Erläuterungen zur Satzung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren an der Philipps-Universität Marburg

Diese Erläuterungen sollen dem besseren Verständnis der Satzung zum Schutz personenbezogener Daten bei multimedialer Nutzung von E-Learning-Verfahren an der Universität Marburg und ihrer Umsetzung dienen.

Die Befolgung rechtlicher Vorschriften ist eine Voraussetzung für die Akzeptanz von E-Learning-Verfahren durch die Studierenden und Lehrenden. Ziel der Satzung ist es, die rechtlichen Anforderungen durch Bundes- und Landesgesetze und europarechtliche Vorgaben in Einklang zu bringen mit den Anforderungen, die aus technischer Sicht an ein funktionierendes, zuverlässiges und effizientes E-Learning-System zu stellen sind.

Erläuterung zu § 1:

Die Vorschrift bestimmt den Anwendungsbereich der Satzung. Der Begriff der „E-Learning-Verfahren" wird in § 2 Nr. 1 näher definiert. Durch ihn wird klargestellt, dass die Satzung keinen Einfluss auf zum Beispiel urheberrechtliche Fragen haben soll. Der Begriff des „Verarbeitens" entspricht dem des § 2 Abs. 2 Hessisches Datenschutzgesetz (HDSG) und umfasst allgemein alle Phasen vom Erheben der Daten bis zum Nutzen. Der Begriff der „personenbezogenen Daten" stammt aus dem allgemeinen Datenschutzrecht. Daten sind dann personenbezogenen, wenn sie sich einer natürlichen Person zuordnen lassen. Ob dies möglich ist, kann von zusätzlichen Informationen abhängen, die der Datenverarbeiterin oder dem Datenverarbeiter zur Verfügung stehen. Daten können daher für eine Datenverarbeiterin oder einen Datenverarbeiter keinen Personenbezug haben, für eine oder einen anderen aber, die oder der Zugang zu weiteren Informationen hat (zum Beispiel ein Mitarbeiterinnen- und Mitarbeiterverzeichnis oder eine Liste der für eine Veranstaltung angemeldeten Studierenden), personenbezogene Daten sein.

Diese Satzung gilt nur, wenn personenbezogene Daten verarbeitet werden. Sind die Daten anonymisiert, fehlt der Personenbezug. Sind die Daten einem Pseudonym zugeordnet, handelt es sich nicht zwangsläufig um personenbezogene Daten. Aus der Sicht der- oder desjenigen, die oder der eine Liste hat, in der die Pseudonyme den Klarnamen zugeordnet werden, liegen personenbezogene Daten vor. Dies bedeutet, dass die- oder derjenige, der Zugang zur Liste hat, die Daten als personenbezogene Daten und damit nach den Vorschriften dieser Satzung zu behandeln hat. Haben die Daten keinen Personenbezug, so ist ein Umgang mit ihnen unproblematisch, da sie kein Risiko für die Rechte der Betroffenen darstellen.

Die Satzung gilt nur für die Universität Marburg. Externe Nutzerinnen und Nutzer können an E-Learning- Verfahren der Universität Marburg teilnehmen, wenn sie die Satzung für sich als gültig anerkennen. Für die Übertragung von personenbezogenen Daten ins Ausland gelten die allgemeinen Vorschriften des § 17 HDSG. Danach können personenbezogene Daten in andere Mitgliedstaaten der Europäischen Union nach den Vorgaben dieser Satzung übermittelt werden. In andere Staaten außerhalb der Europäischen Union dürfen personenbezogene Daten nach § 17 Abs. 2 Satz 1 HDSG nur dann übermittelt werden, wenn die Datenübermittlung ausschließlich im Interesse des Betroffenen liegt oder beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist. Ein angemessenes Schutzniveau hat die Europäische Kommission bisher nur für Argentinien, die Schweiz, Kanada, Guernsey, Jersey und die Isle of Man anerkannt. Es fehlt für die USA und alle asiatischen und afrikanischen Länder. Kooperationen mit Zugriffen aus einer Universität aus diesen Ländern auf personenbezogene Daten in der Universität Marburg sind nur zulässig, wenn diese Universität sich einem ausreichenden Verhaltenskodex unterworfen hat und diesen für sich als verbindlich anerkennt. In diesem Fall ist der Hessische Datenschutzbeauftragte zu kontaktieren, der abschließend entscheidet,

ob die einseitigen Garantien der ausländischen Hochschule den Anforderungen der Datenschutzrichtlinie genügen und eine Übermittlung von personenbezogenen Daten daher zulässig ist oder nicht.

Greifen Lehrende der Universität Marburg aus einem Staat mit nicht angemessenem Datenschutzniveau auf E-Learning-Verfahren in der Universität Marburg zu, ist dies keine Übermittlung, da sie Verantwortliche der Universität Marburg bleiben, und damit nach den Verwendungsregeln dieser Satzung zulässig. Aufgrund des nicht angemessenen Datenschutzniveaus in dem Gastland sollte dies aber möglichst unterlassen werden.

