NR. 23| 2016 21. JULI 2016

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

AMTLICHE BEKANNTMACHUNGEN

DER HEINRICH-HEINE-UNIVERSITÄT DÜSSELDORF

INHALT SEITE

HERAUSGEBER
Die Rektorin der Heinrich-Heine-Universität Düsseldorf
Universitätsstraße 1 · 40225 Düsseldorf · www.hhu.de

REDAKTION
Stabsstelle Justitiariat · Gebäude 16.11
Telefon 0211 81-11518 · justitiariat@hhu.de

IT- BENUTZUNGSORDNUNG DER HEINRICH-HEINE-UNIVERSITÄT DÜSSELDORF VOM 28.06.2016

Präambel

Diese Benutzungsordnung soll die störungsfreie, ungehinderte und sichere Nutzung der informationsverarbeitenden Infrastruktur der Heinrich-Heine-Universität Düsseldorf (HHU) gewährleisten. Die Benutzungsordnung orientiert sich an den gesetzlich festgelegten Aufgaben der HHU sowie an ihrem Mandat zur Wahrung der akademischen Freiheit. Sie stellt Grundregeln für den ordnungsgemäßen Betrieb der informationsverarbeitenden Infrastruktur auf und regelt so das Nutzungsverhältnis zwischen den einzelnen Nutzerinnen und Nutzern sowie der HHU.

Die Steuerungs- und Kommunikationsstruktur für den Bereich der digitalen Informationsversorgung und -verarbeitung, der digitalen Kommunikation und zum Einsatz digitaler Medien ist im IKM-Versorgungskonzept der HHU festgelegt.

Begriffsdefinitionen

Alumni sind ehemalige Mitglieder der HHU, die sich verpflichten, der HHU weiter zum Zweck der Förderung von Forschung und Lehre verbunden zu bleiben.

Authentifizierung ist der eindeutige Nachweis einer von der Benutzerin bzw. vom Benutzer behaupteten Identität. Die Feststellung dieser Identität erfolgt weitestgehend quellsystemübergreifend (i.S.v. Single Sign-On).

Authentifizierungsmedien dienen der Authentifizierung einer elektronischen Identität, in der Regel sind dies Passwörter, es können aber auch modernere Medien sein wie Smartcards.

Autorisierung ist die Überprüfung von Zugriffsrechten auf Dienste und Daten.

Benutzerdaten sind Daten, die die Authentifizierung einer Benutzerin bzw. eines Benutzers erlauben oder für die Provisionierung und Autorisierung der Benutzerin bzw. des Benutzers für Dienste und Daten erforderlich sind.

Provisionierung ist die Weitergabe bestimmter Benutzerdaten an andere Systeme zur Bereitstellung von Zugriffsrechten auf Dienste und Daten, die eine Benutzerin bzw. ein Benutzer benötigt.

Systempasswörter sind Passwörter, die keiner Benutzerin bzw. keinem Benutzer direkt zugeordnet sind, sondern zur Sicherstellung des Betriebs der Kommunikationssysteme und Datenverarbeitungsanlagen dienen. Sie sind mit erheblichen Rechten versehen.

§ 1
Geltungsbereich

Diese Benutzungsordnung gilt für die Nutzung der informationsverarbeitenden Infrastruktur der Heinrich-Heine-Universität Düsseldorf, bestehend aus den Datenverarbeitungsanlagen, Kommunikationssystemen und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung.

§ 2
Rechtsstellung und Organisation des Zentrums für Informations- und Medientechnologie (ZIM)

Das ZIM ist eine zentrale Betriebseinheit der HHU im Sinne von § 29 (2) Hochschulgesetz NRW. Es unterstützt die Universität bei der Durchführung von Datenverarbeitungsaufgaben und bei der rechnergestützten Informationsverarbeitung. Im Rahmen von Kooperationsvereinbarungen kann das ZIM auch Aufgaben für Dritte wahrnehmen. Das ZIM wird durch eine Direktorin bzw. einen Direktor geleitet.

