UniReport

Goethe-Universität | Frankfurt am Main Satzungen und Ordnungen

Satzung zum Schutz personenbezogener Daten in E-Learning-Verfahren an der Johann Wolfgang Goethe-Universität Frankfurt am Main

Genehmigt durch Beschluss des Präsidiums der Johann Wolfgang Goethe-Universität Frankfurt am Main am 6. Dezember 2016

Präambel

An der Goethe-Universität werden zentrale und dezentrale E-Learning-Verfahren, digitale Lehr-, Lern- und Prüfungsverfahren, betrieben. E-Learning-Verfahren fördern und unterstützen das selbstständige Lernen der Studierenden. Außerdem bietet E-Learning Studierenden neue Möglichkeiten, sich im Umgang mit Informations- und Kommunikationstechnologien zu üben und den Erwerb von Studienleistungen zu belegen. Durch E-Learning-Verfahren entstehen auch Risiken für die informationelle Selbstbestimmung der betroffenen Studierenden und der Lehrenden. Diese Satzung vereinheitlicht die Bedingungen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten, unter denen E-Learning-Verfahren angeboten werden. Ziel ist es, die datenschutzrechtlichen Voraussetzungen zu schaffen, 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.

§ 1 Geltungsbereich und Zweck

(1) Diese Satzung gilt für das Erheben, die Verarbeitung und Nutzung personenbezogener Daten der Nutzer und Nutzerinnen von E-Learning-Verfahren, die an der Goethe-Universität betrieben werden.

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

(3) E-Learning-Verfahren sind netzangebundene Lern-, Lehr- und Prüfungsverfahren, 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 Teilnahmevoraussetzungen und Nutzerkreis

(1) Zur Teilnahme an E-Learning-Verfahren sind Nutzer und Nutzerinnen berechtigt, wenn

a.) sie Mitglieder und Angehörige der Goethe-Universität sind und sie einen HRZ-Account antragsweise erhalten haben, oder
b.) sie Nichtmitglieder der Goethe-Universität sind, jedoch ein berechtigtes Interesses gemäß § 3 Ziff. 3 auf Antrag eines / einer Lehrberechtigten der Goethe-Universität nachgewiesen haben.

(2) Voraussetzung ist, dass Nutzer und Nutzerinnen gemäß Abs.1 die Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikations-Infrastruktur der Johann Wolfgang Goethe-Universität vom 11. September 2008 (Allgemeine IuK-Nutzungsordnung)[1] in ihrer jeweils geltenden Fassung sowie diese Satzung schriftlich anerkennen.

[1] Veröffentlicht im UniReport Satzungen und Ordnungen vom 23. September 2008.

(3) Der Antrag zur Teilnahme an E-Learning-Verfahren ist beim Hochschulrechenzentrum zu stellen. Bei minderjährigen Nutzern und Nutzerinnen ist neben den Voraussetzungen gemäß Absatz 1 zusätzlich für die Teilnahme an E-Learning-Verfahren die schriftliche Einwilligung des / der Erziehungsberechtigten vorzulegen.

§ 3 Begriffsbestimmungen

Im Sinne dieser Satzung sind:

(1) Personenbezogene Daten: Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Diese sind im Einzelnen:

a.) Betriebsdaten: Grunddaten eines Verhältnisses zwischen Anbieter / Anbieterin und Nutzer / Nutzerin,
b.) Nutzungsdaten: Aufgrund der bloßen Nutzung von E-Learning-Verfahren anfallende Daten,
c.) Inhaltsdaten: Kommunikationsinhalte der Nutzer und Nutzerinnen,(z. B. Prüfungsergebnisse, Korrekturen).

(2) Datenverarbeitung: Jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten im Sinne von § 2 Abs. 2 Hessisches Datenschutzgesetz (HDSG).

(3) E-Learning-Verfahren: Digitale Lern-, Lehr-und Prüfungsverfahren, die personenbezogene Daten zum Zwecke der Aus-, Fort- und Weiterbildung verarbeiten und darauf zielen, das Lernen und die Kenntnisse der Nutzerinnen und Nutzer zu fördern sowie Daten und Informationen für die Erbringung von Leistungsnachweisen zu verarbeiten.

(4) Verantwortliche: Personen, die im Rahmen von E-Learning-Anwendungen Zugriff auf personenbezogene Daten haben. Dies sind:

a.) Betriebsverantwortliche: Personen, die von der Stelle / Einrichtung, durch die das E-Learning-Verfahren betrieben und administriert wird, als solche benannt wurden (z. B. Systembetreiber; Systemadministratoren für Backend und Front End)
b.) Lehrverantwortliche: Lehrberechtigte und deren Mitarbeitende, die Inhalte auf E-Learning-Systemen Anwendungen bereitstellen.