Abs. 2 bestimmt den Anwendungsbereich in verteilten Systemen. Er gilt nur für Datenverarbeitungsvorgänge, die sowohl dem E-Learning als auch einer weiteren Anwendung zuzuordnen sind. Er gilt also nur, wenn mehrere Zwecke untrennbar in einem einheitlichen Datenverarbeitungsvorgang zusammenkommen. Im Regelfall dürften die Systeme zwar vernetzt, aber dennoch eigenständige Systeme sein. Die Rechtmäßigkeit der Datenverarbeitungsvorgänge ist dann für das jeweilige System nach den jeweils einschlägigen Vorschriften zu beurteilen. Für Vorgänge, die nur unter anderem dem E-Learning dienen, also zum Beispiel die Anmeldung in einem Single-Sign-On-System, gelten die Regeln der Satzung zum Datenschutz im E-Learning. Durch § 1 Abs. 2 wird der Anwendungsbereich entsprechend ausgedehnt, so dass sich die Datenverarbeitung nach den folgenden Vorgaben zu richten hat.

Erläuterung zu § 2:

Nr. 1 definiert E-Learning-Verfahren und damit auch den Anwendungsbereich der Satzung, da diese auf E-Learning-Verfahren beschränkt ist. Zur Anwendbarkeit der Satzung, wenn eine Datenverarbeitung sowohl dem E-Learning als auch anderen Anwendungen dient, siehe § 1 Abs. 2.

Als Nutzerinnen und Nutzer erfasst Nr. 2 sowohl Studierende als auch Lehrende. Lehrenden kommt eine Doppelrolle zu: Sie sind sowohl nach Nr. 2 Nutzerin oder Nutzer, soweit sie an E-Learning-Verfahren teilnehmen, als auch Verantwortliche nach Nr. 3, soweit sie E-Learning-Verfahren im Rahmen ihrer Lehrveranstaltungen anbieten. In ihrer Rolle als Nutzerin oder Nutzer müssen auch Lehrende es dulden, dass ihre personenbezogenen Daten nach den Vorschriften dieser Satzung verarbeitet werden.

Externe Nutzerinnen und Nutzer, die nicht Mitglieder der Hochschule sind, können von einer Satzung der Hochschule nicht erfasst werden. Für sie gelten die Regelungen der Satzung aber dadurch, dass sie die Benutzungsordnung für Informationsverarbeitungs- und Kommunikationssysteme der Universität anerkennen müssen, wenn sie an E-Learning-Verfahren teilnehmen wollen, die in §9 auf ergänzende Regelungen verweist. Zur Übermittlung von Daten ins Ausland siehe auch die Erläuterungen zu § 1.

Nr. 3 definiert die oder den Verantwortlichen für ein E-Learning-Verfahren. Diese oder dieser ist nicht identisch mit der „datenverarbeitenden Stelle“ der Datenschutzgesetze. Diese ist immer die Universität Marburg. Der Begriff der oder des Verantwortlichen soll die Verantwortung innerhalb der Universität Marburg zum Ausdruck bringen. Verantwortlich ist jeweils die Stelle, die Einfluss auf die spezifische Funktion des E-Learning-Verfahrens hat. Dies ist nicht nur die oder der Lehrende, welche oder welcher das E-Learning-Verfahren anbietet und dessen Inhalte bestimmt, sondern auch das Hochschulrechenzentrum, das über die (Datenschutz-)Funktionen vieler E-Learning-Verfahren bestimmt.

Erläuterung zu § 3:

Abs. 1 Satz 1 hält fest, dass eine Verarbeitung personenbezogener Daten nur dann zulässig ist, wenn diese Satzung oder eine andere Vorschrift dies ausdrücklich erlauben. Der Begriff der „personenbezogenen Daten“ wurde in den Erläuterungen zu § 1 näher dargestellt.

Jede Verarbeitung von Daten in E-Learning-Verfahren muss nach dieser Satzung gerechtfertigt sein, wenn sie sich auf „personenbezogene Daten“ bezieht.

Daten dürfen nur dann Personen, auch Lehrenden, zugänglich gemacht werden, wenn dies erforderlich ist, um das Ausbildungsziel zu erreichen. Ausgeschlossen sind dadurch alle Verwendungsweisen, die anderen Zwecken dienen und deshalb erfolgen, weil die Daten „ja ohnehin vorliegen“. Eine Verarbeitung von personenbezogenen Daten, die nicht dem E-Learning dient, ist nach Abs. 2 Satz 1 nur aufgrund einer Einwilligung des betroffenen Studierenden zulässig.