§ 3
IT-Versorgung der Heinrich-Heine-Universität Düsseldorf

Die Aufgaben des ZIM und anderer Bereiche der HHU bei der IT-Versorgung der Universität sind im IKM-Versorgungskonzept beschrieben.

Für die Integration, Koordination und Kontrolle aller Aktivitäten in den Bereichen Informationsversorgung, Informationsverarbeitung und Kommunikation sowie des Einsatzes neuer Medien an der HHU hat das Rektorat die bzw. den Chief Information Officer (CIO) beauftragt.

§ 4
Nutzungsberechtigung und Zulassung zur Nutzung

(1) Zur Nutzung der Dienste des ZIM werden zugelassen

1. Mitglieder und Einrichtungen der HHU;

2. Sonstige Beauftragte der HHU;
3. Lehrbeauftragte der HHU, sofern sie nicht bereits unter Nr. 1. erfasst sind;
4. Gast- und Zweithörer der HHU;
5. das Studentenwerk Düsseldorf;
6. Mitglieder und Angehörige anderer Universitäten und wissenschaftlicher Einrichtungen, sofern sie Kooperationspartner von Mitgliedern der HHU sind und die Nutzungsberechtigung für die Kooperation notwendig ist, für einen befristeten Zeitraum;
7. Personen, die nicht zu dem unter Nr. 1. – 6. aufgeführten Kreis gehören, aber temporär die IT-Dienste der HHU zur Erfüllung ihrer Aufgaben für die HHU nutzen müssen, wie z.B. Mitarbeiterinnen und Mitarbeiter externer Firmen zur Abwicklung von Aufträgen und Projekten der HHU oder nichtwissenschaftliche Mitarbeiterinnen und Mitarbeiter des Universitätsklinikums Düsseldorf (UKD) zur Unterstützung von Lehre und Forschung. Der Zugang erfolgt im Rahmen der datenschutzrechtlichen Regelungen und ist befristet.

(2) Die Zulassung erfolgt ausschließlich zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, zu Zwecken der Informationsversorgung und der Verwaltung, zur Aus- und Weiterbildung sowie zur Erfüllung sonstiger Aufgaben der HHU. Eine hiervon abweichende Nutzung kann zugelassen werden, sofern die Zweckbestimmung des ZIM sowie die Belange der anderen Nutzerinnen und Nutzer nicht beeinträchtigt werden.

(3) Nutzerinnen und Nutzern gemäß § 4 (1) wird automatisch eine Zulassung erteilt, falls es technische Verfahren gibt, die dies unterstützen; anderenfalls erfolgt die Zulassung über eine entsprechende Schnittstelle durch die verantwortlichen Einrichtungen der HHU.

(4) Die Nutzerinnen und Nutzer bilden eine geschlossene Nutzungsgruppe.

(5) Für Alumni (s. §6) und für die registrierten Nutzerinnen und Nutzer der Universitäts- und Landesbibliothek (ULB), die nicht zu den unter (1) 1 - 6 genannten Personenkreisen gehören, ist die Nutzung der Dienste des ZIM eingeschränkt.

§ 5
Elektronische Identität der Nutzerinnen und Nutzer

(1) Zur effektiven und sicheren Nutzung der IT-Dienste der HHU wird ein einheitliches Identitätsmanagement im Rahmen eines Identitymanagementsystems (IDM) vom ZIM betrieben. Die Errichtung und der Betrieb des IDM sind ausschließlich zum Zweck der zentralen Verwaltung von Benutzerdaten für die Authentifizierung, Provisionierung und Autorisierung für alle Einrichtungen der HHU zugelassen.

