung einschlägigen Vorschriften zu beachten.

In die Satzung sollte daher folgende Regelung aufgenommen werden:

„Erfolgt ein einheitlicher Vorgang des Umgangs mit personenbezogenen Daten zumindest auch für Zwecke des E-Learning, gelten die Vorschriften dieser Satzung auch für diesen Vorgang."

6. Anforderungen für E-Learning-Leistungsnachweise

Wenn Lehrveranstaltungen durch E-Learning unterstützt angeboten werden, liegt es nahe, auch den Leistungsnachweis in dieser Form zu erbringen. Der Nachweis einer Prüfungsleistung im Rahmen oder für den Abschluss eines Moduls stellt aber besondere Anforderungen an die Authentizität und Integrität sowie an die Nachweisbarkeit der zu erbringenden Leistung. Es ist daher zu untersuchen, welche rechtlichen Anforderungen an welche Formen von Nachweisen durch E-Learning-Verfahren gestellt werden müssen.

Besonderer Aufmerksamkeit bedürfen computergestützte Präsenzprüfungen.[49] Die Vorteile von computergestützt angebotenen und ebenso ausgewerteten Prüfungen sind offensichtlich: Automatische Korrekturen ersparen erhebliche Personalkosten und sind viel schneller durchzuführen, Studierenden können die Ergebnisse sehr viel zeitnäher mitgeteilt werden.

Es können aber Konflikte mit dem datenschutzrechtlichen Verbot der automatisierten Einzelentscheidung entstehen. Dieses Verbot ist in Art. 15 Abs. 1 DSRL festgelegt und wird durch § 7 Abs. 3 HDSG in nationales Recht umgesetzt. Die Vorschrift in der Datenschutzrichtlinie lautet:

„Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens."

Dieses Verbot, das zugleich ein subjektives Recht gewährt, betrifft einen Sonderfall der Verarbeitung personenbezogener Daten dar, von dem aus Sicht des Gesetzgebers ein erhöhtes Risiko- und Gefährdungspotenzial ausgeht.[50] Das Verbot beruht auf der Annahme, dass die Bewertung von Merkmalen einer Person immer von einem Menschen verantwortet werden muss und nicht vollständig einer technischen Vorrichtung überlassen werden darf.[51] Dabei soll die Vorschrift nicht verhindern, dass automatisierte Verfahren die Entscheidung vorbereiten. Zulässig ist der Vorgang aber nur, wenn die automatisierte Vorentscheidung nicht ungeprüft übernommen wird, sondern ein Mensch die Entscheidung aufgrund einer eigenen Wertung verantwortet.[52]

Die Umsetzung in § 7 Abs. 3 HDSG lautet:

„Unzulässig ist eine zu rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen führende Entscheidung, wenn sie auf einer Bewertung

---

49 S. dazu ausführlich Kalberg, DVBl. 2009, 21 ff.

50 S. Ehmann/Helfrich 1999, Art. 15, Rn. 1 m.w.N.

51 Nungesser 2001, Erl. § 7, Rn. 25.

52 Nungesser 2001, Erl. § 7, Rn. 26 m.w.N.

einzelner Merkmale seiner Person beruht, die ausschließlich durch eine automatisierte Verarbeitung seiner Daten erstellt wurde.“

Wird der Leistungsnachweis eines Studierenden als „nicht bestanden“ gewertet, so ist hierin eine „erhebliche Beeinträchtigung“ zu sehen, da das Wiederholen der Prüfung nur zwei Mal möglich ist und jedes Mal zumindest einen gewissen Zeitaufwand bedeutet, der bei einer bestandenen Prüfung entfiele.[53] Fraglich ist, ob die Bewertung eines Leistungsnachweises eine Bewertung einzelner Merkmale der Person des Studierenden darstellt. Aus der Vorgabe des Art. 15 Abs. 1 DSRL lässt sich entnehmen, dass hierunter auch die berufliche Leistungsfähigkeit des zu Bewertenden fällt. Gleiches gilt für die Ansicht des nationalen Gesetzgebers bei der Umsetzung von Art. 15 Abs.1 DSRL in § 7 Abs. 3 HDSG.[54] Mit der Bewertung einer Klausur als „nicht bestanden“, wird dem Prüfling abgesprochen, die für das mit dem Studium verbundene Berufsziel erforderlichen Kenntnisse und Fähigkeiten erworben zu haben. Daher sind in der Bewertung einer Klausur als „nicht bestanden“ eine Bewertung der Leistungsfähigkeit des Betroffenen und damit auch eine Bewertung von Leistungsmerkmalen zu sehen.[55]

Das Verbot des § 7 Abs. 3 HDSG betrifft aber nur solche Verfahren, bei denen die Entscheidung des Computers nicht noch einmal im Rahmen einer menschlichen Beteiligung überprüft wird, sondern unmittelbar zu einer Entscheidung führt, die dem Betroffenen so verkündet wird.[56] Solange aber eine Nachkorrektur stattfindet, liegt kein Verstoß gegen das datenschutzrechtliche Verbot der automatisierten Einzelentscheidung vor.[57] Da entscheidend ist, dass die Bewertung des Betroffenen *ausschließlich* auf einer automatisierten Entscheidung beruht, ist auch dann kein Verstoß gegen § 7 Abs. 3 HDSG gegeben, wenn dem Betroffenen die üblichen Rechte zur Remonstration zustehen und er eine Überprüfung seines Leistungsnachweises durch einen menschlichen Korrektor verlangen kann.[58]

Probleme können jedoch entstehen, wenn Studierende monieren, dass der bewertete Leistungsnachweis inhaltlich nicht mit dem abgegebenen Leistungsnachweis übereinstimmt. Bei Leistungsnachweisen, die mit Papier und Stift angefertigt werden, müssen die Studierenden ihren Leistungsnachweis unterschreiben. Durch die Verkörperung auf Papier besteht ein gewisser Integritätsschutz, da Radierungen, Streichungen und Ersetzungen im Regelfall Spuren hinterlassen. Die Unterschrift des Studierenden ist geeignet einen Nachweis der Authentizität zu erbringen.[59] Diese Vorteile bestehen bei rein digitalen Leistungsnachweisen nicht.