§ 4 Grundsätze

(1) Der / Die Verantwortliche darf beim Einsatz von E-Learning-Verfahren personenbezogene Daten der Nutzer und Nutzerinnen verarbeiten, soweit diese Satzung oder eine andere Rechtsvorschrift dies ausdrücklich erlaubt. Personenbezogene Daten dieser Personen dürfen nur dann der Öffentlichkeit, den Mitgliedern der Hochschule, den Teilnehmern / Teilnehmerinnen einer Lehrveranstaltung oder dem / der Verantwortlichen für das E-Learning-Verfahren zugänglich gemacht werden, wenn dies für die Zweckerreichung des konkreten E-Learning-Verfahrens erforderlich ist.

(2) Der / Die Verantwortliche darf personenbezogene Daten der Nutzer und Nutzerinnen für andere als die in Absatz 1 genannten Zwecke nur verwenden, soweit der Nutzer / die Nutzerin schriftlich hierzu eingewilligt hat. Die Verarbeitung von Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben ist nur auf Grundlage einer ausdrücklichen schriftlichen Einwilligung der betroffenen Nutzer und Nutzerinnen zulässig (§ 7 Abs. 4 HDSG). Willigt der Nutzer oder die Nutzerin nicht ein, darf ihm / ihr daraus kein Nachteil entstehen.

§ 5 Pflichten des / der Verantwortlichen

(1) Der / Die Betriebsverantwortliche hat vor Beginn für jedes E-Learning-Verfahren eine Vorabkontrolle dem / der Datenschutzbeauftragten der Goethe-Universität zur Prüfung vorzulegen. In der Vorabkontrolle sind Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie insbesondere die technische Sicherung im Umgang mit personenbezogenen Daten zu beschreiben. Nach dem zustimmenden Prüfergebnis der Vorabkontrolle durch den Datenschutzbeauftragten / die Datenschutzbeauftragte hat der / die Betriebsverantwortliche ein Verfahrensverzeichnis gemäß § 6 HDSG anzulegen und dem / der Datenschutzbeauftragten ausgefüllt zu übermitteln.

(2) Der / Die Betriebsverantwortliche hat die Nutzung des E-Learning-Verfahrens anonym oder unter einem Pseudonym zu ermöglichen, soweit dies den in § 1 Abs. 3 genannten Zwecken nicht widerspricht und technisch möglich und zumutbar ist.

(3) Der / Die Betriebsverantwortliche hat für das E-Learning-Verfahren spezifische Nutzungsregelungen festzulegen, aus denen die Rechte und Pflichten der Nutzerinnen und Nutzer hinsichtlich des Umganges mit diesem Verfahren hervorgehen. Vor Nutzung des E-Learning-Verfahrens haben die Nutzer und Nutzerinnen den Nutzungsregelungen zuzustimmen ist (s. Anlage).

§ 6 Betriebsdaten

(1) Der / Die Verantwortliche darf personenbezogene Daten der Nutzer und Nutzerinnen wie insbesondere 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 Goethe-Universität Frankfurt erforderlich sind.

(2) Die Authentifizierung zur Nutzung von digitalen Lehr- und Lern-Verfahren soll über den HRZ-Account erfolgen. Im Fall von digitalen Prüfungsverfahren kann auf schriftlichen begründeten Antrag eine getrennte Authentifizierung erfolgen.

§ 7 Nutzungsdaten

(1) Nutzungsdaten können für eine allgemeine Kontrolle der Akzeptanz und Auswertung des Nutzungsverhaltens nur anonymisiert genutzt werden.

(2) Der / Die Verantwortliche darf personenbezogene Daten eines Nutzers oder einer Nutzerin wie insbesondere Merkmale zur Identifikation des Nutzers oder der Nutzerin, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung oder Angaben über die einzelnen von Nutzer oder Nutzerin benutzten E-Learning-Verfahren nur verarbeiten, soweit dies für die in § 1 Abs. 3 genannten Zwecke erforderlich ist.

(3) Wenn Nutzungsdaten zum Zweck der Optimierung des individuellen Lernweges erhoben werden, darf nur der Nutzer oder die Nutzerin in diese Daten Einsicht nehmen und ist vor der Erhebung darauf hinzuweisen.

§ 8 Inhaltsdaten

Der / Die Verantwortliche darf die vom Nutzer oder der Nutzerin eingegebenen Inhaltsdaten verarbeiten, soweit dies für die in § 1 Ziff. 3 genannten Zwecke erforderlich ist; andere Rechtsvorschriften bleiben unberührt.