(2) Die Stammdaten der im IDM verwalteten Benutzerinnen und Benutzer werden aus den Daten-führenden Systemen importiert. Die folgenden Daten-führenden Systeme sind an das IDM angebunden:

1. Personalverwaltungen für die Mitglieder der HHU (Namensinformation, Geburtsdatum, interne Personalnummer, Kostenstelle der Beschäftigungsstelle, Art des Dienst- und Beschäftigungsverhältnisses, Anfangsdatum und – falls vorhanden – Enddatum des Dienst- und Beschäftigungsverhältnisses, Telefonnummer, E-Mail-Adresse, Raumnummer),

2. Studierendenverwaltung (Festlegung in der Einschreibungsordnung der HHU),

3. Finanzverwaltung (Zuordnung der Finanzierung (Kostenstelle) zur Organisationseinheit),

4. Bibliothekssystem (für externe Nutzerinnen und Nutzer der Universitäts- und Landesbibliothek: Namensinformation, Geburtsdatum, Nummer und Ablaufdatum des Bibliotheksausweises, Hinweis auf eine Sperre der Ausleihkarte bei nicht bezahlten Gebühren, ggf. der Wunsch für ein Zurücksetzen des Passworts),

5. Telefonie (Telefonnummern und Räume),

6. ZIM-Mail-Directory (E-Mail-Adresse).

Personen, die nicht über die Daten-führenden Systeme importiert werden und gemäß § 4 (1) und (6) zuzulassen sind, werden über eine Gästeschnittstelle durch die verantwortlichen Einrichtungen in das IDM eingepflegt.

(3) Der Betrieb des IDM umfasst den Import von Daten aus den angebundenen führenden Systemen, die interne Verarbeitung von Daten und die definierte Übermittlung von Daten an die angebundenen Zielsysteme. Ein Zielsystem nutzt nur die erforderliche Teilmenge der im IDM verarbeiteten Daten. Die an das Zielsystem übermittelten Daten können auf zwei verschiedene Arten genutzt werden:

1. Authentifizierung und Autorisierung der Benutzerin bzw. des Benutzers,

2. Abfrage der zentralen Informationen zur Synchronisation der Benutzerdaten.

(4) Verantwortliche Stelle für den ordnungsgemäßen Betrieb ist das ZIM.

(5) Grundsätzlich sind nur die in § 5 Abs. 2 festgelegten Stammdaten aus den in § 5 Abs. 2 aufgeführten Quellsystemen zur Verarbeitung im IDM zugelassen. Übermittlungen personenbezogener Daten vom IDM an die Zielsysteme sind nur zugelassen, sofern für die Zielsysteme eine entsprechende datenschutzrechtliche Vorabkontrolle durchgeführt worden ist und der Eintrag im Verfahrensverzeichnis der HHU für das IDM entsprechend angepasst wurde.

(6) Im Rahmen des IDM erhält jede Benutzerin und jeder Benutzer eine persönliche passwortgeschützte HHU-Kennung zur Authentifizierung sowie die dienstliche (für Mitarbeiterinnen und Mitarbeiter) bzw. studentische E-Mail-Adresse, in der Regel in der Form vorname.nachname@hhu.de. Dopplungen werden durch neutrale Ergänzungen verhindert.

(7) Es können spezielle E-Mailadressen für den Dienstgebrauch, die keinen Bezug auf den Namen einzelner Personen enthalten, eingerichtet werden (Funktions-E-Mailadressen).

(8) Verarbeitung personenbezogener Daten

1. Im IDM erfolgt die Verarbeitung personenbezogener Daten für die geschlossene Benutzergruppe nach §4.

2. Die Verarbeitung personenbezogener Daten erfolgt im IDM ausschließlich zu den in §4 (3) dieser Ordnung genannten Zwecken.

3. Die im IDM gespeicherten Daten werden nur an Zielsysteme übermittelt, sofern die Übermittlung zum ordnungsgemäßen Betrieb des Zielsystems erforderlich ist und dem in §4 (3) dieser Ordnung genannten Zweck dient.

(9) Zugriffsrechte

Grundlage für die Vergabe der Zugriffsberechtigungen im IDM ist ein mehrstufiges Rechtekonzept. Jede im IDM registrierte Person hat Lesezugriff auf die über sie dort vorhandenen Daten. Zielsystem-Administratorinnen und -Administratoren haben Lesezugriff auf Daten der für ihren Dienst provisionierten IDM-Benutzerinnen und -Benutzer. IDM-Administratorinnen und -Administratoren haben Zugriff auf die Daten aller IDM-Benutzerinnen und -Benutzer.