Abs. 2 Satz 2 regelt die Verarbeitung besonders schützenswerter Daten (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben). Diese ist auch zu Zwecken des E-Learning nur zulässig, wenn eine ausdrückliche Einwilligung der betroffenen Nutzerinnen und Nutzer vorliegt. Dem liegt die Annahme zugrunde, dass der Umgang mit diesen Daten grundsätzlich ein höheres Risiko für die Persönlichkeitsrechte der Betroffenen darstellt als „normale“ Daten. Eine solche Einwilligung ist jedoch nicht bereits dann notwendig, wenn Daten verarbeitet werden, aus denen sich Rückschlüsse auf besonders schützenswerte Angaben zulassen. Ansonsten unterläge jedes Bild, das die Hautfarbe der oder des Abgebildeten erkennen lässt (rassische und ethnische Herkunft), eine Brillenträgerin oder einen Brillenträger (Gesundheit) oder eine Kopftuchträgerin (religiöse Überzeugung) zeigt, dieser besonderen Anforderung. Die erhöhten Anforderungen greifen nur dann, wenn die besondere Information als solche gespeichert wird, wenn also die Studierenden zum Beispiel nach Religionszugehörigkeit oder Gesundheitszustand kategorisiert werden. Derartige Datenverarbeitungsvorgänge greifen tief in die Persönlichkeitsrechte der betroffenen Nutzerinnen und Nutzer ein und sollten daher grundsätzlich vermieden werden. Sind sie aus Gründen des E-Learning notwendig, so sind sie trotzdem nur auf Grund einer ausdrücklichen Einwilligung der Nutzerinnen und Nutzer zulässig. Besonders für diese Angaben sollte von den Möglichkeiten der Anonymisierung der Daten Gebrauch gemacht werden.

Erläuterung zu § 4:

Abs. 1 regelt zwei Pflichten der oder des Verantwortlichen. Zum einen hat sie oder er in einem kurzen, allgemeinverständlichen Datenschutzkonzept zu beschreiben, welche Daten für welchen didaktischen Zweck erhoben und verwendet werden und wer deshalb zu welchen Handlungen berechtigt sein soll. Dieses Datenschutzkonzept ist die Voraussetzung dafür, die notwendigen Maßnahmen der Datensicherheit nach § 13 konkret festzulegen. Zum anderen bestimmt die Vorschrift zugleich den Umfang der notwendigen Information der Nutzerin oder des Nutzers. Das Datenschutzkonzept muss der Nutzerin oder dem Nutzer bereits vor der Anmeldung zum E-Learning-Verfahren und danach bis zu dessen Abschluss jederzeit zur Verfügung stehen.

Abs. 2 sieht ausdrücklich vor, dass Nutzerinnen und Nutzer die Möglichkeit haben sollen, E-Learning-Verfahren anonym oder unter einem Pseudonym zu nutzen. Die Verarbeitung anonymer Daten stellt kein Risiko für die Persönlichkeitsrechte der Betroffenen dar, wenn keine Möglichkeit besteht, die Daten zu re-personifizieren. Der schützende Effekt einer Datenverarbeitung unter einem Pseudonym tritt nur dann ein, wenn die Referenzliste, also die Datei, die Klarnamen und Pseudonyme miteinander verbindet, nicht frei verfügbar ist und auch sonst keine einfache Möglichkeit besteht, die Pseudonyme bestimmten Personen zuzuordnen. Verantwortliche für E-Learning-Verfahren sind gehalten, die Nutzung ihrer Verfahren anonym oder unter einem Pseudonym anzubieten, und so die Persönlichkeitsrechte der Betroffenen nicht stärker zu beeinträchtigen als notwendig.

Der zweite Halbsatz von Abs. 2 stellt zwei Bedingungen dafür auf, dass Verantwortliche ihre E-Learning-Verfahren anonym oder unter Pseudonym anbieten müssen. Die erste Bedingung ist, dass eine derartige Nutzung nicht dem Ziel widerspricht, das Lernen der Nutzerinnen und Nutzer zu fördern, und

ihnen ermöglicht, ihren Leistungsnachweis zu erbringen. In E-Learning-Verfahren, in denen der Leistungsnachweis zum Beispiel durch Mitarbeit in einem Wiki erbracht wird, kann dies nicht anonym geschehen, da die oder der Lehrende dann nicht nachvollziehen kann, wer den Leistungsnachweis erbracht hat und wer nicht. Die andere Voraussetzung ist, dass die Teilnahme anonym oder pseudonym technisch möglich sein muss und keinen unzumutbaren Aufwand verlangen darf. Unzumutbar ist der Aufwand dann, wenn angesichts des Risikos für die informationelle Selbstbestimmung der Betroffenen der zeitliche oder finanzielle Aufwand nicht vertretbar wäre. So könnte rein technisch bei der Übertragung einer Lehrveranstaltung die Gesichter aller zufällig erfassten Studierenden durch Verpixelung unkenntlich gemacht werden. Solange dies aber nicht automatisiert erfolgt, würde der Aufwand hierfür die Kapazitäten eines Fachgebiets bei weitem übersteigen, ohne im Regelfall einen spürbaren Gewinn für die informationelle Selbstbestimmung der Betroffenen zu bieten. Es könnten aber besondere Umstände vorliegen, die in Ausnahmefällen genau diese Maßnahme doch erforderlich machen. Das Kriterium der Zumutbarkeit entbindet nicht von der Pflicht einer sorgfältigen Prüfung des Einzelfalles.