§ 9 Datenverarbeitung für wissenschaftliche Forschungszwecke

(1) Zum Zwecke wissenschaftlicher Forschung dürfen datenverarbeitende Stellen personenbezogene Daten ohne Einwilligung des / der Betroffenen im Rahmen bestimmter Forschungsvorhaben verarbeiten, soweit dessen schutzwürdige Belange wegen der Art der Daten, ihrer Offenkundigkeit oder der Art ihrer Verwendung nicht beeinträchtigt werden. Der Einwilligung des / der Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des / der Betroffenen überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Im Falle des Satz 2 bedarf die Verarbeitung durch Stellen des Landes der vorherigen Genehmigung der obersten Landesbehörde oder einer von dieser bestimmten Stelle. Die Genehmigung muss den Empfänger / die Empfängerin, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Hessischen Datenschutzbeauftragten mitzuteilen.

(2) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungszweck dies zulässt.

(3) Eine Verarbeitung der nach Abs. 1 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Abs. 1 S. 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiterübermittelt werden.

(4) § 33 HDSG bleibt hiervon unberührt.

§ 10 Aufzeichnung und Übertragung von Lehrveranstaltungen

(1) Die Aufzeichnung und die zeitgleiche oder zeitversetzte Übertragung einer Lehrveranstaltung ist zulässig, wenn dies durch den Ausbildungsauftrag der Hochschule geboten ist sowie technisch, organisatorisch und rechtlich 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. Die zeitgleiche oder zeitversetzte Übertragung in E-Learning-Verfahren bedarf der schriftlichen Einwilligung der von der Aufzeichnung und Übertragung betroffenen Personen. Willigt der / die Betroffene nicht ein, darf ihm / ihr daraus kein Nachteil entstehen.

(2) Die Aufzeichnung für die zeitgleiche oder zeitversetze Übertragung für den externen Zugriff durch die Öffentlichkeit (z. B. Internet) ist nur zulässig, wenn die Teilnehmer und Teilnehmerinnen vor der Aufzeichnung über diese informiert

worden sind und sie einschließlich einzelner Wortbeiträge, nicht individualisierbar aufgenommen werden. Ist es nach dem Zweck der Aufzeichnung und der Übertragung (z. B. Öffentlichkeitsarbeit, Werbung) geboten, dass auch (einzelne) Teilnehmer / Teilnehmerinnen erkennbar sind, ist die vorherige Einholung ihrer schriftlichen Einwilligung zur Aufnahme und Übertragung erforderlich. Das Recht am eigenen Bild und die Vorschriften des Kunsturhebergesetzes bleiben unberührt.

(3) Bei Aufzeichnungen, in denen ausschließlich die Lehrkräfte erkennbar sind, obliegt diesen die Entscheidung, welcher Personenkreis Zugriff auf die Aufzeichnung haben soll.

§ 11 Anforderungen an automatisierte Bewertungen

Jede automatisiert erstellte Bewertung eines Leistungsnachweises muss auf Antrag des / der betroffenen Studierenden von einem Korrektor oder einer Korrektorin überprüft werden. Elektronische Bewertungen sind unmittelbar nach Abgabe mit einem elektronisch signierten Zeitstempel zu versehen. Die eindeutige Identifizierbarkeit der elektronischen Daten muss gewährleistet werden.

§ 12 Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Nutzers / der Nutzerin beruht. Er / Sie ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung 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 / die Verantwortliche sicherstellt, dass der Nutzer / die Nutzerin seine / ihre Einwilligung bewusst und eindeutig erteilt hat, die Einwilligung protokolliert wird, der Nutzer / die Nutzerin den Inhalt der Einwilligung jederzeit abrufen und sie jederzeit mit Wirkung für die Zukunft widerrufen kann.

(3) Hat der Nutzer / die Nutzerin seine / ihre Einwilligung widerrufen, so sind seine / ihre 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 / die Nutzerin vor der Löschung oder Anonymisierung hierauf hinzuweisen. Die Teilnahme an einer Lehrveranstaltung darf nicht von der Einwilligung des Nutzers / der Nutzerin in eine Verwendung seiner / ihrer Daten für andere Zwecke abhängig gemacht werden.

§ 13 Speicherfristen

(1) Die Nutzungsdaten gemäß § 7 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.

(2) Die Inhaltsdaten gemäß § 8 sind bis spätestens ein Semester nach Ende der Lehrveranstaltung vom Produktivsystem zu entfernen. Es kann eine zweijährige Speicherung in einem Archiv auf Antrag angeschlossen werden. Spätestens nach Ablauf dieses Zeitraumes sind die Inhaltsdaten zu löschen. Die Speicherfrist von elektronischen Prüfungsleistungen wird insbesondere nach gesetzlichen Aufbewahrungsregelungen (Verordnung über das Verfahren der Immatrikulation, Rückmeldung, Beurlaubung und Exmatrikulation, das Studium als Gasthörerin oder Gasthörer, das Teilzeitstudium und die Verarbeitung personenbezogener Daten der Studierenden an den Hochschulen des Landes Hessen (Hessische Immatrikulationsverordnung)) für prüfungsrelevante Daten bestimmt.

