Ordnung zur Einrichtung und zum Betrieb des Identitätsmanagements an der Pädagogischen Hochschule Heidelberg vom 14.12.2016

Aufgrund von § 8 Abs. 5 des Landeshochschulgesetzes Baden-Württemberg (LHG) vom 1. Januar 2005 in der Fassung vom 10. Juli 2012 hat der Senat der Pädagogischen Hochschule Heidelberg am 15. Juli 2015 in Verbindung mit § 12 Abs. 4 LHG, mit § 15 Abs. 4 des Landesdatenschutzgesetzes Baden-Württemberg (LDSG) vom 18. September 2000 in der Fassung vom 3. Dezember 2013 und mit § 14 Abs. 1 sowie 15 Abs. 1 des Telemediengesetzes (TMG) vom 26. Februar 2007 in der Fassung vom 31. Mai 2010 die folgende Ordnung zur Einrichtung und zum Betrieb des Identitätsmanagements an der Pädagogischen Hochschule Heidelberg beschlossen:

Präambel

Die Pädagogische Hochschule (PH) Heidelberg strebt eine Integration ihrer komplexen und heterogenen IT-Systemlandschaft zu einer konsistenten, redundanzfreien, sicheren und die Persönlichkeitsrechte der Nutzer fördernden Umgebung im Sinne zentraler Dienste an. Zur effektiven, effizienten und sicheren Nutzung zentraler Dienste ist ein einheitliches Identitätsmanagement, im Folgenden IDM genannt, notwendig. Die zentrale Verwaltung der die Nutzer identifizierenden Daten für die zahlreichen, an der PH Heidelberg eingesetzten Quellsysteme und Zielsysteme entlastet die Dienstebetreiber von aufwändigen Routinearbeiten, erleichtert den ordnungsgemäßen Betrieb der eingesetzten Datenverarbeitungsanlagen und erhöht insgesamt das Sicherheitsniveau an der PH Heidelberg.

Das IDM dient der zentralen, einheitlichen und kontrollierten Zuteilung und Verwaltung der Identitäten und der Berechtigungen zur Nutzung von IT-Dienstleistungen aller Mitglieder und Angehörigen der Hochschule, sowie externer Nutzer. Das IDM stellt hierzu einen zentralen Service zum Zweck der Authentifizierung (d.h. dem Nachweis einer behaupteten Identität) sowie der Bereitstellung und Gewährung von Zugriffsrechten für alle hochschulbezogenen Informations- und Kommunikationssysteme und damit der Korrektheit und Aktualität der in diesen Systemen gespeicherten Personen-, Nutzer- und Berechtigungsdaten. Mit dem IDM wird eine Infrastruktur geschaffen, die

es Hochschulmitgliedern und anderen berechtigten Personen erlaubt, sich gegenüber allen IT-Diensten der Hochschule in einheitlicher Weise zu authentifizieren.

Ziel der Einführung des IDM ist, neben der Stärkung der Leistungsfähigkeit und Verbesserung der Servicefreundlichkeit der Hochschule, die Erhöhung des Datenschutzes durch Transparenz hinsichtlich der Verarbeitung personenbezogener Daten, und die Erhöhung der Datensicherheit durch einheitliche und definierte Verfahren zur Authentifizierung und Autorisierung.

§ 1 Geltungsbereich und Zweck

(1) Das IDM betrifft alle Systeme und Informations- und Kommunikationsdienste (IuK-Dienste), die auf der Grundlage der für die PH Heidelberg verabschiedeten Verwaltungs- und Benutzungsordnung durch das Rechenzentrum der PH betrieben werden und eine Authentifizierung der Nutzer voraussetzen.

(2) Zweck des IDM ist die konsolidierte Authentifizierung der Nutzer und zuverlässige Rechteverwaltung für hochschulbezogene Informations- und Kommunikationssysteme bzw. IuK-Dienste.

(3) Das IDM importiert zu diesem Zweck personenidentifizierende Daten aus an der PH Heidelberg eingesetzten Quellsystemen (inklusive bestehender Verzeichnisdienste) bzw. aus manuellen Eingaben zur Person der Nutzer der vom Rechenzentrum bzw. von Verbünden, denen die PH Heidelberg angehört, betreuten Systeme. Zudem exportiert das IDM zu diesem Zweck Ergebnisdaten hinsichtlich der Authentifizierung an festgelegte Zielsysteme (inklusive bestehender Verzeichnisdienste), die von der PH Heidelberg oder von Verbünden, denen die PH Heidelberg angehört, betrieben werden. Die für den Import vorgesehenen Quellsysteme und die für den Export vorgesehenen Zielsysteme sind in der Anlage A aufgelistet. Das Rechenzentrum ist berechtigt, in Abstimmung mit dem behördlichen Datenschutzbeauftragten und dem Personalrat diese Anlage aufgrund aktueller Entwicklungen fortzuschreiben und anzupassen. Die jeweilige Neufassung der Anlage A ist vom Senat zu verabschieden.