Erläuterung zu § 5:

Bestandsdaten sind die so genannten Grunddaten eines Verhältnisses zwischen einer Anbieterin oder einem Anbieter und einer Nutzerin oder einem Nutzer. Diese Daten zeichnen sich durch eine gewisse Beständigkeit aus, auch wenn sie sich grundsätzlich ändern können. Die Aufzählung der Bestandsdaten ist nicht abschließend. Diese Daten dürfen nur verarbeitet werden, wenn und soweit dies für die Registrierung oder für die Nutzung von E-Learning-Verfahren erforderlich ist. Dies ist zum Beispiel der Fall, wenn ein E-Learning-Verfahren nur an Studierende eines bestimmten Studiengangs oder ab einem bestimmten Semester gerichtet sein soll. Die Bestandsdaten müssen aber für die Registrierung oder die Nutzung unerlässlich sein. Möchte eine Lehrende oder ein Lehrender nur aus Interesse gerne wissen, ob ihre bzw. seine Veranstaltung häufiger von Studierenden niedriger oder höherer Semester besucht wird, so ist dies weder für die Registrierung noch für die Nutzung erforderlich und daher auch nicht nach dieser Vorschrift zulässig.

Erläuterung zu § 6:

Nutzungsdaten sind Daten, die bei der aktuelle Nutzung von E-Learning-Verfahren anfallen, wie zum Beispiel Passwörter, Nutzerkennungen, Logfiles über Zugriffe auf E-Learning-Inhalte und ähnliche Daten. Die Aufzählung in Abs. 1 ist nicht abschließend.

Nach Abs. 1 darf die Verarbeitung dieser Daten nur erfolgen, soweit dies für die Nutzung von E-Learning-Verfahren erforderlich ist. Dies ist zum Beispiel der Fall, um überhaupt den Zugriff auf E-Learning-Inhalte zu ermöglichen. Eine weitergehende Verwendung ist jedoch nur dann zu lässig, wenn sie erforderlich ist, um den Zweck des E-Learning-Verfahrens zu erreichen. Eine Lehrende oder ein Lehrender darf daher nicht aus bloßem Interesse nachschauen, welche Studierende zu welchem Zeitpunkt E-Learning-Verfahren genutzt haben. Die Daten können aber zum Beispiel für das Skillmanagement genutzt werden. Im Rahmen des Skillmanagement werden je nach Vorwissen der einzelnen Nutzer und unter Berücksichtigung ihrer individuellen Lernziele nutzergerechte Lernangebote automatisiert durch das System unterbreitet. Diese Zielgenauigkeit von Lerninhalten wird in der Regel durch die Erstellung von Nutzerprofilen unterstützt, für die die Verarbeitung von Nutzungsdaten erforderlich ist.

Nutzungsdaten können für eine allgemeine Kontrolle der Akzeptanz und Auswertung des Nutzungsverhaltens genutzt werden, wenn sie anonymisiert sind. Der Zweck einer allgemeinen Verbesserung des Angebots kann auch mit Nutzungsdaten ohne Personenbezug erreicht werden.

Abs. 2 ermöglicht der oder dem Verantwortlichen für ein E-Learning-Verfahren, Nutzungsdaten aus verschiedenen E-Learning-Verfahren zusammenzuführen, wenn dies erforderlich ist, um das Lernen

der Nutzerinnen und Nutzer zu fördern und ihren Leistungsnachweis zu bewerten. Will eine Verantwortliche oder eine Verantwortlicher wissen, welche weiteren Angebote von den Nutzerinnen und Nutzern seines Verfahrens noch genutzt werden oder, ob Nutzerinnen oder Nutzer andere Verfahren auf die gleiche Art und Weise nutzen wie das seine, so ist stets zu prüfen, ob die dafür verwendeten Nutzungsdaten Personenbezug haben müssen und ob sich der Zweck nicht auch mit anonymen oder zumindest pseudonymisierten Daten erreichen lässt.

Abs. 2 enthält auch eine Beschränkung. Ist die Voraussetzung des § 2 Nr. 1 nicht gegeben, die Zusammenführung der Nutzungsdaten aus verschiedenen E-Learning-Verfahren also nicht zu Zwecken der wissenschaftlichen Ausbildung erforderlich, so hat sie zu unterbleiben. Sie kann nicht auf andere Ermächtigungen zur Datenverarbeitung gestützt werden.

Werden Nutzungsdaten nicht mehr benötigt, sind sie zu löschen oder zu anonymisieren. Im Regelfall dürfte dies für Nutzungsdaten unmittelbar nach Abschluss des Nutzungsvorgangs der Fall sein. Siehe zur Speicherung und Löschung auch § 12 Abs. 2.

Erläuterung zu § 7:

Die Vorschrift regelt die Verwendung der Inhaltsdaten eines E-Learning-Verfahrens. Erst durch die Erstellung von Inhalten werden interaktives Lehren und Lernen und die abschließende Leistungsbewertung ermöglicht. Solche Inhalte sind beispielsweise Lernmaterialien, Übungsaufgaben, Hausarbeiten oder Beiträge in Foren und Wikis. Diese Daten sind direkt mit dem Lehr- und Lernzweck von E-Learning-Verfahren verbunden. Ihre Nutzung durch die oder den Verantwortlichen oder andere Teilnehmende der Lehrveranstaltung muss daher grundsätzlich möglich sein. Sie müssen im Regelfall mit Personenbezug ausgewertet und verarbeitet werden.

Wenn diese Daten nicht mehr erforderlich sind, um das Lernen der Nutzerinnen und Nutzer zu fördern oder den Leistungsnachweis zu erbringen, müssen sie gelöscht oder anonymisiert werden. Nach § 12 Abs. 3 sind Inhaltsdaten regelmäßig zum Ende des Semesters zu löschen, für Abschlussarbeiten gelten die allgemeinen Regeln zur Aufbewahrung.

