weißensee kunsthochschule berlin

Mitteilungsblatt

Herausgeberin:

Die Rektorin der Kunsthochschule
Berlin (Weißensee)
Bühringstraße 20, 13086 Berlin

Nr. 227

19.06.2017

Inhalt:

21 Seiten

Dienstvereinbarung über die Einführung und Anwendung eines Campus Management Systems (CMS)

Dienstvereinbarung

über die Einführung und Anwendung eines Campus Management Systems (CMS)

an der Kunsthochschule Berlin (Weißensee) (khb)

zwischen

der Rektorin

und

dem Personalrat

der Kunsthochschule Berlin Weißensee

Gem. § 74 Personalvertretungsgesetz Berlin (PersVG-Berlin) in der aktuellen Fassung wird zwischen der Leitung und dem Personalrat der weißensee kunsthochschule berlin (khb) nachstehende Dienstvereinbarung über die Anwendung und Weiterentwicklung des IT-Verfahrens „Campus Management System“ (CMS) abgeschlossen.

Präambel

Der Personalrat erkennt die veränderten Anforderungen an die Verwaltungsprozesse insbesondere der Studienverwaltung und die damit einhergehende Notwendigkeit einer neuen Software-Lösung für die weißensee kunsthochschule berlin an.
Mit der Einführung und Nutzung des IT-Verfahrens "Campus Management System" (im folgenden CMS) sowie den daraus möglicherweise entstehenden Veränderungen der Arbeitsorganisation und der Ablaufprozesse verfolgt die Hochschule das Ziel, die Qualität der Arbeitsprozesse im Zusammenhang mit den Kernprozessen von Lehre und Studium zu erhöhen und somit Arbeitsabläufe durch Unterstützung mit adäquaten IT-Werkzeugen zu verbessern.

Diese Dienstvereinbarung regelt die Einführung, Anwendung und Erweiterung des CMS und der eingesetzten Module an der weißensee Kunsthochschule Berlin mit folgenden Zielen:

- Sicherung der Beteiligung der Beschäftigten an der Gestaltung, Evaluierung und bei der Einführung des CMS
- Sicherung der Aus- und Fortbildung aller Beschäftigten im Hinblick auf den Einsatz des CMS

- Schutz der Mitarbeiter_innen vor Gesundheitsschädigung und Arbeitsüberlastung
- Schutz der Anwender_innen und Dienstkräfte vor unzulässiger Nutzung ihrer personengebundenen Daten
- Schutz der Mitarbeiter_innen vor nicht erfahrbaren und nachvollziehbaren individuellen Verhaltens- und Leistungskontrollen
- Schutz der Beschäftigten vor wirtschaftlichen Nachteilen und Abqualifizierung ihrer Tätigkeit

§ 1 Gegenstand und Geltungsbereich

Gegenstand der Dienstvereinbarung ist die Einführung, der laufende Betrieb und die Erweiterung des IT-Verfahrens „Campus Management System“ (im folgenden CMS abgekürzt).

Diese Dienstvereinbarung gilt für alle Beschäftigten der khb, die mit dem CMS oder Teilen davon arbeiten und vom Personalrat der khb vertreten werden.

§ 2 Zweckbestimmung

Das Verfahren CMS hat den Zweck, die Kernprozesse Lehre und Studium über den gesamten Student Life Cycle mit IT-Werkzeugen zu unterstützen.

§ 3 Grundsätze

Da eine abschließende Regelung zum Zeitpunkt der Produktivsetzung des CMS erfahrungsgemäß nicht möglich ist, vereinbaren die Hochschulleitung und die Personalvertretung ein Verfahren, das als kontinuierlicher Verbesserungsprozess installiert wird. Die Hochschule sichert deshalb der Personalvertretung eine Beteiligung bei der Gestaltung des CMS über den Zeitpunkt der Produktivsetzung hinaus zu.

Für die Nutzung und Weiterentwicklung des CMS werden zur Softwareergonomie die Standards der Normenreihe EN ISO 9241, Teil 110 und BildschArbV berücksichtigt. Zur Barrierefreiheit werden die Vorgaben der Verordnung zur Schaffung barrierefreier Informationstechnik (BITV) beachtet.

Während der Einführungsphase des CMS wird der Personalrat über Testtermine des Systems informiert. Ihm ist gestattet, an den Terminen teilzunehmen. Vorschläge des Personalrats werden, soweit technisch möglich, bei der Implementation des CMS berücksichtigt bzw. bei der Weiterentwicklung des Systems berücksichtigt.

Bei der Weiterentwicklung des Systems werden begründete Vorschläge der Nutzer_innen des CMS im Einvernehmen mit dem Personalrat bzw. Vorschläge des Personalrats an den Hersteller der Software weitergeleitet mit dem Ziel, Verbesserungen herbeizuführen.

Ab Beginn des Produktivbetriebs wird der Personalrat auf Antrag bzw. auf Wunsch von Beschäftigten zu Teamsitzungen des Referats für Studienangelegenheiten eingeladen. Zur Evaluation des Einsatzes des CMS hat der Personalrat das Recht, dass ihm einzelne Arbeits- bzw. Geschäftsprozesse präsentiert werden.

Über Änderungen des IT-Systems CMS und die Freischaltung und Nutzung weiterer Module wird der Personalrat rechtzeitig und umfassend informiert.