(4) Zur Erfüllung dieses Zwecks werden Bestandsdaten zu an der PH Heidelberg eingerichteten Mail-Accounts der Nutzer (Telemediendaten) sowie Stammdaten über Mitglieder und Angehörige der PH Heidelberg aus eingerichteten Verwaltungsprogrammen eingelesen und vom IDM verwaltet. Das betrifft auch Stammdaten der Beschäftigten nach § 36 Abs. 1 LDSG sowie der Studierenden nach § 12 Abs. 1 und 4 LHG. Die aus den Quellsystemen zu importierenden Daten, die im IDM zu speichernden Daten und die in die Zielsysteme zu exportierenden Daten sind in der Anlage A aufgelistet. Das Rechenzentrum ist berechtigt, in Abstimmung mit dem behördlichen Datenschutzbeauftragten und dem Personalrat diese Anlage aufgrund aktueller Entwicklungen fortzuschreiben und anzupassen. Die jeweilige Neufassung der Anlage A ist vom Senat zu verabschieden.

(5) Die Verwendung einer Mail-Adresse, die zur Domäne der PH Heidelberg gehört, kann für die Verwaltung der Identifikationsdaten im IDM als Voraussetzung festgelegt werden.

(6) Nutzern steht die Option zur Verfügung, Zugangs- oder Zugriffsbefugnisse in begründeten Einzelfällen unabhängig von der Rechteverwaltung im IDM bzw. in den Zielsystemen zu beantragen. In diesen Fällen findet eine manuelle Prüfung im Rahmen der Rechteverwaltung statt.

(7) Regelungen in anderen Ordnungen der PH Heidelberg oder in Dienstvereinbarungen der PH Heidelberg bleiben von dieser Ordnung unberührt.

§ 2 Begriffsbestimmungen

(1) Das IDM dient der zentralen Verwaltung personenidentifizierender Daten über die Nutzer von Systemen, die durch das Rechenzentrum oder einem Verbund, dem die PH Heidelberg angehört, betrieben werden.

(2) Personenidentifizierende Daten sind Daten, die eine eindeutige Authentifizierung eines Nutzers ermöglichen.

(3) Authentifizierung im Sinne dieser Ordnung ist der eindeutige Nachweis einer vom Nutzer behaupteten Identität.

(4) Eine Authentifizierung ist die Voraussetzung zur Gewährung von Zugangs- und Zugriffsrechten (Autorisierung).

(5) Rechteverwaltung im Sinne dieser Ordnung ist die Bereitstellung von Zugangs- und Zugriffsrechten, die ein Nutzer im Rahmen seiner Tätigkeiten, Aufgaben oder zur Ausübung von Rechten, die im Zusammenhang mit der Nutzung von Informations- und Kommunikationstechnologie bzw. IuK-Diensten an der PH Heidelberg stehen, benötigt.

(6) Zugangsrechte sind Befugnisse eines Nutzers, sich an einem System anmelden zu können.

(7) Zugriffsrechte sind Befugnisse eines Nutzers, ein bestimmtes Programm, eine bestimmte Anwendung oder einen bestimmten IuK-Dienst nutzen zu können bzw. mittels dieses Programms, dieser Anwendung oder dieses IuK-Dienstes gespeicherte Daten einsehen, ggf. verändern, ggf. sperren, ggf. löschen bzw. sonst nutzen zu dürfen oder Daten eingeben zu dürfen.

(8) Nutzer sind Personen, die Mitglied oder Angehöriger der PH Heidelberg oder sonstige Zugangs- oder Zugriffsbefugte auf Systeme oder IuK-Dienste der PH Heidelberg bzw. von Verbünden, denen die PH Heidelberg angehört, sind.

(9) Ein Quellsystem im Sinne dieser Ordnung ist ein System, ein Programm, eine Anwendung oder ein IuK-Dienst, aus dem das IDM Daten importiert.

(10) Ein Zielsystem im Sinne dieser Ordnung ist ein System, ein Programm, eine Anwendung oder ein IuK-Dienst, in das das IDM Daten exportiert.