(3) Bestehen diese Inhaltsdaten aus einer Veranstaltungsaufzeichnung, in der nur die Lehrkräfte erkennbar sind, obliegt diesen die Entscheidung, zu welchem Zeitpunkt diese Aufzeichnung vom System entfernt wird.

(4) Die Goethe-Universität kann im Falle eines Ausscheidens aus einem Dienst- bzw. Rechtsverhältnis der Lehrkräfte, über die Herausnahme der Aufzeichnung aus dem System entscheiden.

(5) Die Betriebsdaten von Mitgliedern der Goethe-Universität (HRZ-Accounts) sind nach der Exmatrikulation oder dem Ausscheiden aus dem Dienst, aus dem System zu entfernen.

(6) Die Betriebsdaten von Nichtmitgliedern der Goethe-Universität sind nach Ablauf ihrer Berechtigung zur Nutzung der E-Learning-Verfahren zu löschen.

§ 14 Datensicherheit

(1) Der / Die Betriebsverantwortliche 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) Für das E-Learning-Verfahren sind Maßnahmen zu treffen, die geeignet sind, dass

a.) die Zweckbindung erhobener Daten gewahrt wird,
b.) ausschließlich die Berechtigten nur auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und personenbezogene Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können,
c.) 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,
d.) personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

§ 15 In-Kraft-Treten

Die Satzung tritt nach Genehmigung durch das Präsidium am Tag nach ihrer Veröffentlichung im UniReport in Kraft. E-Learning-Verfahren, die bereits vor Inkrafttreten dieser Satzung an der Goethe-Universität betrieben werden, sind bis Ende 2017 an die satzungsrechtlichen Vorgaben anzupassen.

Frankfurt am Main, den 16. März 2017

Prof. Dr. Birgitta Wolff

Präsidentin

Impressum
UniReport Satzungen und Ordnungen erscheint unregelmäßig und anlassbezogen als Sonderausgabe des UniReport. Die Auflage wird für jede Ausgabe separat festgesetzt.

Herausgeber Der Präsident der Johann Wolfgang Goethe-Universität Frankfurt am Main

Anlage zur Satzung zum Schutz personenbezogener Daten in E-Learning-Verfahren an der Johann Wolfgang Goethe-Universität Frankfurt am Main vom 29. März 2017

Nutzungsbedingungen für das E-Learning-Verfahren

gemäß § 5 Abs. 3 der Satzung zum Schutz personenbezogener Daten in E-Learning-Verfahren an der Goethe-Universität

Name des / der Verantwortlichen: ……

Institut / Fachbereich: ……

Bezeichnung des E-Learning-Systems: ……

……

Nutzungsbedingungen über die Rechte und Pflichten der Nutzer / Nutzerinnen:

Die Nutzer / Nutzerinnen wurden vor der Nutzung über die Nutzungsbedingungen informiert und haben diesen vor der Nutzung schriftlich zugestimmt.

Ort, Datum

……

……
Verantwortlicher / Verantwortliche

Ort, Datum

……

……
Dekan / Dekanin

Fachbereich: ……

Erläuterungen zur Satzung zum Schutz personenbezogener Daten in E-Learning-Verfahren an der Goethe-Universität

Erläuterungen zu § 1 Geltungsbereich und Zweck

Abs. 1: Die Begriffe „Erheben", „Verarbeiten" und „Nutzung" entsprechen der Regelung des § 2 Abs. 2 Hessisches Datenschutzgesetzes (HDSG) und umfassen allgemein alle Phasen vom Erheben der Daten bis zum Nutzen (z. B. Speicherung, Übermittlung). Der Begriff der „personenbezogenen Daten" stammt aus dem allgemeinen Datenschutzrecht. Daten sind dann personenbezogenen, wenn sie sich einer natürlichen Person zuordnen lassen. Sind die Daten anonymisiert, fehlt der Personenbezug.

Sofern die Goethe-Universität Zugriff auf die Daten hat (die Daten sind an der Goethe-Universität abgelegt und / oder die Software läuft an der Goethe-Universität), gilt diese Satzung.