Bei manchen Anwendungen wie zum Beispiel Lehrevaluationen oder „Meckerecken“, in denen Studierende ohne Konsequenzen ihre Meinung äußern können sollen, sind Inhaltsdaten von Beginn an nur anonym zu verarbeiten.

Urheberrechtliche Probleme sind vom Anwendungsbereich dieser Satzung ausgenommen. Dies ergibt sich bereits aus der Definition des Anwendungsbereichs in § 1 Abs. 1 Satz 1 und ist hier für Inhaltsdaten noch einmal ausdrücklich festgehalten.

§ 9 enthält spezielle Regelungen für besondere Inhaltsdaten, nämlich die Aufzeichnung oder Übertragung von Lehrveranstaltungen.

Erläuterung zu § 8:

Abs. 1 erlaubt die Verarbeitung aller drei Datenarten, also Bestands-, Nutzungs- und Inhaltsdaten für Zwecke der Forschung. In dieser Hinsicht geht die Satzung über ihren eigentlichen Anwendungsbereich, das E-Learning und damit die Lehre, hinaus. Die Verarbeitung zu Forschungszwecken ist nur zulässig, wenn folgende Bedingungen erfüllt sind. Zuerst muss es sich um ein Forschungsvorhaben handeln. Es muss notwendig sein, dafür die Daten mit Personenbezug zu verarbeiten. Gerade bei Forschungsvorhaben dürfte es häufig möglich sein, die Daten anonym oder mit einem Pseudonym, das auch die Forschenden nicht auflösen können, zu verarbeiten. Abs. 1 ist nur einschlägig, wenn die Verarbeitung der Daten mit Personenbezug für den Forschungszweck erforderlich ist. Dies setzt wiederum voraus, dass der Forschungszweck bereits zu Beginn der Datenverarbeitung konkret

umrissen ist. Spätere Erweiterungen, auch in Form von Konkretisierungen, des Forschungszwecks stellen Akte der Datenverarbeitung dar, deren Rechtmäßigkeit wieder zu überprüfen ist.

Ferner dürfen keine schutzwürdigen Belange der betroffenen Nutzerinnen und Nutzer beeinträchtigt werden. Der Begriff der „schutzwürdigen Belange" ist rechtlich nicht abschließend definiert. Da durch die Datenverarbeitung in das Persönlichkeitsrecht eingegriffen wird, können alle Belange schutzwürdig sein, die die Persönlichkeit der oder des Betroffenen betreffen und nach den Vorgaben des Grundgesetzes schützenswert sind. Es gibt keine Möglichkeit der Abwägung. Vielmehr ist die Datenverarbeitung unzulässig, wenn schutzwürdige Belange der Nutzerinnen und Nutzer auch nur beeinträchtigt werden. Darüber hinaus darf die Datenverarbeitung nur aus den in Abs. 1 genannten Gründen keine Beeinträchtigung schutzwürdiger Belange der Nutzerinnen und Nutzer darstellen. Diese Gründe sind die Art der Daten, ihre Offenkundigkeit oder der Art ihrer Verwendung. Sind die verarbeiteten personenbezogenen Daten offenkundig, also für eine nicht beschränkte Zahl von Personen allgemein zugänglich, dann können durch ihre Verarbeitung keine schutzwürdigen Belange der Nutzerin oder des Nutzers beeinträchtigt werden. Ferner könnte die Art der Verarbeitung gegen die Beeinträchtigung schutzwürdiger Belange der oder des Betroffenen sprechen. Wenn die Daten, die zu Zwecken des E-Learning erhoben wurden, vom selben Verantwortlichen zu Forschungszwecken verwendet werden, ohne dass der Kreis derjenigen, der von den Daten Kenntnis nimmt, dadurch erweitert wird, dann ergeben sich für die Nutzerin oder den Nutzer keine zusätzlichen Risiken durch die Datenverarbeitung. Dass wegen der Art der Daten keine schutzwürdigen Belange der oder des Betroffenen berührt sind, ist abstrakt ohne Bezug auf den konkreten Datenverarbeitungsvorgang nicht abschließend zu beurteilen.

Zur Prüfung der Voraussetzungen des Abs. 1 kann folgende Checkliste genutzt werden:
- Handelt es sich um Forschung?
- Ist der Forschungszweck konkret benannt?
- Müssen die Daten zur Erreichung des Forschungszwecks mit Personenbezug verarbeitet werden? Können die Daten nicht anonymisiert oder unter Pseudonym verarbeitet werden?
- Sind keine schutzwürdigen Belange der Nutzerin oder des Nutzers berührt?
    - Wegen der Art der Daten
    - Wegen ihrer Offenkundigkeit
    - Wegen der Art der Verarbeitung

Wird eine dieser Fragen verneint, so kann eine Verarbeitung personenbezogener Daten zu Zwecken der Forschung nicht auf Abs. 1 gestützt werden.

