Hochschule Merseburg
University of Applied Sciences

Amtliche Bekanntmachungen
Nr. 17/2019

Herausgeber: Rektor

Redaktion: Dezernat Akademische Angelegenheiten

Merseburg,
30. September 2019

Inhaltsverzeichnis

Prof. Dr.-Ing. Jörg Kirbs
Rektor

Ordnung zum Datenschutz

Auf der Grundlage der §§ 54, 67 Abs. 2 S.1 des Hochschulgesetzes des Landes Sachsen-Anhalt (HSG LSA), in der Fassung der Bekanntmachung vom 14. Dezember 2010 (GVBl. LSA S.600, GVBl. 2011, S. 561), zuletzt geändert durch Artikel 14 Abs. 15 des Gesetzes vom 13. Juni 2018 (GVBl. LSA S. 72, 118) hat der Senat der Hochschule Merseburg folgende Ordnung zum Datenschutz erlassen:

§ 1 Geltungsbereich

(1) Diese Ordnung ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten an der Hochschule Merseburg.

(2) Mit dieser Ordnung sollen die Grundrechte und Grundfreiheiten von Betroffenen, insbesondere ihr Recht auf Schutz personenbezogener Daten, gewahrt und geschützt werden.

(3) Diese Ordnung gilt persönlich für alle Angehörigen der Hochschule Merseburg im Sinne des Hochschulgesetzes des Landes Sachsen-Anhalt.

(4) Die Gebote und Verbote dieser Ordnung gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser ditelektronisch oder in Papierform von statten geht.

§ 2 Begriffsbestimmungen

(1) Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierbare oder identifizierte natürliche Person beziehen (Betroffener). Hierzu gehören beispielsweise Studierendendaten oder Daten von Beschäftigten wie Name, E-Mail-Adresse, Autokennzeichen, Fotos, Videos oder Tonaufnahmen.

(2) Besondere Arten personenbezogener Daten sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

(3) Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(4) Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

(5) Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(6) Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit einer anderen Stelle über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(7) Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(8) Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

(9) Dritter ist eine natürliche oder juristische Person, die nicht Betroffener, Verantwortlicher oder Auftragsverarbeiter ist, die aber unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiter befugt ist, personenbezogene Daten zu verarbeiten.

(10) Eine Einwilligung des Betroffenen ist jede freiwillige und unmissverständliche Willensbekundung für einen konkreten Fall. Die Einwilligung kann in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung erteilt werden.

§ 3 Datenschutzbeauftragter

(1) Gemäß Art. 37 DS-GVO und §14a des DSG-LSA setzt die Hochschule Merseburg eine beauftragte Person für den Datenschutz (Datenschutzbeauftragter) ein. Diese Person ist in ihrer Funktion weisungsfrei. Die beauftragte Person darf zur Erfüllung der Aufgaben Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen und ist zur Verschwiegenheit verpflichtet.

(2) Der Aufgabenbereich des Datenschutzbeauftragten umfasst:

- Unterstützung der Hochschulleitung bei der Durchsetzung der gesetzlichen Bestimmungen des Datenschutzes,
- Beratung der Hochschulangehörigen bei der Einführung von Verfahren zur Verarbeitung personenbezogener Daten,
- Durchführung einer Vorabkontrolle (siehe § 6),
- Unterrichtung und Beratung von Mitarbeitern über Fragen des Datenschutzes und der Informationsfreiheit nach Abstimmung mit der Hochschulleitung und

- Kontrolle des Verzeichnisses automatisierter Verfahren zur Verarbeitung personenbezogener Daten (Verfahrensverzeichnis, siehe § 13).

(3) Den Datenschutzbeauftragten erreichen Sie unter folgenden Kontaktdaten: datenschutzbeauftragter@hs-merseburg.de.

(4) Die Hochschule und ihre Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen.

§ 4 Umgang mit personenbezogenen Daten

(1) Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, eine gesetzliche Norm erlaubt explizit die Verarbeitung personenbezogener Daten. Diese dürfen nach der DS-GVO grundsätzlich verarbeitet werden:
- bei einem bestehenden Vertrags- oder Rechtsverhältnis mit dem Betroffenen,
- im Zuge vorvertraglicher Maßnahmen auf Anfrage des Betroffenen sowie der Vertragsabwicklung mit den Betroffenen,
- wenn und soweit der Betroffene eingewilligt hat,
- wenn eine rechtliche Verpflichtung besteht, der die Hochschule unterliegt,
- wenn berechtigte Interessen der Hochschule bestehen, sofern nicht Interessen oder Grundrechte des Betroffenen überwiegen, insbesondere wenn es sich um ein Kind handelt. Datenverarbeitung unter Berufung auf ein berechtigtes Interesse sollte jedoch nicht ohne vorherige Beratung mit dem Datenschutzbeauftragten vorgenommen werden.