§ 4 Auswirkungen auf die Beschäftigten, Rechte der Beschäftigten

(1) Beschäftigte, deren Tätigkeiten mit dem CMS im Zusammenhang stehen, werden über die Veränderungen betrieblicher Abläufe umfassend informiert. Sie werden rechtzeitig und gründlich geschult. Hierzu werden geeignete Schulungsangebote unterbreitet

(2) Darüber hinaus wird für die in das IT-Verfahren CMS involvierten Mitarbeiter_innen ein auch online verfügbares Nutzer_innenhandbuch erstellt. Darüber hinaus werden Hilfetexte zu einzelnen Funktionen im System eingestellt.

(3) Beschäftigte, deren Aufgaben sich durch die Einführung des CMS ändern, werden mindestens

gleichwertig eingesetzt und dafür entsprechend qualifiziert.
Herabgruppierungen oder betriebsbedingte Kündigungen sind im Zusammenhang mit der Einführung und dem Betrieb des CMS ausgeschlossen.

(4) Sind übermäßige Belastungen der Beschäftigten absehbar oder wird eine übermäßige Belastung festgestellt, werden die Ursachen analysiert und es wird gemeinsam mit dem Personalrat nach Lösungen gesucht, die Belastungen zu reduzieren.

(5) Einführung und Änderungen des CMS sowie dessen Betrieb werden so geplant, dass die Regelungen in den einschlägigen Gesetzen, Tarifverträgen und Dienstvereinbarungen (z.B. bzgl. der Arbeitszeit) eingehalten werden.

§ 5 Durchführung von Qualifizierungsmaßnahmen

(1) Vor dem Einsatz der CMS-Software bzw. vor einer nicht unerheblichen Änderung werden die Betroffenen
rechtzeitig und umfassend über ihre neuen Aufgaben, über die neuen Arbeitsmethoden und über die neue Funktion bzw. Komponente unterrichtet und soweit erforderlich dafür qualifiziert.
Ziel der Qualifizierung ist nicht nur das Erlernen einer Abfolge von Bearbeitungsschritten, sondern das
grundsätzliche Verständnis des jeweiligen IT-Systems im Hinblick auf die Anforderungen des Arbeitsplatzes.

(2) Bei der Durchführung der Qualifizierungsmaßnahmen werden besondere persönliche Bedingungen, wie
z.B. eine Behinderung oder eine Teilzeitbeschäftigung, berücksichtigt.

(3) Den Beschäftigten wird ausreichend Zeit und Gelegenheit zur Einarbeitung gegeben. Die Beschäftigten
haben bei Bedarf Anspruch auf ergänzende Nach- und Vertiefungsschulungen.

(4) Die erforderlichen Qualifizierungsmaßnahmen werden rechtzeitig vor ihrer Durchführung mit dem Personalrat abgestimmt.

(5) Die für die Qualifizierungsmaßnahmen erforderliche Zeit ist Arbeitszeit. Alle Qualifizierungsmaßnahmen
finden in der Regel während der üblichen Arbeitszeit statt. Die Teilnehmer/innen von Schulungsmaßnahmen erhalten auf Wunsch zum Abschluss eine schriftliche Teilnahmebestätigung mit den Inhalten.

§ 6 Personenbezogene Daten

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich im Rahmen der gesetzlichen Grundlagen zu den im Verfahrensverzeichnis angegebenen Zwecken. Eine Einsichtnahme durch bzw. Auskunfterteilung an Dritte über personenbezogene Daten ist ausgeschlossen, außer es besteht dafür eine gesetzliche Verpflichtung.

§ 7 Auswertung von Verfahrensdaten (Leistungs- und Verhaltenskontrolle)

(1) Die Erfassung und Verarbeitung aller Daten, die im Zusammenhang mit Bewerbungs-, Studien- und Prüfungsvorgängen benötigt werden, dienen nicht der Leistungs- und Verhaltenskontrolle der Anwender_innen. Daten, die im Verfahren anfallen und aus Gründen der Systemsicherheit und des Datenschutzes erforderlich sind, werden nur zu diesem Zweck verwendet. Die Einsichtnahme in Datenbestände richtet sich nach dem Grundsatz der aufgaben- und zuständigkeits bezogenen Berechtigung. Dies wird in einem Rollen- und Berechtigungskonzept festgelegt.

(2) Verfahrensdaten dürfen grundsätzlich nur bei Unregelmäßigkeiten des Systems ausgewertet werden.
Der Personalrat ist neben dem/ der Datenschutzbeauftragten vorab zu informieren.

(3) Wenn hinreichende Anhaltspunkte den Verdacht auf ein schweres arbeitsrechtliches Fehlverhalten von Beschäftigten begründen, hat der Arbeitgeber den Personalrat über den Sachverhalt zu informieren und es ist mit ihm sowie unter Einbeziehung des/ der Datenschutzbeauftragten das weitere Vorgehen zur Frage nach einer Möglichkeit zur Datenauswertung einvernehmlich und rechtskonform festzulegen. Die Rechte der Beschäftigten aus dem PersVG bleiben davon unberührt.