Abs. 2 bestimmt den Anwendungsbereich in verteilten Systemen. Er gilt für Datenverarbeitungsvorgänge, die sowohl dem E-Learning als auch einer weiteren Anwendung zuzuordnen sind, wenn also mehrere Zwecke untrennbar in einem einheitlichen Datenverarbeitungsvorgang zusammenkommen, wenn also beispielsweise ein Beitrag zu einem Wiki der Errichtung einer allgemeinen Wissensbasis dient, andererseits aber auch den Charakter einer individuellen Hausaufgabe in einem Kurs hat. Für Vorgänge, die (auch wenn nur unter anderem) dem E-Learning dienen, gelten die Regeln der Satzung zum Datenschutz im E-Learning-Verfahren.

Erläuterungen zu § 2 Teilnahmevoraussetzungen und Nutzerkreis

Abs. 1: Nutzerinnen und Nutzer, die an E-Learning-Verfahren teilnehmen, müssen die IuK-Nutzungsordnung der Goethe-Universität anerkennen. Für Universitätsmitglieder erfolgt die entsprechende Vereinbarung schon bei der Zuweisung des HRZ-Accounts, für Externe ohne HRZ-Account ist eine separate Anerkennung erforderlich.

Das berechtigte Interesse beurteilt der / die Lehrberechtigte, der / die den entsprechenden Antrag für den / die Externe stellt (z. B. für Schülerstudierende).

Abs. 2: Um die IUK-Nutzungsordnung wirksam anerkennen zu können, ist Volljährigkeit erforderlich, daher sind die Erziehungsberechtigten verantwortlich für die Nutzung von E-Learning.

Erläuterungen zu § 3 Begriffsbestimmungen

Abs. 1: Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffene / Betroffener).

Beispiele für Betriebsdaten sind: Name, Matrikelnummer, Studienfach, E-Mail-Adresse.
Beispiele für Nutzungsdaten sind: Beginn und Umfang der Nutzung, Zugriff auf bestimmte Inhalte, Verbindungsdaten.
Beispiele für Inhaltsdaten sind: Chat- und Forenbeiträge, hochgeladene Dateien, Hausaufgaben, Wiki-Einträge, Prüfungsergebnisse, Korrekturen.

Der Umgang mit den einzelnen Datenarten wird in den §§ 6 – 8 und in § 13 Speicherfristen näher ausgeführt.

Abs. 2: Datenverarbeitung ist jede Verwendung gespeicherter oder zur Speicherung vorgesehener personenbezogener Daten. Im Sinne der nachfolgenden Vorschriften ist dies:

(1) Erheben: Das Beschaffen von Daten über den Betroffenen / die Betroffene.
(2) Speichern: Das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung.

(3) 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.
(4) Sperren: Das Verhindern weiterer Verarbeitung gespeicherter Daten.
(5) Löschen: Das Unkenntlichmachen gespeicherter Daten ungeachtet der dabei angewendeten Verfahren.

Abs. 3: Alle Verfahren, mit denen die Lehre digital unterstützt bzw. durchgeführt wird und bei denen personenbezogene Daten verarbeitet werden, fallen unter diese Bestimmung.

Eine anonyme digitale Umfrage zur Lehre, aus der nicht ersichtlich wird, wer daran teilgenommen hat, fällt nicht unter diese Satzung, da der Personenbezug im rechtlichen Sinne fehlt. Entscheidend ist, dass an keiner Stelle die Tatsache der Teilnahme oder die Antworten einer individuellen Person zugeordnet werden können.

Abs. 4: Lehrverantwortliche haben eine Zwitterposition in dieser Satzung: Zum einen haben sie zumindest begrenzt Zugang zu den Personendaten der Teilnehmenden ihrer Veranstaltung, zum anderen sind sie selbst Nutzer der Systeme und ihre eigenen Daten sind schutzwürdig. Bestimmte technische Erfordernisse gehen über die Möglichkeiten der Lehrverantwortlichen hinaus, daher werden an dieser Stelle auch die Betriebsverantwortlichen eingeführt, die unter anderem für die Datensicherung (§ 14) verantwortlich sind.

Erläuterungen zu § 4 Grundsätze

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.

In Abs. 2 ist die Verarbeitung von besonderen schutzwürdigen Daten geregelt. Hierfür gilt § 7 Abs. 4 HDSG:

„(4) Soweit nicht eine Rechtsvorschrift die Verarbeitung personenbezogener Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben vorsieht oder zwingend voraussetzt, darf eine Verarbeitung nur nach §§ 33-35 und § 39 (Datenverarbeitung für wissenschaftliche Zwecke; Datenschutz bei Dienst- und Arbeitsverhältnissen, Übermittlung an öffentlich-rechtliche Religionsgesellschaften, Verarbeitung personenbezogener Daten durch den Landtag und der kommunalen Vertretungsorgane) erfolgen. Im Übrigen ist eine Verarbeitung aufgrund dieses Gesetzes nur zulässig, wenn sie ausschließlich im Interesse des Betroffenen / der Betroffenen liegt und der Hessische Datenschutzbeauftragte vorab gehört worden ist."