(2) Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck, so beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

(3) Falls möglich, sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitung sind vorzuziehen.

(4) Die Änderung einer Ziel- oder Zweckbestimmung, die einer Datenerhebung ursprünglich zugrunde gelegt wurde, ist neben der erklärten Einwilligung durch den Betroffenen nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist. Hierbei sind insbesondere die vernünftigen Erwartungen des Betroffenen hinsichtlich einer solchen Weiterverarbeitung gegenüber dem Unternehmen, die Art der verwendeten Daten, die Folgen für den Betroffenen sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

(5) Der Betroffene ist bei der Erhebung seiner personenbezogenen Daten umfassend über den Umgang mit seinen Daten zu informieren. Diese Informationen finden Sie in der Datenschutzerklärung der Hochschule Merseburg unter: www.hs-merseburg.de/datenschutz.

(6) Werden personenbezogene Daten nicht beim Betroffenen erhoben, sondern anderweitig beschafft, ist der Betroffene nachträglich und umfassend gemäß

Art. 14 DS-GVO über den Umgang mit seinen Daten zu informieren. Dies gilt auch für die Änderung einer Ziel- und Zweckbestimmung der Datenverarbeitung.

(7) Personenbezogene Daten müssen sachlich richtig und wenn nötig auf dem neuesten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die jeweilige Fachabteilung oder der jeweilige Fachbereich hat für die Umsetzung durch die Etablierung entsprechender Prozesse Sorge zu tragen. Ebenso sind Datenbestände regelmäßig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu prüfen.

§ 5 Vorabkontrolle / Datenschutz-Folgeabschätzung und Verfahrensverzeichnis

(1) Vor der Einführung jeglicher Verarbeitung ist eine Vorabkontrolle durchzuführen, bei der die Einhaltung der datenschutzrechtlichen Bestimmungen zu überprüfen ist. Unter Vorabkontrolle ist eine Risikoabschätzung zu verstehen, ob die mit der Verarbeitung verbundenen Risiken für die betroffene Person hinnehmbar sind.

(2) Zu diesem Zwecke ist die für den Datenschutz beauftragte Person rechtzeitig und umfassend durch den Verantwortlichen zu informieren. Ohne erfolgte Vorabkontrolle darf keine Verarbeitung personenbezogener Daten durchgeführt werden.

(3) Verarbeitungstätigkeiten sind zwingend in Verarbeitungsverzeichnissen zu dokumentieren. Hierzu ist das bereitgestellte Formblatt zu verwenden. Der Datenschutzbeauftragte kann zur Beratung hinsichtlich der gesetzlich geforderten Informationen hinzugezogen werden.

(4) Die Hochschule Merseburg stellt der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist der Datenschutzbeauftragte im Einvernehmen mit der Hochschulleitung.

§ 6 Datenübermittlung

(1) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

(2) Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der Empfangsstelle kein angemessenes Datenschutzniveau vorhanden ist und über besondere Vertragsklauseln nicht hergestellt werden kann.

§ 7 Auftragsdatenverarbeitung

(1) Sämtliche Verarbeitungsvorgänge personenbezogener Daten, bei denen Hochschulfremde beteiligt sind oder bei denen Auftragsverarbeiter als externe Dienstleister handeln, dürfen nur auf der Grundlage schriftlich dokumentierter vertraglicher Beziehungen durchgeführt werden. Alle derartigen

Verträge sind vor der Unterzeichnung durch die Stabsstelle Recht der Hochschule Merseburg zu prüfen; das betrifft auch alle Änderungen und Ergänzungen dieser Vertragsbeziehungen.

(2) Der Dienstleister ist von den Verantwortlichen der jeweiligen Bereiche im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen.

(3) Mündlich erteilte Anweisungen müssen unverzüglich schriftlich dokumentiert werden.

§ 8 Datenschutz in Lehre und Forschung

(1) Professoren und Professorinnen sowie Lehrkräfte haben die umfassende Verpflichtung, auch bei den wissenschaftlichen Arbeiten ihrer Studierenden die Einhaltung der datenschutzrechtlichen Bestimmungen zu überwachen. Das betrifft insbesondere Projekte im Internet.

(2) Alle Umfragen und Interviews, welche zu wissenschaftlichen Zwecken oder in der Lehre durchgeführt werden, sind zur Vorabkontrolle dem Datenschutzbeauftragten zur Kenntnis zu geben. Bei deren Durchführung ist § 6 zu beachten.

§ 9 Datenminimierung, Privacy by Desgin / Privacy by Default

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einem Betroffenen zu erheben, zu verarbeiten oder zu nutzen („Datenminimierung“). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen. Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern, so insbesondere den Grundsatz der Datenminimierung.