Bei E-Klausuren entstehen große Datenmengen und das Manipulationsinteresse ist sehr groß. Ein geeignetes Mittel zum Integritätsnachweis sind Zeitstempel, mit denen die „abgegebenen“ E-Klausuren unmittelbar nach „Abgabe“ versehen werden. Bei Zeitstempeln werden die Daten oder deren Hashwert mit einer Zeit verknüpft und dann digital signiert.[60] Durch die Sig-

---

53 Ebenso Kalberg, DVBl. 2009, 23; zur Frage, ob auch eine „rechtliche Folge“ vorliegt s. Kalberg, DVBl. 2009, 22f.

54 S. für die vergleichbare Vorschrift des § 6a BDSG BT-Drs. 14/4329, 37.

55 Kalberg, DVBl. 2009, 23.

56 Nungesser 2001, Erl. § 7, Rn. 25 f.

57 So Kalberg, DVBl. 2009, 23, die dies auch dann für gegeben hält, wenn der „menschliche Nachkorrektor nur Teile der Klausurbewertung einer Überprüfung unterzieht.“

58 So zu Recht und überzeugend Kalberg, DVBl. 2009, 23.

59 S. dazu ausführlich Gassen 2003, 102 ff.

60 Eckert 2006, 393.

nierung des Hashwerts ist gesichert, dass der Zeitstempel sich auf die E-Klausur bezieht, die danach nicht mehr unbemerkt geändert werden kann. Wird der Zeitstempel unmittelbar, also mit einer minimalen Zeitdifferenz, nach „Abgabe“ erzeugt, so ist dadurch auch gesichert, dass die E-Klausur nicht zwischen Abgabe und Zeitstempelung manipuliert wurde, weil hierfür keine Zeit war.

Die strengen Vorgaben des Signaturgesetzes an qualifizierte Zeitstempel nach § 9 SigG müssen hierfür nicht erfüllt sein. Ein externer Zertifizierungsdiensteanbieter muss daher nicht eingeschaltet werden. Es ist ausreichend, wenn die E-Klausuren mit der Systemzeit versehen und dann vom Verantwortlichen für das E-Learning-Verfahren qualifiziert signiert werden.

Daher sollte folgende Regelung in die Satzung aufgenommen werden:

> *„Jede automatisiert erstellt Bewertung eines Leistungsnachweises muss auf Antrag des betroffenen Studierenden von einem Korrektor überprüft werden. Elektronische Leistungsnachweise sind unmittelbar nach Abgabe mit einem elektronisch signierten Zeitstempel zu versehen.“*

7. Sicherung der Freiwilligkeit

Grundsätzlich soll die Datenverarbeitung, die für E-Learning-Verfahren erforderlich ist, durch die Datenschutz-Satzung abgedeckt sein. Die Einwilligung stellt zwar grundsätzlich ein gutes Mittel dar, die **Selbst**bestimmung der Studierenden zu garantieren. Wird die Einwilligung aber zum Regelfall und für die Erreichung des Studienziels unabdingbar, besteht bezogen auf die Studierenden die Gefahr, dass sie zu einer Formalität verkommt und nicht mehr freiwillig erteilt wird. Aber auch für die Hochschule ist die Einwilligung als Regelform der Legitimierung des Umgangs mit personenbezogenen Daten nachteilig, weil sie ein unter Umständen kompliziertes und umfangreiches Einwilligungsmanagement erfordert.[61]

Die Satzung soll daher die regelmäßig erforderliche Datenverarbeitung abdecken, nur für den Ausnahmefall, der durch die Satzung nicht gedeckt ist, soll eine Einwilligung vorgesehen werden. Diese ist allerdings nur dann wirksam, wenn sie freiwillig erteilt wird. Für die Frage der Freiwilligkeit ist nach der Art der Veranstaltung zu unterscheiden.

Grundsätzlich ist davon auszugehen, dass die Einwilligung dann freiwillig ist, wenn in den Fällen, in denen die Satzung die Verarbeitung personenbezogener Daten nicht rechtfertigt, verschiedene Möglichkeiten des Leistungsnachweises existieren. Dies bedeutet, dass bei Wahlpflichtveranstaltungen oder freiwilligen Zusatzleistungen im Regelfall von einer Freiwilligkeit der Einwilligung ausgegangen werden kann. Etwas anderes gilt bei Pflichtveranstaltungen, die von jedem Studierenden besucht werden müssen. Hier kann nicht davon ausgegangen werden, dass eine Einwilligung freiwillig erteilt wird, wenn der Leistungsnachweis nur erreicht werden kann, wenn in den Umgang mit personenbezogenen Daten eingewilligt wird. Eine nicht freiwillig erteilte Einwilligung ist aber unwirksam, da sie nicht den gesetzlichen Vorgaben entspricht.[62] Pflichtveranstaltungen dürfen also nicht in einer Form angeboten werden, die Datenverarbeitungen erfordert, in die Studierende einwilligen müssen, wenn sie die Veranstaltung besuchen wollen. Darüber hinaus darf die datenschutzrechtliche Einwilli-