Abs. 2 führt eine strenge Zweckbindung ein. Satz 1 stellt ausdrücklich klar, dass eine Verarbeitung nur zu Forschungszwecken zulässig ist und die Daten danach nicht weiter verwendet werden dürfen. Satz 2 begrenzt die Möglichkeit der Übermittlung der Daten. Daten, die für Zwecke der Forschung verarbeitet wurden, dürfen nur zu Forschungszwecken und nur aufgrund einer Einwilligung der Nutzerin oder des Nutzers an Forschende in anderen Forschungsinstitutionen weitergegeben werden. Beispielsweise stellt die Weitergabe der in der Universität Marburg zur didaktischen Forschung erhobenen personenbezogenen Daten an ein didaktisches Forschungsprojekt in einer anderen Hochschule eine Übermittlung im datenschutzrechtlichen Sinne dar. Solange die Daten Personenbezug haben, ist dies nur aufgrund einer Einwilligung der Betroffenen zulässig.

Erläuterungen zu § 9:

Eine besondere Form von Inhaltsdaten sind Videoaufnahmen von Lehrveranstaltungen. Sie können im Wesentlichen in drei Formen erhoben und verwendet werden:
(1) Die direkte Übertragung in einen anderen Hörsaal oder an Teilnehmende der Lehrveranstaltung an einem anderen Ort ohne Aufzeichnung (Live-Streaming),

(2) Aufzeichnung und Speicherung für einen späteren Zugriff durch Teilnehmende der Veranstaltung oder
(3) zeitgleiche oder zeitversetzte Übertragung für einen externen Zugriff durch die Öffentlichkeit, zum Beispiel über das Internet.

Bei Videoaufnahmen wird immer die Lehrperson erfasst. Sie muss der Aufnahme zustimmen. Dies betrifft sowohl die Variante (1) als auch (2). Die Teilnehmenden der Lehrveranstaltung zu unterrichten, gehört zu den Dienstpflichten oder zum Lehrauftrag der Lehrenden.

Für die Aufnahme einer Lehrveranstaltung ist es nicht erforderlich, bestimmte Studierende aufzunehmen. Auch wenn dies so weit wie möglich vermieden werden soll, lässt es sich nicht stets vermeiden, dass auch Studierende aufgenommen werden. Studierenden soll die Möglichkeit gegeben werden, das „Rampenlicht" zu meiden. Werden sie doch aufgezeichnet, können die Videodaten innerhalb des Kreises der Teilnehmenden verwendet werden, wenn die Studierenden bei Besuch der Veranstaltung wussten, dass die Veranstaltung aufgezeichnet wird. Studierende sollten daher bereits im Vorlesungsverzeichnis darüber informiert werden, welche Veranstaltungen auf Video aufgezeichnet und zu welchen Zwecken und in welchem Umfang weiterverwendet werden.

Nicht von der Vorschrift erfasst sind Aufnahmen von Lehrveranstaltungen, die für Zwecke der Öffentlichkeitsarbeit oder der Werbung der Öffentlichkeit zur Verfügung gestellt werden (Variante 3). Zur Öffentlichkeit gehören auch die Mitglieder der Hochschule, die nicht an der Lehrveranstaltung teilnehmen. In diesem Fall ist nach §§ 22 Kunsturhebergesetz eine – formlose – Zustimmung der Aufgenommenen erforderlich.

Erläuterungen zu § 10:

Wenn Lehrveranstaltungen durch E-Learning unterstützt werden, liegt es nahe, auch den Leistungsnachweis in dieser Form zu erbringen und automatisiert zu korrigieren, um Zeit und Kosten zu sparen.

Nach § 7 Abs. 3 HDSG ist jedoch eine Entscheidung, „die zu rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen führt", unzulässig „wenn sie auf einer Bewertung einzelner Merkmale seiner Person beruht, die ausschließlich durch eine automatisierte Verarbeitung seiner Daten erstellt wurde." Solange aber eine Nachkorrektur stattfindet, liegt kein Verstoß gegen das datenschutzrechtliche Verbot der automatisierten Einzelentscheidung vor. Daher fordert Satz 1, dass der Leistungsnachweis auf Antrag der oder des betroffenen Studierenden von einem Korrektor oder einer Korrektorin überprüft werden muss.

Probleme können jedoch entstehen, wenn Studierende monieren, dass der bewertete Leistungsnachweis inhaltlich nicht mit dem abgegebenen Leistungsnachweis übereinstimmt. Satz 2 fordert daher als ein geeignetes Mittel zum Nachweis der Unverfälschtheit, dass die „abgegebenen" Leistungsnachweise unmittelbar nach „Abgabe" mit einem elektronischen Zeitstempel versehen werden. Bei Zeitstempeln werden die Daten oder deren elektronische „Kurzfassung" (Hashwert) mit einer sicheren Zeitangabe verknüpft und zusammen elektronisch signiert. Wird der Zeitstempel unmittelbar, also mit einer minimalen Zeitdifferenz, nach „Abgabe" von der oder dem Verantwortlichen automatisch erzeugt, ist dadurch auch gesichert, dass der Leistungsnachweis nicht zwischen Abgabe und Zeitstempelung manipuliert wurde, weil hierfür keine Zeit war.