§ 10 Rechte von Betroffenen

(1) Betroffene haben das Recht auf Auskunft über die in der Hochschule Merseburg über ihre Person gespeicherten personenbezogenen Daten.

(2) Bei der Bearbeitung von Anträgen auf Auskunft ist die Identität der betroffenen Person zweifelsfrei festzustellen. Bei Zweifeln an der Identität können zusätzliche Angaben vom Antragsteller angefordert werden.

(3) Die Auskunftserteilung erfolgt schriftlich, es sei denn der Betroffene hat den Antrag auf Auskunft elektronisch gestellt. Der Auskunft ist eine Kopie der Daten des Betroffenen beizufügen, die, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie

alle weiteren gesetzlich geforderten Informationen nach Art. 15 DS-GVO beinhaltet, um den Betroffenen die Verarbeitung bewusst zu machen und die Rechtmäßigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch des Betroffenen werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Das Rechenzentrum legt den hierfür vorzusehenden Standard fest.

(4) Betroffene haben einen Anspruch auf Berichtigung ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.

(5) Der Betroffene hat das Recht auf Löschung seiner personenbezogenen Daten unter den folgenden Voraussetzungen:
   a) die Verarbeitung der Daten ist für die Erfüllung des Zwecks nicht mehr erforderlich,
   b) der Betroffene hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung,
   c) ihre Verarbeitung ist unzulässig,
   d) der Betroffene legt Widerspruch gegen die Verarbeitung zu Werbezwecken ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen - zu begründenden - persönlichen Situation,
   e) es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

(6) Der Betroffene kann die Einschränkung der Verarbeitung seiner Daten verlangen, wenn:
   a) die Richtigkeit der personenbezogenen Daten strittig ist, jedoch nur so lange, wie die Richtigkeit durch die zuständige Fachabteilung oder den zuständigen Fachbereich überprüft wird oder
   b) die Verarbeitung unzulässig ist, der Betroffene die Datenlöschung aber ablehnt und Einschränkung verlangt, oder
   c) die Hochschule die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, der Betroffene die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
   d) der Betroffene Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Fachabteilung noch mit der Prüfung des Widerspruchs befasst ist.
   e) Der Betroffene ist innerhalb eines Monats über alle ergriffenen Maßnahmen, die auf seinen Antrag hin erfolgt sind, zu informieren.
   f) Der Datenschutzbeauftragte steht dem Betroffenen bei der Wahrung seiner Rechte beratend zur Verfügung.

§ 11 Auskunftsersuchen Dritter über Betroffene

Sollte eine Stelle Informationen über Betroffene anfordern, so beispielsweise Fachbereiche oder Beschäftigte der Hochschule Merseburg oder Behörden, ist eine Weitergabe von Informationen nur zulässig, wenn

(1) die Auskunft gebende Stelle ein berechtigtes Interesse hierfür darlegen kann, und

(2) eine gesetzliche Norm zur Auskunft verpflichtet, sowie

(3) die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

§ 12 Werbung

(1) Die werbliche Ansprache von Betroffenen per Brief, Telefon, Fax, oder E-Mail ist grundsätzlich nur zulässig, wenn der Betroffene zuvor in die Verwendung seiner Daten zu Werbezwecken eingewilligt hat.
(2) Ausnahmen sind nur beim Vorliegen einer Erlaubnisnorm zulässig. Bitte konsultieren Sie diesbezüglich den Datenschutzbeauftragten**.**

§ 13 Schulung

Hochschulangehörige, die ständig oder regelmäßig Zugang zu personenbezogenen Daten haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten betreiben oder entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Der Datenschutzbeauftragte entscheidet über Form und Turnus der entsprechenden Schulungen**.**

§ 14 Nutzung von IT-Ressourcen

Für alle dienstlichen Datenübertragungen oder -verarbeitungen (Dateitransfer, Terminplanung, E-Mail, Messengerdienste, Cloud-Computing usw.) sind Server der Hochschule, des DFN-Vereins oder entsprechende Ressourcen der Wissenschaftsinstitutionen der Bundesrepublik Deutschland zu nutzen. Wenn das in begründeten Einzelfällen nicht möglich ist, so ist streng darauf zu achten, dass die Datenverarbeitung oder -speicherung ausschließlich auf Servern stattfindet, die den deutschen Datenschutzgesetzen bzw. der DS-GVO unterliegen.