Die anderweitige Verwendung laut Abs. 2 kann online durch einen OK-Knopf erlaubt werden; das Erteilen der Erlaubnis muss jedoch optional bleiben und die Teilnahme am E-Learning-Verfahren darf nicht davon abhängen.

Erläuterungen zu § 5 Pflichten des / der Verantwortlichen

Abs. 1 regelt zwei Pflichten des / der Betriebsverantwortlichen. Der / Die Betriebsverantwortliche hat eine Vorabkontrolle gemäß § 7 Abs. 6 HDSG vor jeder automatisierten Datenverarbeitung von personenbezogenen Daten durchzuführen.

§ 7 Abs. 6 HDSG regelt:

„(6) Wer für den Einsatz oder die wesentliche Änderung eines Verfahrens zur automatisierten Datenverarbeitung zuständig ist, hat vor dem Beginn der Verarbeitung zu untersuchen, ob damit Gefahren für die in § 1 Abs. 1 Nr. 1 geschützten Rechte verbunden sind; dies gilt in besonderem Maße für die in § 7 Abs. 4 genannten Daten. Das Verfahren darf nur eingesetzt werden, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische und organisatorische Maßnahmen verhindert werden können. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zur Prüfung zuzuleiten."

Eine Checkliste für die Durchführung der Vorabkontrolle kann bei der zuständigen Datenschutzbeauftragten unter dsb@uni-frankfurt.de angefordert werden.

Nach der Vorabkontrolle ist ein Verfahrensverzeichnis gemäß § 6 HDSG anzulegen, das an den Datenschutzbeauftragten / die Datenschutzbeauftragte zu übermitteln und dort zu hinterlegen ist. Das Formular des Verfahrensverzeichnisses sowie eine Checkliste für die Vorabkontrolle kann bei der Datenschutzbeauftragten über dsb@uni-frankfurt.de angefordert werden.

Abs. 2 weist die Betriebsverantwortlichen an, sofern technisch machbar, die anonyme Nutzung der Verfahren ermöglichen.

Abs. 3: Aus der Satzung lassen sich die Nutzungsregeln ableiten. Es ist Aufgabe der Betriebsverantwortlichen, diese zu dokumentieren und transparent zu machen und in einer Form vorzulegen, dass die Nutzer diese verstehen und seine / ihre Zustimmung dazu eingeholt werden kann. Dabei ist allgemeinverständlich zu beschreiben, welche Daten (z. B. für welchen didaktischen Zweck) erhoben und verwendet werden und wer deshalb zu welchen Handlungen berechtigt sein soll. Diese Nutzungsregelungen sind die Voraussetzung dafür, die notwendigen Maßnahmen der Datensicherheit nach § 14 konkret festzulegen. Während das Verfahrensverzeichnis den Nutzer / die Nutzerin darüber informiert, wie mit seinen / ihren Daten umgegangen wird, weisen die Nutzungsregeln den Nutzer / die Nutzerin darauf hin, wie er / sie selbst u. a. mit den Daten umzugehen hat.

Erläuterungen zu § 6 Betriebsdaten

Bei Betriebsdaten handelt es sich um Bestandsdaten, die sich durch eine gewisse Beständigkeit auszeichnen, auch wenn sie sich grundsätzlich ändern können. Die Nutzung von E-Learning-Verfahren fällt dann nicht unter diese Regelung, wenn aus den Daten kein Rückschluss auf die einzelne Person erfolgen kann (Alias-Identitäten, keine gültigen E-Mail- oder IP-Adressen).

Abs. 1: Diese Daten dürfen nur verarbeitet werden, wenn und soweit dies für die Registrierung oder für die Verwaltung 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 Betriebsdaten müssen für die Registrierung oder die Nutzung unerlässlich sein. Möchte ein Lehrender / eine Lehrende nur aus Interesse gerne wissen, ob seine / ihre 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.

Abs. 2: Dass die Authentifizierung über den HRZ-Account erfolgt (und die Betriebsdaten damit selektiv aus der Nutzer-Datenbank gezogen werden), wird hier als Regelfall festgelegt. Die getrennte Authentifizierung hingegen wird als Sonderfall eingeordnet, wenn zum Beispiel das gewählte Prüfungssystem noch nicht an die Authentifizierungs-Datenbank des HRZ angeschlossen ist oder ausdrücklich externen Nutzern ein Zugang zur E-Prüfung ermöglicht werden soll. Details zur Teilnahmeberechtigung externer Nutzer sind in § 2 ausgeführt.