---

61 S. hierzu im Folgenden.

62 Dies ist in § 4a Abs. 1 Satz 1 BDSG ausdrücklich festgelegt; s. allg. zum Erfordernis der freien Entscheidung bei Einwilligungen Holznagel/Sonntag, in: Roßnagel 2003, Kap. 4.8, Rn. 54.

gung eines Studierenden nicht gleichzeitig Voraussetzung für weitere Leistungen wie zum Beispiel die Erlangung eines Seminarplatzes sein. In einer solchen Konstellation wäre die Freiwilligkeit der Einwilligung nicht mehr gewahrt.[63]

Datenschutzrechtliche Einwilligungen sind nach § 7 Abs. 2 HDSG grundsätzlich schriftlich zu erteilen. Dies wäre wegen des Medienbruchs für E-Learning-Verfahren sehr umständlich. Greift § 13 Abs. 2 TMG, könnte jedoch die Einwilligung auch in dem dort beschriebenen elektronischen Verfahren erteilt werden. E-Learning Verfahren sind Telemedien im Sinn des § 1 Abs. 1 TMG, da sie elektronische Informations- und Kommunikationsdienste sind, die nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen bestehen, oder Rundfunk im Sinn von § 2 RStV sind.[64] Gemäß § 1 Abs. 1 Satz 2 TMG gelten die Regelungen des Telemediengesetzes auch für öffentliche Stellen, unabhängig davon, ob sie für die Nutzung ihrer Dienste ein Entgelt erheben. Für die Qualifikation als Telemediendienst kommt es daher weder auf den Umstand der Entgeltlichkeit noch auf den Faktor der unbestimmten Zahl von Nutzern an, die diesen Dienst in Anspruch nehmen: Ein Telemediendienst kann auch in geschlossenen Nutzergruppen angeboten werden, solange ein Anbieter-Nutzer-Verhältnis nach § 11 TMG vorliegt.[65]

Diese Regelungen des Telemediengesetzes gehen als spezielle Regelungen zum Datenschutz in ihrem Anwendungsbereich dem Hessischen Datenschutzgesetz vor. Das Telemediengesetz regelt jedoch nur den Umgang mit Bestands- und Nutzungsdaten, nicht aber den Umgang mit Inhaltsdaten. Diese sind allerdings umfangreich und haben eine gewichtige Bedeutung in einem E-Learning-Verfahren. Daher genügt die Anwendung des § 13 Abs. 2 TMG nicht, um für E-Learning-Verfahren einheitlich eine elektronische Form der Einwilligung zu nutzen. Daher sollte die Regelung des § 13 Abs. 2 TMG sinngemäß in die Datenschutz-Satzung übernommen und auf alle Daten – auch die Inhaltsdaten – ausgeweitet werden.

Daher wird folgende Formulierung vorgeschlagen:

> *An die Stelle der Schriftform tritt die elektronische Form, wenn der Verantwortliche sicherstellt, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen und sie jederzeit mit Wirkung auf die Zukunft widerrufen kann.*

Da nach dem Vorbild des § 13 Abs. 2 TMG für Nachweiszwecke die Einwilligung protokolliert werden muss, der Nutzer den Inhalt der Einwilligung jederzeit abrufen und sie jederzeit mit Wirkung auf die Zukunft widerrufen können muss, ist ein umfangreiches Einwilligungsmanagement notwendig. Jede Einwilligung ist zu protokollieren und zu jedem Nutzer sind die verschiedenen Einwilligungen, die er erteilt hat, zu speichern und ihm jederzeit zugänglich zu machen. Bei einem Widerruf ist der Wegfall der Rechtfertigung für die weitere Datenspeicherung und -verarbeitung an die E-Learning-Verfahren weiter zu melden, in der eine Löschung oder Sperrung der Daten durchzuführen ist.

Um das Einwilligungsmanagement handhabbar zu halten und individuelle Speicherungen unterschiedlicher Einwilligungstexte zu vermeiden, sollten diese typisiert und für gewisse

---

63 Ebenso Zilkens/Heinrich, RDV 2007, 12.

64 Zum Begriff Telemedien und seine Abgrenzung zum Rundfunk und zur Telekommunikation s. Roßnagel, NVwZ 2007, 744f.

65 S. Roßnagel, NVwZ 2007, 745. Zum TDDSG s. auch Roßnagel/Jandt/Müller/Gutscher/Heesen 2006, 71.

Zeiträume einheitlich genutzt werden. Hierzu wird vorgeschlagen, hochschulweit oder für Typen von E-Learning-Verfahren zumindest für die Dauer eines Semesters eine einheitliche Fassung der Einwilligungsklausel zu verwenden. Dies hat zwar den Nachteil, dass Änderungen oder Ergänzungen der Einwilligungsklausel erst zu Beginn des nächsten Semesters vorgenommen werden können. Dafür kann aber den Studierenden, die in diesem Semester eine Einwilligung erklärt haben, jederzeit die für dieses Semester geltende Einwilligungserklärung zugänglich gemacht werden, ohne individuell unterschiedliche Versionen personenbezogen speichern zu müssen. Diese Regelung sollte von den Verantwortlichen als operative Klugheitsregel beachtet werden, ohne sie aber als verpflichtend in die Datenschutz-Satzung aufzunehmen.