Erläuterung zu §11:

Die übliche Verarbeitung personenbezogener Daten in E-Learning-Verfahren wird durch die §§ 5 bis 9 erlaubt. Ist dies ausnahmsweise nicht der Fall, kann die Verarbeitung personenbezogener Daten nur durch eine Einwilligung der Betroffenen gerechtfertigt werden.

Die Einwilligung ist der stärkste Ausdruck des Rechts auf informationelle Selbstbestimmung, da sie es der oder dem Betroffenen überlässt, selbst über Art, Umfang, Zweck und Dauer des Umgangs mit seinen Daten zu entscheiden. Dies ist jedoch nur möglich, wenn die Nutzerin oder der Nutzer weiß, worin sie oder er einwilligt, also was mit ihren oder seinen Daten geschehen wird, und wenn sie oder er die Entscheidung über die Einwilligung frei von äußeren Zwängen treffen kann. Daher darf eine Nutzerin oder ein Nutzer nicht gezwungen sein, eine Einwilligung zu erteilen, um eine Veranstaltung zu besuchen, die sie oder er besuchen muss. Dagegen ist grundsätzlich 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 von einer Freiwilligkeit der Einwilligung ausgegangen werden kann.

Abs. 1 Satz 2 garantiert, dass es sich um eine so genannte „informierte Einwilligung" handelt, die oder der Betroffene also genau weiß, was sie oder er tut. Dazu gehört auch, dass sie oder er um die Folgen der Verweigerung der Einwilligung weiß.

Die Einwilligung muss nach Abs. 1 Satz 3 schriftlich, also von der oder dem Erklärenden handschriftlich unterschrieben oder mit einer qualifizierten Signatur versehen abgegeben werden. Wird die Einwilligung mit anderen Erklärungen zusammen abgegeben, so ist sie nach Satz 4 besonders hervorzuheben. Sie darf nicht im Kleingedruckten versteckt werden.

Alternativ kann die Einwilligung nach Abs. 2 Satz 1 immer auch elektronisch erklärt werden, wenn die oder der Verantwortliche sicherstellt, dass die Nutzerin oder der Nutzer ihre bzw. seine Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, die Nutzerin oder der Nutzer den Inhalt der Einwilligung jederzeit abrufen kann und sie jederzeit mit Wirkung auf die Zukunft widerrufen kann. Sind die Voraussetzungen nicht gegeben, handelt es sich nicht um eine wirksame Einwilligung und eine darauf gestützte Datenverarbeitung ist unzulässig. Wird die Einwilligung zu einem späteren Zeitpunkt widerrufen, so wird hierdurch die Datenverarbeitung, die vorgenommen wurde, als die Einwilligung noch galt, nicht rückwirkend unzulässig.

Wenn wegen besonderer Umstände, etwa Eilbedürftigkeit oder eines besonderen Interesses der Nutzerin oder des Nutzers, die oder der zur Abgabe einer formgerechten Einwilligung nicht in der Lage ist, eine andere Form angemessen ist, kann die Einwilligung nach Abs. 1 Satz 3 ausnahmsweise auch formlos erklärt werden.

Zur einfacheren Handhabung des Einwilligungsmanagements ist zu empfehlen, Einwilligungserklärungen – soweit erforderlich – jeweils nur zu Semesterbeginn zu ändern und ihre Geltung möglichst auf das jeweilige Semester zu begrenzen, so dass für alle Einwilligenden pro Semester und E-Learning-Verfahren immer nur ein identischer Einwilligungstext zum Abruf bereit gehalten werden muss.

Abs. 2 Satz 4 enthält ein so genanntes Kopplungsverbot. Dieses verhindert, dass die Teilnahme an einer Lehrveranstaltung von der Einwilligung der Nutzerin oder des Nutzers in eine Verwendung seiner Daten für andere Zwecke als die Nutzung im Rahmen des E-Learning-Verfahrens abhängig gemacht werden darf. Dadurch soll die Freiwilligkeit der Einwilligung gewahrt werden.

Erläuterung zu §12:

Speicherfristen orientieren sich daran, ob die personenbezogenen Daten weiterhin für die Erreichung des Zwecks erforderlich sind. Grundsätzlich ist daher eine einzelfallbezogene Prüfung erforderlich, die auf den konkreten Zweck der Datenverarbeitung abstellt. Aufgrund des erheblichen Umfangs, in dem Daten für das E-Learning an einer Hochschule verarbeitet werden, wäre der Aufwand für konkrete

Prüfungen jedes Einzelfalles zu groß. Aus diesem Grund sieht die Satzung verallgemeinerte Speicherfristen für die verschiedenen Datenarten vor.

Bestandsdaten von Studierenden sind grundsätzlich bis zur Exmatrikulation zu speichern, weil Studierende bis zu diesem Zeitpunkt an E-Learning-Verfahren teilnehmen können. Will eine Studierende oder ein Studierender prinzipiell nicht an E-Learning-Verfahren teilnehmen, so kann sie oder er beantragen, dass ihre bzw. seine Bestandsdaten bereits früher gelöscht werden. Die Löschung bezieht sich nur auf Bestandsdaten, die zu Zwecken des E-Learning gespeichert wurden. Für die Immatrikulation und andere Aufgaben der Hochschule richtet sich die Befugnis zur Datenspeicherung nach den hierfür einschlägigen Regelungen. Entscheidet sich die oder der Studierende nachträglich dafür, doch an E-Learning-Verfahren teilzunehmen, so sind seine Bestandsdaten wieder zu speichern.