§ 8 Auftragsdatenverarbeitung

Bei einer Datenverarbeitung durch Dritte, stellt die Hochschulleitung sicher, dass die gesetzlichen Regelungen, insbesondere die des Datenschutzes, beachtet werden. Über alle vertraglichen Änderungen wird neben dem/ der Datenschutzbeauftragten auch der Personalrat umgehend informiert.

§ 9 Dokumentation des IT-Verfahrens CMS

(1) Das IT-Verfahren CMS ist im Verfahrensverzeichnis beschrieben. Das Verfahrensverzeichnis ist der Dienstvereinbarung angefügt.

(2) Die Ausführung folgender Funktionen wird, soweit dies technisch realisierbar ist, automatisch in der Datenbank protokolliert
- jede Erweiterung der Softwarefunktionalität (Releasenotes)
- jede Änderung personenbezogener Daten der Beschäftigten
- jede Änderung der Zugriffe inkl. Änderungen am Rollen- und Rechtemodell

(3) Dabei ist jeweils zu protokollieren, wer wann welche dieser Aktivitäten ausgeführt hat.

(4) Der Personalrat erhält zur Wahrnehmung seiner Kontrollrechte das Recht zur Einsichtnahme in die Protokolle der Datenbank, unter Hinzuziehung des/ der Datenschutzbeauftragten. Auf Verlangen werden dem Personalrat hierzu technische Hilfsmittel und Expertise zur Verfügung gestellt.

§ 10 Rechte des Personalrats

(1) Über alle Änderungen der CMS-Software ist der Personalrat rechtzeitig, fortlaufend und umfassend zu informieren.

(2) Der Personalrat hat das Recht, an den Arbeitsgruppen, die im Rahmen der Struktur des Einführungsprojekts eingerichtet werden, teilzunehmen. Über die Entsendung von Mitgliedern des Personalrats bzw. von anderen Mitgliedern der Hochschule, die von diesem beauftragt sind, entscheidet der Personalrat.
Diese Teilnahme ersetzt nicht die vollständige Informationspflicht der Hochschule gem. PersVG und bedeutet nicht die Zustimmung des Personalrats zu den besprochenen Themen.

(3) Dem Personalrat sind alle Unterlagen über das Projekt, die zur Wahrnehmung seiner Aufgaben erforderlich sind, zugänglich zu machen und ggf. in einer für Laien geeigneten Form ausführlich zu erläutern.

§ 11 Inkrafttreten, Änderungen, Kündigung, Nachwirkung, Bekanntgabe

Diese Dienstvereinbarung tritt mit ihrer Unterzeichnung in Kraft.

Die Hochschulleitung und der Personalrat verpflichten sich, unverzüglich Verhandlung aufzunehmen, sollte sich aus dem Betrieb des CMS die Notwendigkeit zur Änderung dieser Dienstvereinbarung ergeben.

Diese Dienstvereinbarung kann mit einer Frist von drei Monaten zum Ende eines jeden Kalenderjahres schriftlich gekündigt werden. Im Falle einer Kündigung gelten die Regelungen der Dienstvereinbarung für den Zeitraum von 12 Monaten nach. Die Hochschulleitung und der Personalrat verpflichten sich jedoch unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufzunehmen.

Sollten einzelne Bestimmungen dieser Dienstvereinbarung ungültig oder unwirksam sein oder auf Grund rechtlicher Vorschriften ungültig werden, so bleiben die übrigen Bestimmungen davon unberührt.

Änderungen der Dienstvereinbarung bedürfen der Schriftform.

Die Hochschulleitung gibt diese Dienstvereinbarung in ihrer jeweils gültigen Fassung den betroffenen Beschäftigten in geeinigter Weise bekannt. Sie wird im Mitteilungsblatt der khb veröffentlicht.

Anlage
Verfahrensverzeichnis

Berlin, den 11.04.2017

gez. Baumann

Leonie Baumann
Rektorin

Berlin, den 26.04.2017

gez. Witt

Johannes Witt
Vorsitzender des Personalrats

Verfahrensverzeichnis

Inhalt

Verfahrensverzeichnis
Stand: 10.04.2017
Version 1.1 LA

1 Grundsätzliche Angaben

Beschreibung der Verfahren:

Bewerbung und Zulassung

Das mehrstufige Bewerbungs- und Zulassungsverfahren an der weißensee kunsthochschule berlin, im Folgenden kurz mit khb bezeichnet, ist in Zukunft online über das neue Campusmanagementsystem der CampusCore – Software für Hochschulen GmbH & Co. KG, im Folgenden kurz mit CampusCore bezeichnet, möglich. Studieninteressierte können sich dazu mit ihren Daten über das Portal registrieren, ihre Bewerbung dort einreichen und das Prüfungsentgelt bezahlen. Die gesamte Kommunikation im Bewerbungsverfahren erfolgt über das System, das die Kandidatinnen und Kandidaten schrittweise durch das Aufnahmeverfahren führt. CampusCore unterstützt auch das Hochladen von studiengangsspezifischen zusätzlichen Dokumenten und Materialien, die gegebenenfalls im Rahmen der Vorauswahl von der Zulassungskommission gesichtet und bewertet werden. Stellvertretend kann die Dokumentation des Bewerbungsverfahrens statt von der Zulassungskommission auch vom Referat für Studienangelegenheiten der khb übernommen werden.