Zur Sicherung der Freiwilligkeit werden folgende Ergänzungen der Satzung empfohlen:

> *„Hat der Nutzer seine Einwilligung widerrufen, so sind seine personenbezogenen Daten zu löschen oder zu anonymisieren, sofern keine Vorschriften ihre weitere Aufbewahrung erfordern. Sofern durch die Löschung oder Anonymisierung die Bewertung eines Leistungsnachweises nicht mehr möglich ist, ist der Nutzer vor der Löschung oder Anonymisierung hierauf hinzuweisen. Die Teilnehme an einer Lehrveranstaltung darf nicht von der Einwilligung des Nutzers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden."*

8. Sicherheitsanforderungen an E-Learning-Verfahren

Die rechtlichen Vorgaben an den Umgang mit personenbezogenen Daten müssen durch technisch-organisatorische Maßnahmen unterstützt werden. Daher müssen in die Satzung auch Anforderungen aufgenommen werden, wie die E-Learning-Verfahren zu sichern sind. Dabei ist es aufgrund der ständigen Weiterentwicklung der Technik wenig sinnvoll, in der Satzung selbst konkret auszuformulieren, welche Verschlüsselungstechniken, Schlüssellängen oder ähnliche Sicherungsmaßnahmen erforderlich sind. Der Aufwand, der zur Gewährleistung der Datensicherheit zu betreiben ist, muss nach § 10 Abs. 1 Satz 2 HDSG immer in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.[66]

Sicherungsmaßnahmen sollen und dürfen nur dann ergriffen werden, wenn der Zweck des E-Learning-Verfahrens dies gebietet. Dabei ist zu berücksichtigen, dass viele E-Learning-Verfahren dem Konzept des Web 2.0 folgen und gerade dadurch ihren didaktischen Erfolg erzielen, dass sie den Teilnehmern die Möglichkeit geben, Inhalte einzugeben, zu ändern, zu lesen, in Gruppen zu bearbeiten, zu versenden und abzurufen. Daher kann sich die Zweckbestimmung des Umgangs mit den Daten, können sich die Rechte zum Zugriff oder zur Veränderung, die Notwendigkeit der Protokollierung und der Nachprüfbarkeit von Aktionen von E-Learning-Verfahren zu E-Learning-Verfahren stark unterscheiden. Zum Beispiel kann es dem Zweck angebotener E-Learning-Verfahren entsprechen, dass sie anonym zu nutzen sind. Dazu gehören solche Angebote wie eine „Meckerecke" oder die Evaluation.[67] Würden bei derartigen Angeboten die üblichen Sicherheitsmaßnahmen ohne Rücksicht auf das konkrete Angebot umgesetzt, so wäre dies kontraproduktiv. Bei einer Nachvollziehbarkeit und der Möglichkeit der Zuordnung von Bewertungen einer Lehrveranstaltung zum Nutzer, der sie abgegeben hat, würde sich dies negativ auf die Qualität der Ergebnisse der Angebote auswirken. Umgekehrt kann in anderen E-Learning-Verfahren sich die Leistungsbewertung auf Beiträge der

---

66 S. dazu Nungesser 2001, § 10, Rn. 7 ff.

67 Zum Datenschutz bei der Lehrevaluation an Hochschulen s. Wettern, DuD 2008, 29 ff.

Teilnehmer beziehen. In diesem Fall muss eindeutig nachvollziehbar sein, von wem die Einträge stammen. Deshalb sind die Vorgaben zur Datensicherung immer im Licht des konkreten Angebots auszulegen und zu verstehen.

Die Verpflichtung zur technisch-organisatorischen Sicherung der E-Learning-Verfahren sollte daher in die Satzung aufgenommen werden. Hierzu wird folgende Regelung vorgeschlagen:

> *„Der Verantwortliche hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die auf Grundlage dieser Satzung erhobenen und verwendeten Daten angemessen vor Missbrauch zu schützen. Erforderlich sind Maßnahmen dann, wenn sie nach dem Zweck des konkreten E-Learning-Verfahrens geboten sind und ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."*

Wer auf welche Daten aus Gründen des E-Learning, also um die mit den E-Learning-Verfahren verfolgten Zwecke zu erreichen, zugreifen darf, lässt sich nicht abstrakt ohne Rücksicht auf das konkrete E-Learning-Verfahren sagen. Erforderlich ist daher eine Regelung, die variabel ist und sich am Zweck des E-Learning-Verfahrens orientiert.

Dabei existieren mehrere Gruppen von möglicherweise Berechtigten. Vom Verantwortlichen für das E-Learning-Verfahren, über die anderen Teilnehmer einer Lehrveranstaltung, sämtlichen Mitgliedern der Hochschule und der Öffentlichkeit kann damit der Kreis derjenigen, die auf die Daten zugreifen dürfen, immer weiter gezogen werden. Die Begrenzung beginnt dabei schon mit den Verantwortlichen für das E-Learning-Verfahren. Obwohl sie Anbieter des Verfahrens ist, gibt es zahlreiche Konstellationen, in denen auch für sie ein Zugriff auf die Daten nicht notwendig ist. So kann es zum Beispiel erforderlich sein, um den Erfolg eines E-Learning-Verfahrens zu überprüfen, zu erfahren, ob ein konkretes Angebot überhaupt von den Nutzern angenommen wird. Dafür könnte es aus Sicht des Verantwortlichen erforderlich sein, zu wissen, wie viele Nutzer pro Woche auf bestimmte Daten zugreifen. Es ist aber nicht notwendig zu wissen, welche Nutzer dies genau sind oder auch wann sie zugreifen. Wenn die Zugriffsrechte an der Erforderlichkeit ausgerichtet werden, kann vermieden werden, dass einzelne Nutzer vom Verantwortlichen auf ihr Nutzungsverhalten angesprochen werden, welches zum Beispiel auch Rückschlüsse auf allgemeine Lern- und Lebensgewohnheiten zulassen könnte.