Erläuterungen zu § 7 Nutzungsdaten

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.

Abs. 1: 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.

Nach Abs. 2 darf die Verarbeitung dieser Daten nur erfolgen, soweit dies für die Nutzung von E-Learning-Verfahren erforderlich ist. Dies ist z. B. der Fall, um überhaupt den Zugriff auf E-Learning-Inhalte zu ermöglichen. Eine weitergehende Verwendung ist jedoch nur dann zulässig, wenn sie erforderlich ist, um den Zweck des E-Learning-Verfahrens zu erreichen (also nicht zur allgemeinen Kontrolle, siehe Abs. 1). Ein Lehrender / Eine Lehrende darf daher nicht aus bloßem Interesse nachschauen, welcher Studierende zu welchem Zeitpunkt E-Learning-Verfahren genutzt hat.

Nach Abs. 3 können die Daten aber zum Beispiel für das Skillmanagement genutzt werden. Im Rahmen des Skillmanagements 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.

Erläuterungen zu § 8 Inhaltsdaten

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 den Verantwortlichen oder andere Teilnehmer der Lehrveranstaltung muss daher grundsätzlich möglich sein. Sie müssen im Regelfall mit Personenbezug ausgewertet und verarbeitet werden.

Urheberrechtliche Fragestellungen sind vom Anwendungsbereich dieser Satzung ausgenommen.

Erläuterungen zu § 9 Datenverarbeitung für wissenschaftliche Forschungszwecke

Abs. 1 erlaubt die Verarbeitung aller drei Datenarten, also Betriebs-, 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 Forscher 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. Schutzwürdige Belange werden insbesondere beeinträchtigt, wenn die Verarbeitung, gemessen an ihrer Eignung und ihrer Erforderlichkeit zu dem vorgesehenen Zweck, Betroffene unverhältnismäßig belastet. Die Abwägungskriterien bezüglich des schutzwürdigen Interesses, Offenkundigkeit entspricht den Regelungen des § 33 HDGS.

Abs. 2 führt eine strenge Zweckbindung ein. Satz 1 stellt ausdrücklich klar, dass eine Verarbeitung nur zu Forschungszwecken zulässig ist und die Daten nicht zu anderen Zwecken verwendet werden dürfen.

Abs. 3 begrenzt die Möglichkeit der Übermittlung der Daten. Daten, die für Zwecke der Forschung verarbeitet wurden, dürfen nur zu Forschungszwecken und nur aufgrund einer Einwilligung des Nutzers / der Nutzerin an Forscher und Forscherinnen in anderen Forschungsinstitutionen weitergegeben werden. Solange die Daten Personenbezug haben, ist dies nur aufgrund einer Einwilligung der Betroffenen zulässig. Hier geht es um einen Satz von personenbezogenen Rohdaten. Dies ist nicht zu verwechseln mit der Weitergabe von anonymen Forschungsergebnissen.

Abs. 4: § 33 HDGS „Datenverarbeitung für wissenschaftliche Zwecke“ wird durch diese Regelungen nicht ersetzt.

Erläuterungen zu § 10 Aufzeichnung und Übertragung von Lehrveranstaltungen

Abs. 1: Auch wenn dies so weit wie möglich vermieden werden soll, lässt es sich (z.B. bei einer Vorlesungsaufzeichnung) 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 trotzdem 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 diese weiterverwendet werden.

Abs. 2: Wird die Aufzeichnung öffentlich gemacht (z.B. auf YouTube), sind die erkennbaren Personen besonders zu schützen. Es reicht nicht aus, wenn im Fall der Individualisierung lediglich im Vorfeld der Aufnahme informiert wird; es ist eine schriftliche Einwilligung hierfür erforderlich.

Abs. 3: Werden keine schutzwürdigen Belange Dritter (der Veranstaltungsteilnehmenden) berührt, kann der Lehrende /die Lehrende frei bestimmen, ob die Aufzeichnung universitätsintern oder öffentlich verfügbar sein soll.

Erläuterungen zu § 11 Anforderungen an automatisierte Bewertungen

Probleme können 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 dem Verantwortlichen automatisch erzeugt, ist dadurch auch gesichert, dass der Leistungsnachweis nicht zwischen Abgabe und Zeitstempelung manipuliert wurde, weil hierfür keine Zeit war.

Erläuterungen zu § 12 Einwilligung

Abs. 1: Die übliche Verarbeitung personenbezogener Daten in E-Learning-Verfahren wird durch die §§ 6-10 erlaubt. Ist dies ausnahmsweise nicht der Fall, kann die Verarbeitung personenbezogener Daten nur durch eine Einwilligung des Betroffenen / der Betroffenen gerechtfertigt werden.