An die Auswahl der zukünftigen Studierenden schließt sich das Zulassungsverfahren an, in dem bereits eingegebene Daten übernommen werden. Die Bewerber_innen werden aufgefordert, statistische Angaben im Bewerber_innenportal zu ergänzen und erhalten einen Termin zur Einschreibung. Sämtliche Bewerbungen sind ein Jahr im System aktiv, danach können sie manuell archiviert werden, wobei sensible personenbezogene Daten gelöscht und die verbleibenden Daten anonymisiert werden. Die Bewerbungen werden für vier Jahre archiviert.
Die ausgewählten Bewerber_innen werden vom Referat für Studienangelegenheiten immatrikuliert, sobald diese ihre Einschreibgebühren gezahlt und eventuelle Auflagen erfüllt haben. Die neuen Studierenden erhalten eine Matrikelnummer und beginnen damit offiziell ihr Studium an der khb.

Studienverlauf

Der gesamte Studienverlauf von der Immatrikulation bis zur Exmatrikulation wird in CampusCore abgebildet. Unterstützt werden alle Prozesse im Rahmen des Studiums wie Rückmeldung, Beurlaubung, Studien- bzw. Fachrichtungswechsel und Studienabschluss. Eine Schnittstelle zum ServiceCenter Haushalt ermöglicht die Gebührenverwaltung mit CampusCore. Mit der Exmatrikulation werden die Rechte der Studierenden im CMS eingeschränkt und die Abschlussdaten für das Statistische Landesamt erhoben.

Prüfungs- und Leistungsverwaltung

Alle im Studium erworbenen Leistungen werden in CampusCore dokumentiert. Die Leistungserfassung wird an der khb sowohl vorrangig durch die Lehrenden erfolgen, die dann über das System die Noten einpflegen, als auch in Ausnahmefällen stellvertretend über das Referat für Studienangelegenheiten. Bestehende Noten können nur durch das Referat für Studienangelegenheiten geändert werden. Die Notenberechnung erfolgt nach den in der Prüfungsordnung hinterlegten Regeln über das System. Studierende können jederzeit Einsicht in ihre eigenen Leistungen nehmen. Lehrende haben Zugriffsrechte auf die Leistungsdaten ihrer jeweiligen Studierenden und können über das Campusmanagementsystem auch Dokumente und Informationen zu den Lehrveranstaltungen bereitstellen.

Studiendokumentationen, Leistungs-, Teilnahme- und Studienbescheinigungen sind für die Studierenden zu jedem Zeitpunkt über das System abrufbar. CampusCore unterstützt auch die Ausgabe von Zeugnissen und Urkunden inklusive der Berechnung der Studienabschlussnote. Das Referat für Studienangelegenheiten erstellt die Abschlussdokumente über das System und übermittelt die Prüfungsstatistik an das Statistische Landesamt.

Veranstaltungsplanung

Im Rahmen der Lehrveranstaltungsplanung werden Teilnehmer_innen von Lehr- und anderen Veranstaltungen mit ihrem Namen und ihrer jeweiligen Rolle im Zeit- und Raumplanungstool ASIMUT erfasst, damit individuelle Gruppen-Zeitpläne erstellt werden können. So können Termine für alle Hochschulmitglieder und Lehrbeauftragte verwaltet werden. Die Raum- und Stundenplanung erfolgt auf Grundlage der Personendaten, die in CampusCore hinterlegt sind. ASIMUT unterscheidet zwei verschiedene Ebenen: Die öffentliche Benutzeroberfläche steht allen angemeldeten Nutzern des Systems zur Verfügung und erlaubt Einsicht in den persönlichen Zeitplan sowie in die Tagesansicht aller Veranstaltungen des nach Räumen gruppierten Stundenplans. Auf dieser Ebene können auch Reservierungsanfragen für Sondertermine, z,B. Studienabschlusspräsentationen gestellt werden. Nutzer_innen mit Administrator_innenrechten haben darüber hinaus Zugang zum geschlossenen Planungsbereich, innerhalb dessen auch die Logaktivitäten der Nutzer_innen eingesehen, Buchungsquoten festgelegt und Personendaten verwaltet werden können.

Die Namen der Organisator_innen und Lehrenden sowie ihre jeweilige Rolle in der Veranstaltung sind in der Regel für alle berechtigten Nutzer_innen des Systems sichtbar.
Die Sichtbarkeit der Namen der Teilnehmer_innen einer Veranstaltung, insbesondere teilnehmender Studierender, bleibt hingegen eingeschränkt auf den für die jeweilige Veranstaltung angemeldeten Personenkreis.
Bei Notwendigkeit können die Sichtrechte öffentlicher Nutzer_innen hinsichtlich der Teilnehmer_innen-Namen oder der Veranstaltungsdetails weiter eingeschränkt werden.
Die spezifischen Sichtrechte werden im Rollen- und Rechtemanagement definiert.

Art der Verarbeitung / Software:

Die eingegebenen personenbezogenen Daten werden mittels der Software im Rahmen des Campus-Management-Systems der CampusCore – Software für Hochschulen GmbH & Co. KG, im Folgenden kurz mit CampusCore bezeichnet, verarbeitet und gespeichert. Die Verarbeitung und die Speicherung der Daten erfolgt auf DV-Systemen der CampusCore, die in Dortmund, Deutschland, betrieben werden.