Eine Regelung muss daher abstrakt an der Erforderlichkeit des Zugriffs auf die Daten, um den Zweck des E-Learning-Verfahrens zu erreichen, orientiert werden. Ist der Zugriff auf die Daten durch eine Person oder Gruppe hierfür nicht erforderlich, ist er unzulässig.

Daher wird folgende Regelung zur Aufnahme in die Datenschutz-Satzung vorgeschlagen:

> *„Personenbezogene Daten von Nutzern dürfen nur dann der Öffentlichkeit oder den Mitgliedern der Hochschule oder den Teilnehmern einer Lehrveranstaltung oder dem Verantwortlichen für das E-Learning-Verfahren zugänglich gemacht werden, wenn dies erforderlich ist, um den Zweck des konkreten E-Learning-Verfahrens zu erreichen."*

Anforderungen zur Gewährleistung der Datensicherheit können nur technisch und organisatorisch umsetzen, was vorher rechtlich definiert wurde. Wer welche Daten zu welchem Zweck eingeben darf, wer welche Daten zu welchem Zweck zur Kenntnis nehmen, verändern, speichern, übertragen und löschen darf, welche Daten zu welchem Zweck zu protokollieren und

wem zur Verfügung zu stellen sind und die Beantwortung vieler weiterer Fragen zur Bestimmung der Berechtigungen und deren Grenzen sind von der konkreten Zielsetzung des E-Learning-Verfahren abhängig. Um die erforderlichen Sicherheitsmaßnahmen bestimmen zu können, ist es erforderlich, dass der Verantwortliche die Daten, Zwecke und Berechtigungen in einem kurzen Datenschutzkonzept beschreibt. Durch dieses erzeugt er nicht nur die notwendig Grundlage für die Bestimmung der erforderlichen Datensicherungsmaßnahmen. Indem er dieses den Nutzern zur Kenntnis bringt, kann er zugleich auch seine Informationspflichten erfüllen.

Daher wird empfohlen, die Vorschrift zu den Pflichten des Verantwortlichen wie folgt neu zu fassen:

> *"Der Verantwortliche hat für jedes E-Learning-Verfahren in einem kurzen, allgemeinverständlichen Datenschutzkonzept Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie die Rechte der Beteiligten zu beschreiben. Er hat das Datenschutzkonzept den Nutzern vor der Anmeldung zu einem E-Learning-Verfahren zugänglich zu machen und bis zum Abschluss des E-Learning-Verfahrens jederzeit abrufbar zu halten".*

Auch wenn die Ziele von E-Learning-Verfahren und die daraus abzuleitenden Datenschutzkonzepte sich stark unterscheiden können, werden dennoch typische Datensicherungsmaßnahmen immer wieder gefordert werden. Zumindest in Bezug auf diese typischen Datensicherungsmaßnahmen ist die Generalklausel zur Datensicherung in der Satzung so zu konkretisieren, dass sie den Verantwortlichen Anhaltspunkte gibt, welche Sicherungsmaßnahmen von ihnen gefordert werden. Dies betrifft vor allem Vorgaben zur Begrenzung des Zugriffs auf Daten, deren Weitergabe, die Nachvollziehbarkeit von Handlungen sowie die Gewährleistung der Verfügbarkeit und der Zweckbindung.

Ein wesentliches Sicherungsziel ist immer die Gewährleistung der Zweckbindung. Wie diese zu gewährleisten ist, muss für jedes E-Learning-Verfahren spezifisch festgelegt werden. Vielfach dürfte die Trennung von Funktionen, die Festlegung von Rollen und Berechtigungen (zum Beispiel Administrator, Verantwortlicher, Nutzer oder eine andere Rolle), die Begrenzung des Zugriffs nur über Anwendungen, die die verschiedenen Rollen umsetzen, und über die unterschiedliche Verschlüsselung der Datensätze erforderlich sein.[68]

Soweit nach dem Datenschutzkonzept eine Zugriffskontrolle erforderlich ist, geht es nicht nur darum, den Zugriff von Unberechtigten auf personenbezogene Daten zu verhindern. Vielmehr soll auch gewährleistet werden, dass der Zugriff der Berechtigten auf die Daten begrenzt bleibt, auf die sich ihre Berechtigung erstreckt. Ferner muss gesichert werden, dass die Berechtigten mit den Daten nur so verfahren können (nur Lesen, nur Eingeben, nur Verändern) wie es ihrer Berechtigung entspricht. Diese Begrenzungen sind in der alltäglichen Praxis wichtiger als die Abwehr der Zugriffe gänzlich Unberechtigter.[69] Dies kann erreicht werden durch Kontrolle der Zugriffsbefugnisse (nach Daten, Programmen und Art des Zugriffs), Protokollierung von Zugriffen, Funktionsbegrenzung und Verschlüsselung der Daten.[70]

---

68 S. dazu Heibey, in: Roßnagel 2003, 579 ff.; Ernestus, in: Simitis 2006, § 9, Rn. 163; Gola/Schomerus 2007, § 9, Rn. 29.