§ 15 Datenlöschung

(1) Personenbezogene Daten müssen zuverlässig gelöscht bzw. vernichtet werden, sobald der Zweck erfüllt ist, für den sie erhoben wurden. Das gilt, solange dem keine anderen rechtlichen Vorschriften zur Aufbewahrung oder Archivierung entgegenstehen. Durch geeignete organisatorische Maßnahmen ist das Fortbestehen der Bedingungen zur Aufbewahrung oder Archivierung regelmäßig zu überprüfen. Nach Wegfall von Bedingungen zur Aufbewahrung ist eine Löschung zeitnah zu veranlassen. Löschvorgänge können auch automatisiert erfolgen und sollen dokumentiert werden.

(2) Bei jeder Löschung sind auch Datensicherungen mit vertretbarem technischem Aufwand zu berücksichtigen.

(3) Zur sicheren Vernichtung von Datenträgern unterhält die Hochschule Merseburg Vertragsbeziehungen zu einem entsprechend zertifizierten Unternehmen. Entsprechende Bedarfe sind mit dem Dezernat Liegenschaften und Technik abzustimmen.

§ 16 Datengeheimnis

(1) Hochschulangehörigen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Beschäftigte der Hochschule

Merseburg sind vor Aufnahme ihrer Tätigkeit auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten. Die Verpflichtung erfolgt durch das Dezernat Personal unter Verwendung des hierzu vorgesehenen Formulars.

(2) Mitarbeiter mit besonderen Geheimhaltungsverpflichtungen (z. B. Fernmeldegeheimnis nach § 88 TKG) werden von der Hochschulleitung ergänzend darauf schriftlich verpflichtet.

§ 17 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) In Abhängigkeit der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit hat für jedes Verfahren eine dokumentierte Schutzbedarfsfeststellung und Analyse hinsichtlich der Risiken für Betroffene zu erfolgen.

(2) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten wird ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren verbindlich ist. Hierin ist insbesondere der Stand der Technik ebenso zu berücksichtigen, wie Mittel und Maßnahmen zur Verschlüsselung und Datensicherung. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Maßnahmen regelmäßig zu überprüfen und zu bewerten.

(3) Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Türen unbesetzter Räume sind zu verschließen. Wirksame Maßnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren.

(4) Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden. Passwörter müssen eine minimale Länge von zehn Zeichen aufweisen und aus einem Zeichenmix bestehen. Passwörter dürfen nicht notiert oder aus leicht zu erratenden Begriffen gebildet werden, insbesondere nicht Begriffe, die im Zusammenhang mit dem Unternehmen stehen.

(5) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-know-Prinzip“). Zugriffsberechtigungen müssen jederzeit genau und vollständig festgelegt und dokumentiert sein.

(6) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

(7) Zu unterschiedlichen Zwecken erhobene personenbezogene Daten sind getrennt voneinander zu verarbeiten. Die Trennung von Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen.

(8) Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind im vertretbaren Aufwand zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten können aufgezeichnet und protokolliert werden.

§ 18 Verletzungen des Schutzes von Daten („Datenpanne“)

(1) Sollten personenbezogene Daten unrechtmäßig Dritten offenbart worden sein, ist darüber unverzüglich die Hochschulleitung zu informieren. Die Hochschulleitung bezieht unverzüglich den Datenschutzbeauftragten im Rahmen der Sachverhaltsaufklärung ein.

(2) Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

(3) Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt ausschließlich durch die Hochschulleitung. Betroffene werden durch die Hochschulleitung informiert, wobei der Datenschutzbeauftragte beratend hinzugezogen wird.

§ 19 Folgen von Verstößen

Ein grob fahrlässiger oder gar vorsätzlicher Verstoß gegen diese Ordnung kann für Beschäftigte arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen für alle Hochschulangehörigen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

§ 20 Rechenschaftspflicht

Die Einhaltung der Vorgaben dieser Richtlinie muss jederzeit nachgewiesen werden können. Hierbei ist insbesondere auf die Nachvollziehbarkeit und Transparenz getroffener Maßnahmen zu achten, so beispielsweise über zugehörige Dokumentationen.

§ 21 Anlagen

Das Formblatt Vorfallmeldung finden Sie unter:
www.hs-merseburg.de/datenschutz.
Das Formblatt Verarbeitungsverzeichnis befindet sich im Home-Intranet der Hochschule Merseburg
im Sharepoint der Hochschule Merseburg.

§ 22 Inkrafttreten

Diese Ordnung tritt mit Veröffentlichung in den Amtlichen Bekanntmachungen der Hochschule Merseburg in Kraft. Die Amtliche Bekanntmachung vom 16.10.2013 (Nr.13/2013) tritt außer Kraft.

Ausgefertigt aufgrund des Beschlusses des Senats vom 27.06.2019 sowie der Genehmigung des Rektors vom 27.09.2019.

Merseburg, den 30. September 2019

Prof. Dr.-Ing. Jörg Kirbs
Rektor