(11) Import im Sinne dieser Ordnung bedeutet, dass Daten in einem System, einem Programm, einer Anwendung oder einem IuK-Dienst eingelesen werden.

(12) Export im Sinne dieser Ordnung bedeutet, dass Daten in ein System, ein Programm, eine Anwendung oder einen IuK-Dienst übertragen und dort importiert werden.

(13) Bestandsdaten sind Daten im Sinne von § 14 Abs. 1 TMG.

(14) Stammdaten sind Daten, die zur systemtechnischen Anlage von Personen, die mittels eines Systems bzw. IuK-Dienstes verwaltet werden, benötigt werden.

(15) Ein Verbund ist ein hochschulübergreifender Zusammenschluss. Im Rahmen des IDM sind nur Verbünde im Sinne von § 28 Abs. 1 Nr. 3 LHG relevant.

(16) Konsolidiert ist eine Authentifizierung eines Nutzers, wenn es genau eine PH-weite Identität für einen Nutzer gibt.

(17) Zuverlässig ist eine Rechteverwaltung, wenn einem Nutzer nicht mehr Zugangs- und Zugriffsrechte zustehen, als dieser für die Erledigung seiner Tätigkeiten, Aufgaben oder zur Ausübung von Rechten, die im Zusammenhang mit der Nutzung von Informations- und Kommunikationstechnologie bzw. IuK-Diensten an der PH Heidelberg stehen, benötigt.

§ 3 Verantwortlichkeiten

(1) Für den Betrieb des IDM und seiner Schnittstellen zu Quellsystemen und Zielsystemen ist das Rechenzentrum der PH Heidelberg verantwortlich.

(2) Für die Zulässigkeit der Einrichtung und des Betriebs der eingerichteten Schnittstellen zum Import in das IDM bzw. Export aus dem IDM ist die jeweilige datenverarbeitende Stelle verantwortlich.

§ 4 Verarbeitung personenbezogener Daten

(1) Im IDM werden personenbezogene Daten der Nutzer verarbeitet im Sinne von § 3 Abs. 2 LDSG.

(2) Die Verarbeitung personenbezogener Daten erfolgt im IDM ausschließlich zu den in § 1 dieser Ordnung festgelegten Zwecken. Die dazu verarbeiteten Daten unterliegen im IDM der besonderen Zweckbindung aus § 15 Abs. 4 LDSG.

(3) Die im IDM gespeicherten Daten dürfen nur an Zielsysteme exportiert werden, soweit diese für den ordnungsgemäßen Betrieb des Zielsystems erforderlich sind und dies den in § 1 dieser Ordnung festgelegten Zwecken dient. Die Zwecke der Verwendung der exportierten Daten im Zielsystem bestimmen sich ansonsten anhand der zugehörigen Rechtsgrundlagen für das Zielsystem. Die Authentifizierung bzw. Rechtevergabe für das Zielsystem darf stellvertretend im IDM vorgenommen werden.

(4) Zur Erfüllung der in § 1 dieser Ordnung festgelegten Zwecke dürfen für das IDM erforderliche Daten aus Quellsystemen in das IDM importiert werden.

(5) Beim Ausscheiden eines Nutzers aus den Zugangs- bzw. Zugriffsberechtigten auf Systeme oder IuK-Dienste der PH Heidelberg bzw. der Verbünde, denen die PH Heidelberg angehört, werden die Nutzerdaten im IDM gesperrt. Die Löschungsfristen sind in der zum IDM im Verfahrensverzeichnis dokumentierten Verfahrensbeschreibung festgelegt (Anlage C).

(6) Kennungen, die zur Vergabe und Verwaltung von Zugangsrechten verwendet werden, und Mail-Account-Daten der Nutzer werden mit Ablauf der Löschungsfrist dauerhaft archiviert, um eine nochmalige Vergabe dieser IDM-Daten an andere Personen verhindern zu können. Tritt ein ausgeschiedener Nutzer zu einem späteren Zeitpunkt wieder in die PH Heidelberg ein bzw. wird nutzungsbefugt auf Systeme bzw. IuK-Dienste der PH Heidelberg werden die gesperrten IDM-Daten, soweit erforderlich, wieder aktiviert.

(7) Durch die zentrale und stellvertretend für die Zielsysteme erfolgende Datenhaltung von Authentifizierungsdaten im IDM wird der Grundsatz der Datensparsamkeit aus § 9 Abs. 1 LDSG umgesetzt und die effiziente sowie effektive Umsetzung der Maßnahmen aus § 9 Abs. 3 LDSG ermöglicht und unterstützt.