69 S. Ernestus, in: Simitis 2006, § 9, Rn. 100f.

70 S. dazu und zu weiteren Maßnahmen Heibey, in: Roßnagel 2003, 580 ff.; Ernestus, in: Simitis 2006, § 9, Rn. 108f.

In manchen E-Learning-Verfahren ist es notwendig, nachträglich feststellen zu können, welche Daten wann von wem eingegeben, aber auch verändert oder gelöscht oder an welche Stellen sie weitergegeben worden sind. Zu erreichen ist dieses Ziel regelmäßig nur durch eine Protokollierung der Zugriffe und Handlungen.[71] Eingaben, Änderungen, Löschungen und Weitergaben sind dann in besonderen Protokolldateien zu speichern. In die Protokolldateien sind auch gescheiterte Zugriffsversuche aufzunehmen. Müssen Protokolldateien ausgewertet werden, so muss dies nach dem Vier-Augen-Prinzip durch eine andere Person als den Systemadministrator geschehen.[72] Die Umsetzung dieser Sicherungsmaßnahmen kann abhängig vom konkreten E-Learning-Verfahren auch kontraproduktiv sein. In solchen Fällen ist auf diese Sicherungsmaßnahmen zu verzichten.

Schließlich ist auch ein Schutz vor zufälliger Zerstörung zu bieten und nicht nur vor dem absichtlichen, widerrechtlichen Löschen von Daten. Eine zufällige Zerstörung kann zum Beispiel durch Wasserschäden, Brände oder Stromausfälle eintreten.[73] Die Verfügbarkeit kann zum Beispiel durch Ausarbeitung eines Datensicherungskonzepts, regelmäßige Backups, Dokumentation von Sicherungsläufen und Testen der Restore-Funktion gewährleistet werden.[74]

Zur Ergänzung der Satzung wird folgende Regelung vorschlagen:

> *„Soweit dies nach dem Datenschutzkonzept des jeweiligen E-Learning-Verfahrens notwendig ist, sind vor allem Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass*
>
> 1. *die Zweckbindung erhobener Daten gewahrt wird,*
> 2. *ausschließlich die Berechtigten nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,*
> 3. *nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt und an welche Stellen sie weitergegeben worden sind,*
> 4. *personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.“*

---

71 Heibey, in: Roßnagel 2003, 592; Gola/Schomerus 2007, § 9, Rn. 26.

72 Ernestus, in: Simitis 2006, § 9, Rn. 144f.

73 Heibey, in: Roßnagel 2003, 584; Gola/Schomerus 2007, § 9, Rn. 28.

74 Ernestus, in: Simitis 2006, § 9, Rn. 159.

Vorschläge zur Änderungen der Satzung

zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren an der Universität Kassel

Änderungen *kursiv* und rot

§ 1 Geltungsbereich

(1) Diese Satzung gilt für die Verarbeitung personenbezogener Daten der Nutzer von E-Learning-Verfahren, die an der Universität Kassel zur Vermittlung einer wissenschaftlichen Ausbildung verwendet werden.

(2) Erfolgt ein einheitlicher Vorgang der Verarbeitung personenbezogener Daten zumindest auch für Zwecke des E-Learning, gelten die Vorschriften dieser Satzung auch für diesen Vorgang.

§ 2 Begriffsbestimmungen

Im Sinne dieser Satzung sind

1. E-Learning-Verfahren netzangebundene Lern-, Lehr- und Prüfverfahren, die personenbezogene Daten zum Zwecke der wissenschaftlichen Ausbildung erheben, verarbeiten und nutzen, und darauf zielen, das Lernen der Nutzer zu fördern und ihren Leistungsnachweis zu erbringen,

2. Nutzer Lehrende, Studierende, Zweithörer und Gasthörer im Sinne der §§ 15 und 16 Hessische Immatrikulationsverordnung, die E-Learning-Verfahren verwenden,

3. Verantwortliche für E-Learning-Verfahren jede Stelle der Hochschule, die E-Learning-Verfahren bereithält oder den Zugang zu ihrer Nutzung vermittelt.

§ 3 Grundsätze

(1) Der Verantwortliche darf beim Einsatz von E-Learning-Verfahren personenbezogene Daten der Nutzer verarbeiten, soweit diese Satzung oder eine andere Rechtsvorschrift dies ausdrücklich erlaubt. *Personenbezogene Daten von Nutzern dürfen nur dann der Öffentlichkeit oder den Mitgliedern der Hochschule oder den Teilnehmern einer Lehrveranstaltung oder dem Verantwortlichen für das E-Learning-Verfahren zugänglich gemacht werden, wenn dies erforderlich ist, um den Zweck des konkreten E-Learning-Verfahrens zu erreichen.*

(2) Der Verantwortliche darf personenbezogene Daten der Nutzer für andere als die in Absatz 1 genannten Zwecke *verarbeiten*, soweit der Nutzer eingewilligt hat. *Die Verarbeitung von Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben von Nutzern zu Zwecken des E-Learning ist nur auf Grundlage einer ausdrücklichen Einwilligung der betroffenen Nutzer zulässig.*

§ 4 Pflichten des Verantwortlichen

(1) Der Verantwortliche hat für jedes E-Learning-Verfahren in einem kurzen, allgemeinverständlichen Datenschutzkonzept Art, Umfang und Zwecke der Verarbeitung personenbezogener Daten sowie die Rechte der Beteiligten zu beschreiben. Er hat das Datenschutzkonzept den Nutzern vor der Anmeldung zu einem E-Learning-Verfahren zugänglich zu machen und bis zum Abschluss des E-Learning-Verfahrens jederzeit abrufbar zu halten

(2) Der Verantwortliche hat die Nutzung des E-Learning-Verfahrens anonym oder unter Pseudonym zu ermöglichen, soweit dies den in § 2 Nr. 1 genannten Zwecken nicht widerspricht und technisch möglich und zumutbar ist.