Fachlich Verantwortlich:

Fachlich verantwortlich ist die weißensee kunsthochschule berlin.

IT-Verantwortliche Person / Abteilung:

Verantwortlich aus Sicht der IT ist das ServiceCenter-IT, als untergeordnete Stelle der weißensee kunsthochschule berlin.

Verantwortliche Stelle

Weißensee kunsthochschule berlin
Bühringstr. 20
13086 Berlin

Die weißensee kunsthochschule berlin ist gemäß § 1 Berliner Hochschulgesetz eine staatliche Kunsthochschule und eine rechtsfähige Körperschaft des öffentlichen Rechts sowie zugleich eine staatliche Einrichtung gemäß § 2 Berliner Hochschulgesetz. Aufsichtsbehörde ist:
Der Regierende Bürgermeister von Berlin
Senatskanzlei – Wissenschaft und Forschung

Gesetzlich vertreten wird die weißensee kunsthochschule berlin von ihrer Rektorin, Leonie Baumann.

Hochschulleitung

Hochschulleitung:

Leonie Baumann, Rektorin
Prof. Wim Westerveld, Prorektor (bis 31.03.2017) / Prof. Dr. Jörg Petruschat (ab 01.04.2017)
Prof. Hannes Brunner, Prorektor (bis 31.03.2017) / Prof. Christiane Sauer (ab 01.04.2017)
Silvia Durin, Kanzlerin

IT-Leitung:

ServiceCenter IT

Anschrift Verantwortliche Stelle

Weißensee kunsthochschule berlin
Bühringstr. 20
13086 Berlin

Zweckbestimmung der Datenverarbeitung

Verfahren	Zweckbestimmung	Rechtsgrundlage
Bewerbung und Zulassung	• Kommunikation mit den Bewerber_innen, • Bewertung der Zugangsvoraussetzungen, • Durchführung der Vorauswahl / Eignungsprüfungen • Zulassungen zum Studium	Zulassungsordnungen der khb, §5 Kunsthochschulzugangs-verordnung
Studienverlauf	• Immatrikulation • Rückmeldung • Exmatrikulation • Erfüllung von Berichtspflichten: Studienverlaufsstatistik, Studierenden- und Prüfungsstatistik, Absolvent_innenstatistik • hochschulinterne statistische Auswertungen • Evaluationen • Datenaustausch mit dem Servicecenter Haushalt • Gebührenverwaltung	§ 6 BerlHG, StudDatVO, Hochschulstatistikgesetz
Prüfungs- und Leistungsverwaltung	• Leistungsdokumentation • Bereitstellen von Studien- und Leistungsbescheinigungen • Berechnung von Abschlussnoten	§§ 33ff BerlHG, Rahmenstudien- und Prüfungsordnung der khb

	• Erstellung der Studienabschluss-dokumente	
Veranstaltungsplanung	• Stunden- und Raumplanung, • Kollisionsprüfungen innerhalb der Veranstaltungsplanung	

Betroffene Personengruppen, Daten oder Datenkategorien

Kreis der betroffenen Personengruppen

Bewerber_innen sowie Studierende der khb
Mitarbeiter_innen der Hochschulverwaltung
Lehrende der khb
Servicecenter Haushalt
Sicherheitsbeauftragter der khb

Art der gespeicherten Daten/Datenkategorien

Allgemeine Daten von Studierenden (= Stammdaten inkl. Adressen und Hochschul-Organisation)

Foto
Vorname
Nachname
Namenszusatz
Weitere Vornamen
Geburtsname
Geburtsdatum
Geburtsort
Geburtsland
Staatsangehörigkeiten
Anrede
Geschlecht
Heimatwohnsitz
Semesterwohnsitz
Telefonnummern
Emailadresse
Abschluss einer Krankenversicherung/ Kennziffer der Krankenversicherung

Fachgebiete

Zugangsdaten

Benutzername
Passwort
gesperrt
aktiviert

Gruppen

Attribute sind nicht relevant, nur die Zuordnung ist als personenbezogene Information zu werten.

Rollen

Attribute sind nicht relevant, nur die Zuordnung ist als personenbezogene Information zu werten.

Allgemeine Studieninformationen, berufspraktische Tätigkeit vor dem Studium

Matrikelnummer
Start-Hochschulsemester
Haupt-Hochschule
Hörer_innenstatus
Befreiung vom Semesterticket
Grund für die Befreiung vom Semesterticket
Begründung für die Befreiung vom Semesterticket
Berufsausbildung mit Abschluss
Praktikum oder Volontariat im Hinblick auf das derzeitige Studium

Schulische Ausbildung (HZB und Daten, die für Studierende erhoben werden)

Hochschulzugangsberechtigung
Art der Hochschulzugangsberechtigung
Name der Hochschulzugangsberechtigung
Datum
Land
Region
Verwaltungsbezirk
Kommentar

Studienbuch

khb-Matrikelnummer
erfolgreich abgeschlossene Module
ohne Erfolg besuchte Module
Anzahl der im Studium (bisher) erworbenen LP
Anzahl der Wiederholungsprüfungen
Noten für Modulprüfungen
Themen von Studien-Abschlussprojekten und –arbeiten
Mentor_innen für Studien-Abschlussprojekte