Die Einwilligung ist der stärkste Ausdruck des Rechts auf informationelle Selbstbestimmung, da sie es dem Betroffenen / der Betroffenen überlässt, selbst über Art, Umfang, Zweck und Dauer des Umgangs mit seinen Daten zu entscheiden. Dies ist jedoch nur möglich, wenn der Nutzer / die Nutzerin weiß, worin er / sie einwilligt, also was mit seinen / ihren Daten geschehen wird, und wenn er / sie die Entscheidung über die Einwilligung frei von äußeren Zwängen treffen kann. Daher darf ein Nutzer / eine Nutzerin nicht gezwungen sein, eine Einwilligung zu erteilen, um eine Veranstaltung zu besuchen, die er / sie 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. 2 letzter Satz enthält ein so genanntes Kopplungsverbot. Dieses verhindert, dass die Teilnahme an einer Lehrveranstaltung von der Einwilligung des Nutzers / der Nutzerin 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.

Erläuterungen zu § 13 Speicherfristen

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.

Abs. 1: Hier geht es um Nutzungsdaten, die entweder nicht von vornherein anonymisiert sind oder die keinem konkreten Lehrziel zuzuordnen sind (siehe § 7).

Abs. 2: Die Regelung bezüglich der Inhaltsdaten geht davon aus, dass Veranstaltungen grundsätzlich zu Semesterende beendet sind und zwei Semester später kein Bedürfnis mehr nach den Inhaltsdaten des vorigen Semesters besteht.

Ein Fall, der eine Ausnahme darstellen würde, wäre, dass die Lernenden längerfristig Zugang zu einer Forendiskussion haben sollen, die sie selbst geführt haben, um im Rückblick individuelle Lernfortschritte nachvollziehen zu können. Hier leitet sich aus dem Zweck des Forums die Notwendigkeit der längerfristigen Speicherung ab. Ähnlich gelagert sind Selbstlernmodule, die zum längerfristigen Üben und Rekapitulieren gedacht sind und den Lernfortschritt für die Lernenden sichtbar machen. Anders verhält es sich hingegen mit einer Forendiskussion aus der Vergangenheit, die anderen Lernenden als Anschauungsmaterial dienen soll. Dies wirkt sich nicht auf das Erreichen des Lernzieles des / der ursprünglich Beitragenden aus und daher lässt sich keine Berechtigung der dauerhaften Speicherung dieser personenbezogenen Daten herleiten. Der / Die ursprüngliche Beitragende darf erwarten, dass sein / ihr Beitrag gelöscht oder anonymisiert wird, ohne dass er /sie dies selbst in die Wege leiten müsste.

Abs. 3 wiederholt die Bestimmungen aus §10 Abs. 3. Wenn nur der Lehrende / die Lehrende erkennbar ist, kann dieser / diese frei über die Dauer des Zugangs zur Veranstaltungsaufzeichnung bestimmen.

Abs. 4 schränkt Abs. 3 für den Fall ein, dass der / die Aufgezeichnete aus dem Universitätsdienst ausscheidet. Er / Sie kann nicht verlangen, dass die Universität die Aufzeichnung dauerhaft verfügbar hält.

Erläuterungen zu § 14 Datensicherheit

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.

Abs. 1 enthält eine Generalklausel, die die Pflichten der Betriebsverantwortlichen in allgemeiner Form darstellt.

Abs. 2 beschreibt vier typische Schutzmaßnahmen. Ob und in welcher Form die Schutzmaßnahmen notwendig sind, ergibt sich aus der nach § 5 Abs. 1 zu erstellenden Vorabkontrolle 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 die Berechtigungen (z. B. Administrator / Administratorin, Verantwortlicher / Verantwortliche, Nutzer / Nutzerin 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 der Vorabkontrolle 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 durch eine Festlegung der Kontrolle der Zugriffsbefugnisse (nach Daten, Programmen und Art des Zugriffs), Protokollierung von Zugriffen, Funktionsbegrenzung und Verschlüsselung der Daten erreicht werden.
In manchen E-Learning-Verfahren ist es notwendig, nachträglich feststellen zu können, welche Daten wann und 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. Sollen Protokolldateien ausgewertet werden, so muss dies nach dem Vier-Augen-Prinzip durch eine andere Person als den Systemadministrator / die Systemadministratorin geschehen. Die Umsetzung dieser Sicherungsmaßnahmen kann abhängig vom konkreten E-Learning-Verfahren auch kontraproduktiv sein. In solchen Fällen ist auf diese Sicherungsmaßnahmen zu verzichten.