§ 5 Bestandsdaten

(1) Der Verantwortliche darf personenbezogene Daten der Nutzer wie Name, Anschrift, Matrikelnummer, Studienfach, Studiensemester oder E-Mail-Adresse nur verarbeiten, soweit sie für die Registrierung oder für die Nutzung von E-Learning-Verfahren an der Universität Kassel erforderlich sind.

§ 6 Nutzungsdaten

(1) Der Verantwortliche darf personenbezogene Daten eines Nutzers *wie insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung oder Angaben über die einzelnen vom Nutzer benutzten E-Learning-Verfahren* nur verarbeiten, soweit dies für die Nutzung dieser Verfahren erforderlich ist.

(2) Der Verantwortliche darf die Nutzungsdaten eines Nutzers über die Nutzung verschiedener E-Learning-Verfahren zusammenführen, soweit dies für die Wahrnehmung der in § 2 Nr. 1 genannten Zwecke erforderlich ist.

§ 7 Inhaltsdaten

Der Verantwortliche darf Kommunikationsinhalte jeglicher Art der Nutzer, unbeschadet von urheberrechtlichen Vorschriften verarbeiten, soweit dies für die in § 2 Nr. 1 genannten Zwecke erforderlich ist.

§ 8 Forschung

(1) Der Verantwortliche darf die in §§ 5, 6 und 7 genannten Daten zum Zwecke wissenschaftlicher Forschung verarbeiten, soweit dies für die Verfolgung konkreter Forschungszwecke erforderlich ist und schutzwürdige Belange des Nutzers wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Verwendung nicht beeinträchtigt werden.

(2) Eine Verarbeitung der in den Absatz 1 genannten Daten ist zu anderen als Forschungszwecken unzulässig. Sie dürfen nur zu Forschungszwecken und nur mit Einwilligung des Nutzers an andere Stellen übermittelt werden.

§ 9 Aufzeichnung und Übertragung von Lehrveranstaltungen

Die Aufzeichnung und die zeitgleiche oder zeitversetzte Übertragung einer Lehrveranstaltung ist zulässig, wenn dies durch den Ausbildungsauftrag der Hochschule geboten ist sowie tech-

nisch und organisatorisch sichergestellt ist, dass nur an der Lehrveranstaltung teilnehmende Personen die Aufzeichnung zur Kenntnis nehmen können. Über die Aufzeichnung und Übertragung einer Lehrveranstaltung sind die Teilnehmenden vor der Aufzeichnung zu informieren.

§ 10 Anforderungen an Leistungsnachweise

Jede automatisiert erstellt Bewertung eines Leistungsnachweises muss auf Antrag des betroffenen Studierenden von einem Korrektor überprüft werden. Elektronische Leistungsnachweise sind unmittelbar nach Abgabe mit einem elektronisch signierten Zeitstempel zu versehen.

§ 11 Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Nutzers beruht. Er ist auf den vorgesehenen Zweck der Verarbeitung sowie soweit erforderlich auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) An die Stelle der Schriftform tritt die elektronische Form, wenn der Verantwortliche sicherstellt, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen und sie jederzeit mit Wirkung für die Zukunft widerrufen kann. Hat der Nutzer seine Einwilligung widerrufen, so sind seine personenbezogenen Daten zu löschen oder zu anonymisieren, sofern keine Vorschriften ihre weitere Aufbewahrung erfordern. Sofern durch die Löschung oder Anonymisierung die Bewertung eines Leistungsnachweises nicht mehr möglich ist, ist der Nutzer von der Löschung oder Anonymisierung hierauf hinzuweisen. Die Teilnehme an einer Lehrveranstaltung darf nicht von der Einwilligung des Nutzers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden.

§ 12 Speicherfristen

(1) Die in § 5 genannten Bestandsdaten sind bis zur Exmatrikulation zu speichern. Auf Antrag des Nutzers können diese Daten auch früher gelöscht werden. Bestandsdaten der Zweithörer und Gasthörer nach §§ 15 und 16 Hessische Immatrikulationsverordnung sind solange zu speichern, wie sie an Lehrveranstaltungen der Universität Kassel teilnehmen dürfen.

(2) Die in § 6 genannten Nutzungsdaten sind unverzüglich nach dem Nutzungsvorgang zu löschen, es sei denn, sie sind für die Durchführung eines E-Learning-Verfahrens oder für die Erbringung eines Leistungsnachweises erforderlich.

(3) Die in §§ 7 *und 9* genannten Inhaltsdaten sind bis zum Ende des jeweiligen Semesters zu löschen, in dem das E-Learning-Verfahren eingesetzt wird. Die Speicherungsfrist von elektronischen Abschlussarbeiten wird nach der allgemeinen Aufbewahrungsregelung für Abschlussarbeiten bestimmt.