Statistik

Immatrikulation

Ersteinschreibung in Deutschland
Hochschule
Semester

Hochschulsemester
Urlaubssemester
Praxissemester
Semester am Studienkolleg
Einschreibung an einer anderen Hochschule -> Studieninformationen

Studium im vorhergehenden Semester (vor Immatrikulation)

Allgemeine Informationen
Hochschulkontext
Erster Studiengang -> Studieninformationen
Zweiter Studiengang -> Studieninformationen

Auslandsaufenthalte

Erstes Land
Monate
Zweites Land
Monate
Ab SoSe 2017: je Gradierter_n max 3 studienbezogene Auslandsaufenthalte:
Land des Auslandsaufenthaltes
Dauer
Art des Auslandsaufenthaltes
Art des Mobilitätsprogramms
Im Ausland erworbene anerkannte ECTS

bereits abgelegte Abschlussprüfungen

Letzte Prüfung -> Studieninformationen
Datum
Prüfungsergebnis
Gesamtnote
Vorletzte Prüfung -> Studieninformationen
Datum
Prüfungsergebnis
Gesamtnote

Studieninformationen

Hochschule

Land
Region
Verwaltungsbezirk
Abschlussprüfung
Erstes Studienfach
Zweites Studienfach
Drittes Studienfach

Exmatrikulation

- Geschlecht
- Geburtsdatum
- Matrikelnummer
- Staatsangehörigkeit(en)
- abgelegte Abschlussprüfungen
- Exmatrikulationsgrund
- Anzahl der Fachsemester
- Art der Prüfung
- Studienfach
- Monat / Jahr des Prüfungsabschlusses
- Prüfungsergebnis
- Freiversuche
- Gesamtnote

Veranstaltungsplanung: öffentliche Nutzeroberfläche

- Name
- Studiengang
- Art der Veranstaltung
- Zeitraum der Veranstaltung
- Ort der Veranstaltung
- Rolle des Teilnehmers / der Teilnehmerin in der Veranstaltung

Veranstaltungsplanung: Administratorebene

zusätzlich zu den Daten, die über die öffentliche Nutzeroberfläche eingesehen werden können, sind auf der Administratorebene folgende Merkmale einsehbar:

- Nutzername
- Emailadresse
- Privilegien im System
- eventuelle Buchungsquoten

- Angehörigkeit zu Personengruppen im System
- Protokolldatei der einzelnen Veranstaltungen

Die Regelungen zur Erhebung, Speicherung und Nutzung der Studierendendaten gründen auf:

- § 6 des Berliner Hochschulgesetzes (BerlHG) in der Fassung vom 26.07.2011
- die Berliner Studierendendatenverordnung (StudDatVO) in der Fassung vom 09.11.2005
- Anlage zu § 1 Nummer 28 StudDAtVO.

Adressat_innen

Die Empfänger_innen oder Kategorien von Personen, denen die Daten mitgeteilt werden können, werden im Folgenden benannt.

Die Sichtrechte und Bearbeitungsrechte werden unter Wahrung aller datenschutzrechtlichen Vorgaben im Rollen- und Rechtemanagement definiert, mit dem Datenschutzbeauftragen zusätzlich abgestimmt und in einem Rollen und Rechte-Katalog dokumentiert.

Interne Adressat_innen innerhalb der Hochschule

CMS-Beauftragte
Mitarbeiter_innen des Referats für Studienangelegenheiten
Mitarbeiter_innen der Fachbebietsverwaltungen
Angehörige der Zulassungskommissionen
Mitarbeiter_innen des ServiceCenter Haushalt
Mitarbeiter_innen der Steuerungsdienste Haushalt und Personal
Mitarbeiter_innen der Bibliothek und Technikleihe/Setup
Lehrende der khb
Studierende

Externe Adressat_innen und Dritte

Bewerber_innen
Statistisches Landesamt
Senatskanzlei – Wissenschaft und Forschung
Statistisches Bundesamt

Regelfristen für die Löschung der Daten

Welche fristabhängige Löschung vorgesehen?

Die Bestimmungen zur Löschung von personenbezogenen Daten ergeben sich aus § 6 a des Berliner Hochschulgesetzes (BerlHG) in der Fassung vom 26.07.2011, sowie aus § 4 der Berliner Studierendendatenverordnung (StudDatVO) in der Fassung vom 09.11.2005.

In CampusCore haben nur Personen mit der Rolle „Administrator_in“ das Recht, Daten zu löschen. Sowohl die Löschung als auch die Anonymisierung der Daten kann massenweise über eine Aufgabenzuweisung von berechtigten Personen erfolgen. Ein automatisiertes Verfahren ist nicht vorgesehen.

Auskunftserteilung

Auskünfte zu den Daten gibt das Referat für Studienangelegenheiten bzw. das Berichtswesen

Geplante Datenübermittlung

Geplante Datenübermittlung in Drittstaaten: (außerhalb der EU)

Keine

Drittstaaten

Keine

Rechtsgrundlage bei Datentransfer in unsichere Drittländer

Keine

Name und Anschrift der Empfänger_innen

Keine

Beurteilung der Angemessenheit technischer und organisatorischer Maßnahmen

Die personenbezogenen Daten werden von der CampusCore, im Folgenden auch Auftragnehmer genannt, auf eigenen DV-Systemen bearbeitet und gespeichert. Der Betrieb findet im Rechenzentrum der ingenit GmbH & Co. KG, im folgenden auch Subunternehmer genannt, statt.