§ 5 Zugriffsrechte

(1) Grundlage für die Vergabe von Zugriffsberechtigungen im IDM ist ein mehrstufiges Rechtekonzept.

(2) Die im Rahmen der Administration des IDM eingerichteten Zugriffsrechte sind in der Anlage B beschrieben. Das Rechenzentrum ist berechtigt, in Abstimmung mit dem behördlichen Datenschutzbeauftragten und dem Personalrat diese Anlage aufgrund aktueller Entwicklungen fortzuschreiben und anzupassen. Die jeweilige Neufassung der Anlage B ist vom Senat zu verabschieden.

§ 6 Technische und organisatorische Maßnahmen

(1) Die zum Schutz des IDM ergriffenen technischen und organisatorischen Maßnahmen sind in der zum IDM im Verfahrensverzeichnis dokumentierten Verfahrensbeschreibung dokumentiert (Anlage C).

(2) Die Beschreibung der ergriffenen Maßnahmen darf durch das Rechenzentrum in Abstimmung mit dem behördlichen Datenschutzbeauftragten und dem Personalrat diese Anlage C aufgrund aktueller Entwicklungen fortgeschrieben und anpassen. Die jeweilige Neufassung der Anlage C ist vom Senat zu verabschieden.

(3) Protokolldaten im Rahmen des Störfall- und Changemanagements sind zwei Wochen aufzubewahren. Hierzu zählen Nachweise über den Datenimport ins IDM, Nachweise über die Datensicherung und Nachweise über systemtechnische Änderungen der IDM Systeme.

(4) Protokolldaten im Rahmen der Verfahrensdokumentation sind fünf Jahre aufzubewahren. Hierzu zählen Nachweise über die Rechteverwaltung des IDM und Nachweise über die Rechteverwaltung mittels IDM, soweit die Zielsysteme keine längeren Aufbewahrungsfristen vorschreiben.

§ 7 Schlussbestimmungen und Übergangsvorschriften

(1) Das IDM ist aufgrund der technologischen Entwicklung und der sich stetig wandelnden Systemlandschaft an der PH Heidelberg einer permanenten Änderung unterworfen. In den Anlagen zu dieser Ordnung sind daher die jeweils aktuellen Gegebenheiten darzustellen. Die entsprechende Umsetzung hat daher in Abstimmung mit dem behördlichen Datenschutzbe-

auftragten und dem Personalrat unabhängig von der formellen Verabschiedung der Anpassung durch den Senat zu erfolgen. Eine Ablehnung einer Anpassung durch den Senat führt zur Rücksetzung des vorherigen Zustandes, bis ein Einvernehmen hergestellt werden kann. Der vorherige Zustand muss für diesen Zeitraum wiederherstellbar sein.

(2) In den Anlagen werden Sachverhalte beschrieben, die einem besonderen Schutzbedarf unterliegen und daher nicht zu veröffentlichen sind, um den ordnungsgemäßen Betrieb der Quellsysteme, der Zielsysteme und des IDM selbst nicht zu gefährden. Daher werden die Anlagen dieser Ordnung nicht veröffentlicht. Eine begründete Einsichtnahme kann beim behördlichen Datenschutzbeauftragten bzw. beim Personalrat vorgenommen werden.

(3) Die derzeitige Nutzerverwaltung des Rechenzentrums verbleibt im Produktivbetrieb, bis ihre Funktionalität vollständig durch das IDM abgelöst ist. In dieser Übergangszeit werden beide Systeme parallel betrieben.

§ 8 Veröffentlichung und Inkrafttreten

(1) Diese Ordnung tritt am Tage nach Veröffentlichung in den Amtlichen Bekanntmachungen der PH Heidelberg in Kraft.

(2) Die Anlagen treten jeweils nach erfolgter Abstimmung mit dem behördlichen Datenschutzbeauftragten der PH Heidelberg und dem Personalrat der PH Heidelberg in Kraft.

Heidelberg, 14.12.2016

gez. Prof. Dr. Hans-Werner Huneke
(Rektor)

Anlagen zu dieser Ordnung

A. Übersicht zu den vom IDM genutzten Datenarten und zu den am IDM angeschlossenen Quell- und Zielsystemen.
(Dokument: IDM_01_Übersicht_DatenQuellenZiele_HD)

B. Administrations- und Berechtigungskonzepts des IDM.
(Dokument: IDM_02_AdminBerechtigungskonzept_HD)

C. Verfahrensbeschreibung zum IDM nach § 11 LDSG.
(Dokument: IDM_03_Verfahrensbeschreibung_11LDSG_HD)