Für Nutzungsdaten ist in Abs. 2 festgelegt, dass diese grundsätzlich unverzüglich nach Beendigung des Nutzungsvorgangs zu löschen sind. „Unverzüglich" bedeutet nicht immer „sofort", sondern vielmehr, dass nicht schuldhaft gezögert werden darf, sie zu löschen, wenn keine Gründe für die weitere Aufbewahrung ersichtlich sind. Dass Nutzungsdaten unverzüglich zu löschen sind, ergibt sich bereits aus der Zweckbindung der Daten und dem Erforderlichkeitsprinzip, dass Daten nur gespeichert werden dürfen, wenn ihre weitere Verarbeitung erforderlich ist. Diese Forderung wird hier aus Klarstellungsgründen noch einmal wiederholt.

Inhaltsdaten sind nach Abs. 3 grundsätzlich zum Ende des Semesters zu löschen, in dem sie erhoben wurden. Diese Regelung geht davon aus, dass Veranstaltungen grundsätzlich zu Semesterende beendet sind und im folgenden Semester kein Bedürfnis mehr nach den Inhaltsdaten des vorigen Semesters besteht. Soweit die Inhaltsdaten ausnahmsweise auch im folgenden Semester für die Lehrveranstaltung benötigt werden, können sie solange weiter gespeichert bleiben. Etwas anderes gilt für Inhaltsdaten, die gleichzeitig auch elektronische Abschlussarbeiten darstellen. Sie sind ebenso wie sonstige Prüfungsakten aufzubewahren.

Erläuterung zu § 13:

Die Vorschrift regelt die Anforderungen an die Datensicherheit. Sie ist im vertretbaren Umfang technikneutral gefasst, um nicht immer wieder der technischen Entwicklung angepasst werden zu müssen. Sie enthält in Abs. 1 eine Generalklausel und in Abs. 2 Konkretisierungen für die wichtigsten Datensicherungsmaßnahmen.

Abs. 1 Satz 1 enthält die allgemeine Vorgabe, dass Daten angemessen gegen Missbrauch durch erforderliche technische und organisatorische Maßnahmen zu schützen sind. Satz 2 definiert den Begriff der „Erforderlichkeit", indem er auf den Schutzzweck abstellt. Technische und organisatorische Maßnahmen können nie absoluten Schutz bieten. Ob Schutzmaßnahmen zu überwinden sind, ist immer eine Frage des Aufwands, den der Angreifer zu betreiben bereit ist. Um an den Schutz der Daten keine übertriebenen Forderungen zu stellen, wird der Aufwand durch den Schutzzweck auch begrenzt. Wie hoch der technisch-organisatorische Aufwand ist, den Betroffene zum Schutz ihrer Daten verlangen können, hängt davon ab, wie schutzbedürftig die Daten sind, also wie groß der Schaden ist, der angerichtet werden kann, wenn die Daten missbraucht werden. Satz 2 enthält auch noch eine weitere Einschränkung: Schutzmaßnahmen sind überhaupt nur dann zu treffen, wenn sie nach dem Zweck des konkreten E-Learning-Verfahrens geboten sind.

Abs. 2 beschreibt vier typische Schutzmaßnahmen. Ob und in welcher Form sie notwendig sind, ergibt sich aus dem nach § 4 Abs. 1 zu erstellenden Datenschutzkonzept des jeweiligen E-Learning-Verfahrens.

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 Administratorin/Administrator, Verantwortliche/Verantwortlicher, Nutzerin/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.

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. Dies kann erreicht werden durch eine Festlegung der Kontrolle der Zugriffsbefugnisse (nach Daten, Programmen und Art des Zugriffs), Protokollierung von Zugriffen, Funktionsbegrenzung und Verschlüsselung der Daten.

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. Eingaben, Änderungen, Löschungen und Weitergaben sind dann in besonderen Protokolldateien zu speichern. In die Protokolldateien sind auch gescheiterte Zugriffsversuche aufzunehmen. Müssen Protokolldateien ausgewertet werden, muss dies nach dem Vier-Augen-Prinzip durch eine andere Person als die Systemadministratorin oder den Systemadministrator geschehen. 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 vor dem absichtlichen, widerrechtlichen Löschen von Daten. Eine zufällige Zerstörung kann zum Beispiel durch Wasserschäden, Brände oder Stromausfälle eintreten. Die Verfügbarkeit kann zum Beispiel durch Ausarbeitung eines Datensicherungskonzepts, regelmäßige Backups, Dokumentation von Sicherungsläufen und Testen der Restore-Funktion gewährleistet werden.

Erläuterung zu § 14:

Die Geltung der Satzung ist vorerst auf fünf Jahre begrenzt. Bereits nach dem Ablauf von vier Jahren ist ein Erfahrungsbericht über die Umsetzung der Satzung zu erstellen. Wenn dem Erfahrungsbericht zu entnehmen ist, dass Handlungsbedarf besteht, soll der Erfahrungsbericht auch Vorschläge enthalten, wie die Satzung überarbeitet, insbesondere konkretisiert, werden sollte.