Zutrittskontrolle

Unbefugten wird der Zutritt zu den Datenverarbeitungsanlagen (DV-Systeme), mit denen die personenbezogenen Daten verarbeitet und genutzt werden, verwehrt. Der Zutritt zu den Räumlichkeiten mit den DV-Systemen ist über eine 6-stiftige geschützte Schließanlage über Profilzylinder mit Sicherungskarte gesichert und ist nur autorisierten Personen mit einem entsprechenden Schlüssel möglich.

Die Räumlichkeiten befinden sich im Technologiezentrum Dortmund. Zutritt haben (Stand 10.12.2015):
Mitarbeiter_innen des Auftragnehmers
Mitarbeiter_innen des Subauftragnehmers, beschränkt auf die Personengruppe der Administrator_innen,
Mitarbeiter_innen des Technologiezentrums, beschränkt auf die Personengruppe der Haustechnik, die Feuerwehr Dortmund (im Fall der Alarmierung durch die Feuerlöschanlage oder zur Begehung), sowie der Wachschutz des Technologiezentrums.

Zugangskontrolle

Es wird verhindert, dass die DV-Systeme von Unbefugten genutzt werden können, denn eine direkte Anmeldung an der Konsole der DV-Systeme ist nur mit entsprechenden Zugangsdaten möglich und erfordert Zutritt zu den Räumlichkeiten nach 1. Zutrittskontrolle. Allein die Mitarbeiter_innen des Auftragnehmers sowie die Administrator_innen des Subauftragnehmers haben Zutritt zu den Räumlichkeiten und besitzen die Zugangsdaten zu den DV-Systemen. Dem restlichen Personenkreis nach 1. Zutrittskontrolle sind die notwendigen Zugangsdaten zu den DV-Systemen nicht bekannt und ihnen ist ein wie auch immer gearteter Zugang zu den DV-Systemen untersagt.
Das Passwort für den Login an den DV-Systemen über die Konsole oder über den SSH-Zugang unterliegt keiner regelmäßigen Änderung. Jedoch ist eine Passwortrichtlinie vorhanden, die auch technisch erzwungen wird, nach der die Passwörter mindestens 15 Zeichen lang sein müssen und mindestens aus Ziffern, Kleinbuchstaben, Großbuchstaben und zwei Sonderzeichen bestehen müssen.
Passwörter der Dienste-Logins (u. a. MySQL) unterliegen keiner regelmäßigen Änderung und keiner technisch erzwungenen Passwortrichtlinie. Organisatorisch ist jedoch vorgegeben, dass die Passwörter für die Dienste ebenfalls nach der obigen Passwortrichtlinie manuell generiert werden.

Der elektronische Zugang zu den DV-Systemen über Netzwerk ist durch Firewall-Technologie geschützt. Die Firewall besteht in einem separaten vorgeschalteten Paketfilter, der lediglich Pakete für die Ports für HTTP (80) und HTTPS (443) sowie für den SSH Zugang (Port xxxxx - lediglich für die

feste IP des CampusCore-Administrationsnetzes a.b.c.d2) passieren lässt. Diese Regeln gelten sowohl von außen (Internet) als auch von innen (DMZ). Zusätzlich sind auf den DV-Systemen Paketfilter installiert, die ebenfalls nur Pakete für die Ports HTTP, HTTPS und SSH (eingeschränkt auf die feste IP des CampusCore-Administrationsnetzes) passieren lassen, und ebenfalls von außen (DMZ) und innen (das jeweilige DV-System).

Zugangsdaten zu den DV-Systemen sind nur Administrator_innen des Auftraggebers und des Auftragnehmers bekannt. Zugangsdaten zur Administration des vorgeschalteten Paketfilters sind nur den Administrator_innen des Auftragnehmers bekannt.

Zugriffskontrolle

Der Auftragnehmer und der Subauftragnehmer führen ausschließlich Tätigkeiten durch, die im Gegenstand des Auftrags beschrieben sind. Der Auftragnehmer verfügt über die zu diesem Zweck notwendige Berechtigungen in den DV-Systemen. Zu diesem Zweck nicht notwendige Berechtigungen (z.B. Datenbankpassworte, Zugangsdaten zur Applikation an sich, etc.) erhält der Auftragnehmer nicht.
Für Berechtigungskonzepte und die Ausgestaltung der Zugriffskontrolle von auf den DV-Systemen durch den Auftragnehmer betriebenen Diensten und Applikationen ist ausschließlich der Auftragnehmer verantwortlich. Dem Subauftragnehmer ist ein Zugriff auf derartige Dienste untersagt.

Weitergabekontrolle

Der Auftragnehmer und der Subauftragnehmer können in der Ausübung ihrer Tätigkeit gemäß dem Gegenstand des Auftrags mit auf den DV-Systemen hinterlegten personenbezogenen Daten in Kontakt kommen. Daher ist es dem Auftragnehmer und insbesondere dem Subauftragnehmer untersagt, seine ihm eingeräumten Berechtigungen auf den DV-Systemen missbräuchlich zu verwenden, um in den Besitz von personenbezogenen Daten zu gelangen.
Für die Realisierung der Weitergabekontrolle in Bezug auf die auf den DV-Systemen vom Auftragnehmer betriebenen Dienste und Applikationen ist ausschließlich der Auftragnehmer verantwortlich.