§ 13 Datensicherheit

(1) Der Verantwortliche hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die auf Grundlage dieser Satzung erhobenen und verwendeten Daten angemessen vor Missbrauch zu schützen. Erforderlich sind Maßnahmen dann, wenn sie nach dem Zweck des konkreten E-Learning-Verfahrens geboten sind und ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Soweit dies nach dem Datenschutzkonzept des jeweiligen E-Learning-Verfahrens notwendig ist, sind vor allem Maßnahmen zu treffen, die geeignet sind, zu gewährleisten, dass

1. *die Zweckbindung erhobener Daten gewahrt wird,*

2. *ausschließlich die Berechtigten nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,*

3. *nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt und an welche Stellen sie weitergegeben worden sind,*

4. *personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.*

§ 14 In-Kraft-Treten, Befristung

Die Satzung tritt am Tag nach ihrer Veröffentlichung im *Mitteilungsblatt der Universität Kassel* in Kraft. Ihre Geltungsdauer wird auf fünf Jahre begrenzt, Spätestens vier Jahre nach In-Kraft-Treten legt der Präsident *oder* die Präsidentin in Abstimmung mit dem *oder* der Datenschutzbeauftragten einen Erfahrungsbericht über die Handhabung und Wirksamkeit der Satzung vor, der bei Bedarf auch Vorschläge zur Überarbeitung, insbesondere zur Konkretisierung, erhalten soll.

Literaturverzeichnis:

Artikel-29-Datenschutzgruppe, Arbeitsdokument: Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer, Working Paper 74, 3.6.2003, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_de.pdf.

Artikel-29-Datenschutzgruppe, Arbeitsunterlage: Übermittlungen personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU, Working Paper 12, 24.6.1998, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_de.pdf.

Cremer, H., „…und welcher Rasse gehören Sie an?“ – Zur Problematik des Begriffs „Rasse“ in der Gesetzgebung, Deutsches Institut für Menschenrechte (Hrsg.), Policy Paper vom 8.9.2008, http://files.institut-fuer-menschenrechte.de/488/d81_v1_file_48b3bc51eb1d9_pp_rasse.pdf.

Dreier, H., Grundgesetz, Band 1, 2. Aufl., Tübingen 2004.

Eckert, C., IT-Sicherheit, 4. Aufl., München u.a. 2006.

Ehmann, E./Helfrich, M., Datenschutzrichtlinie – Kurzkommentar, Köln 1999.

Flisek, C., Datenschutzrechtliche Fragen des E-Learning an Hochschulen, CR 2004, 62 – 69.

Gassen, D., Digitale Signaturen in der Praxis, Köln 2003.

Gola, P./Schomerus, R., Bundesdatenschutzgesetz – Kommentar, 9. Auflage, München 2007.

Holzhausen, H., Die Safe-Harbor-Vereinbarung als Methode zur Sicherung eines „angemessenen Datenschutzniveaus“ im Sinne der EG-Datenschutzrichtlinie, 2002, http://www-en.eulisp.uni-hannover.de/media/Abschlussarbeiten/holzhausen_heike.pdf.

Kalberg, N., Rechtsfragen computergestützter Präsenzprüfungen im Antwort-Wahl-Verfahren, DVBl. 2009, 21 – 28.

Kuner, C., European Data Protection Law, 2. Aufl., Oxford 2007.

Libertus, M., Die Einwilligung als Voraussetzung für die Zulässigkeit von Bildnisaufnahmen und deren Verbreitung, ZUM 2007, 621 – 628.

v. Mangoldt, H./Klein, F./Starck, C., Das Bonner Grundgesetz, Band 1, 5. Aufl. München 2005.

Maurer, H., Allgemeines Verwaltungsrecht, 16. Aufl., München 2006.

Nungesser, J., Hessisches Datenschutzgesetz unter Berücksichtigung der EG-Datenschutzrichtlinie, 2. Aufl., Stuttgart 2001.

Roßnagel, A., Handbuch Datenschutzrecht, München 2003.

Roßnagel, A., Anmerkung zu EuGH, Urteil vom 6.11.2003 – Rs. C-101/01 (Lindqvist/Schweden), MMR 2004, 95 ff., MMR 2004, 99 – 100.

Roßnagel, A., Das Telemediengesetz, NVwZ 2007, 743 – 748.

Roßnagel, A./Jandt, S./Müller, J./Gutscher, J./Heesen, J., Datenschutzfragen mobiler kontextbezogener Systeme, Wiesbaden 2006.

Roßnagel, A./Pfitzmann, A./Garstka, H., Modernisierung des Datenschutzrechts, Rechtsgutachten für das Bundesinnenministerium, Berlin 2001.

Rost, M., Datenschutz und Datensicherheit an deutschen Hochschulen, DANA 2008, 11 – 14.

Sams, B., Single-Sign-On-Systeme – Eine Übersicht, Jaxenter 1/2008, http://it-republik.de/jaxenter/artikel/Single-Sign-On-Systeme-1499.html.

Schnabel, C., Das Recht am eigenen Bild und der Datenschutz, ZUM 2008, 657 – 662.

Simitis, S., Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden 2006.

Spindler, G./Schuster, F., Recht der elektronischen Medien, München 2008.

Studentenwerk Kassel, Sozialerhebung 2006, http://www.studentenwerk-kassel.de/fileadmin/user_upload/Startseite_PDFs/18_Sozialerhebung_online.pdf.

Wettern, M., Schutz von Studierenden-Daten, RDV 2006, 14 – 18.

Wettern, M., Lehrevaluation an Hochschulen, DuD 2008, 29 – 33.

Zilkens, M./Heinrich, C., Entbindet die Freiheit von Forschung und Lehre den Hochschullehrer von der Beachtung des Datenschutzes?, RDV 2007, 9 – 14.