Eingabekontrolle

Für die Realisierung der Eingabekontrolle in Bezug auf die auf den DV-Systemen vom Auftragnehmer betriebenen Dienste und Applikationen ist ausschließlich der Auftragnehmer verantwortlich. Der Zugriff auf derartige Dienste und Applikationen ist dem Subauftragnehmer untersagt.

Auftragskontrolle

Der Auftragnehmer und der Subauftragnehmer führen ausschließlich Tätigkeiten durch, die im Gegenstand des Auftrags beschrieben sind. Die Tätigkeiten des Subauftragnehmers, bei denen Zugriff auf die DV-Systeme erfolgt, beschränken sich auf die im Gegenstand des Auftrags mit dem Subauftragnehmer genannten Komponenten, in diesem Fall auf die Softwarekomponenten des Betriebssystems. Der Subauftraggeber ist für von ihm auf den DV-Systemen betriebene Dienste und Applikationen selbst verantwortlich.

Verfügbarkeitskontrolle

Die Hardware der DV-Systeme stellt der Auftragnehmer zur Verfügung und ist für die verwendeten Maßnahmen gegen zufällige Zerstörung in Bezug auf die Hardware der DV-Systeme selbst verantwortlich (z.B. Festplatten-RAID).

Der Subauftragnehmer stellt eine unterbrechungsfreie Stromversorgung für das Gerät zur Verfügung. Des Weiteren erstellt der Subauftragnehmer laut dem Gegenstand des Auftrags eine nächtliche Sicherung der DV-Systeme, welche verschlüsselt abgelegt wird. Das Verschlüsselungsverfahren ist ein asymmetrisches Verfahren nach Stand der Technik. Dem Subauftragnehmer wird lediglich der öffentliche Schlüssel zur Kenntnis gebracht, der für die Erstellung der Sicherung benötigt wird. Der zur Wiederherstellung der Datensicherung notwendige private Schlüssel wird vom Auftragnehmer erzeugt und ist nur ihm bekannt. Für den Fall, dass gesicherte Daten auf die DV-Systeme zurückgespielt werden müssen, fordert der Subauftragnehmer den privaten Schlüssel beim Auftragnehmer an und setzt diesen ein. Der Auftragnehmer erstellt innerhalb von 3 Werktagen, beginnend nach vollständiger Wiederherstellung der DV-Systeme, ein neues Schlüsselpaar, mit dem, wie oben beschrieben verfahren wird.

Die täglich durchgeführte Sicherung wird nach folgender Methode durchgeführt: Es wird monatlich eine vollständige, wöchentlich eine differenzielle und täglich eine inkrementelle Sicherungskopie auf einen Festplatten-RAID-5-System auf einen eigenen Backupserver erstellt, der in einem anderen Brandabschnitt liegt als die DV-Systeme. Bei der vollständigen Sicherung werden alle relevanten Daten des Systems gesichert. Bei einer differenziellen Sicherung werden alle Daten, die sich seit dem letzten Vollbackup geändert haben, gesichert und bei einer inkrementellen Sicherung werden alle Daten, die sich gegenüber der letzten Sicherung geändert haben, gesichert. Die täglichen Sicherungsdatensätze werden über 62 Tage vorgehalten und dann automatisch durch ein Programm gelöscht.

Trennungsgebot

Für die Realisierung der Trennungskontrolle in Bezug auf die auf den DV-Systemen vom Auftragnehmer betriebenen Dienste und Applikationen ist ausschließlich der Auftragnehmer verantwortlich. Der Zugriff auf derartige Dienste und Applikationen ist dem Subauftragnehmer untersagt.

Stellungnahme der Datenschutzbeauftragten

Datum der Dokumentation

Dieses Verfahrensverzeichnis wurde am 27.02.2017 erstellt und beruht auf der Vorlage des Datenschutzbeauftragten vom dd.mm.2017.

Bestehender Handlungsbedarf

Es besteht kein Handlungsbedarf.

Freigabe durch die Datenschutzbeauftragte

Gemäß der datenschutzrechtlichen Bestimmungen nach dem Bundesdatenschutzgesetz (BDGS), dem Berliner Datenschutzgesetz (BlnDSG), dem Berliner Hochschulgesetz (BerlHG) und der Berliner Studierendendatenverordnung (StudDatVO) wurde die Sammlung, Verarbeitung und Speicherung der in diesem Verfahrensverzeichnis genannten personenbezogenen Daten geprüft.

Das Verfahren zur Verarbeitung der in diesem Verfahrensverzeichnis beschriebenen personenbezogenen Daten wird durch die_den zuständige_n Datenschutzbeauftragte_n der khb abgenommen.

Alle späteren Erweiterungen des Campusmanagementsystems CampusCore sowie Änderungen und Ergänzungen im Rollen- und Rechtemanagement bedürfen einer Ergänzung dieses Verfahrensverzeichnisses und der nochmaligen Abnahme desselben durch den Datenschutzbeauftragten.

Berlin, Dienstag, 11. April 2017

gez. Gunter Eisermann

_____

Datenschutzbeauftragter Gunter Eisermann