(10) Selbstadministration
Die Selbstadministration ermöglicht es der Benutzerin bzw. dem Benutzer, ihr bzw. sein informationelles Selbstbestimmungsrecht wahrzunehmen und Einsicht in die über sie bzw. ihn gespeicherten Daten zu nehmen.

(11) Beendigung der Nutzungsberechtigung

1. Die Nutzungsberechtigung wird gesperrt
   - mit der Abmeldung durch den Nutzer bzw. die Nutzerin,
   - mit dem Ablauf einer befristet erteilten Nutzungsberechtigung,
   - wenn mit der Nutzungsberechtigung verbundene Pflichten (§ 7), Bedingungen oder Auflagen nicht erfüllt werden,
   - mit dem Ausscheiden als Mitglieder der HHU drei Monate nach Beendigung des Arbeitsverhältnisses, soweit nichts anderes bestimmt ist,
   - bei Studierenden sechs Monate nach Ausscheiden zur Wahrung von Prüfungsansprüchen,
   - mit dem Tod.
2. Der Nutzer bzw. die Nutzerin wird über die Beendigung der Nutzungsberechtigung elektronisch informiert, sofern sie oder er noch lebt.
3. Nach Ausscheiden einer Nutzerin bzw. eines Nutzers aus der geschlossenen Nutzungsgruppe kann sie bzw. er in den Status einer Alumna bzw. eines Alumnus wechseln (§ 6).
4. Die Löschung der Daten der Benutzerinnen und Benutzer im IDM erfolgt spätestens nach Ablauf von einem Jahr nach der Sperrung der Nutzungsberechtigung (s. 1.).
5. Sofern die Daten für eine Abrechnung der genutzten IT-Dienstleistungen und Ressourcen erforderlich sind, kann die Löschung der Benutzerdaten unterbleiben. Die Speicherung kann für den Zeitraum erfolgen, für den diese Daten zu Zwecken der Rechnungslegung und Rechnungsprüfung erforderlich sind.

§ 6
Alumni

(1) Die Rolle einer Alumna bzw. eines Alumnus umfasst das Führen eines Postfaches mit der E-Mail-Adresse (i.d.R.: vorname.nachname@hhu.de). Auf Antrag kann einer Alumna bzw. einem Alumnus die Nutzung weiterer IT-Einrichtungen der HHU gewährt werden, sofern diese im Interesse der HHU liegt. Diese Nutzung wird zeitlich angemessen befristet.

(2) Die Alumna bzw. der Alumnus muss diese Rolle aktiv alle 2 Jahre nach Aufforderung durch das ZIM verlängern. Unterbleibt die Verlängerung, werden die Kennung und die damit verbundene E-Mail-Adresse gesperrt und nach Ablauf eines Jahres nach der Sperrung endgültig gelöscht.

§ 7
Rechte und Pflichten der Nutzerinnen und Nutzer

(1) Nutzerinnen und Nutzer haben das Recht, die Einrichtungen, Datenverarbeitungsanlagen, Kommunikationssysteme und sonstige Einrichtungen zur rechnergestützten Informationsverarbeitung des ZIM nach Maßgabe dieser Benutzungsordnung zu nutzen. Eine hiervon abweichende Nutzung bedarf einer gesonderten Zulassung.

(2) Die Nutzerinnen und Nutzer sind verpflichtet,

(Allgemein)

1. die Vorgaben der Benutzungsordnung zu beachten und die Grenzen der Nutzungserlaubnis einzuhalten, insbesondere die Nutzungszwecke nach § 4 (3) zu beachten;

2 alles zu unterlassen, was den ordnungsgemäßen Betrieb der Einrichtungen der HHU nach allgemeinem Kenntnisstand stören kann;

3. alle Datenverarbeitungsanlagen, Kommunikationssysteme, Einrichtungen zur rechnergestützten Informationsverarbeitung und sonstigen Einrichtungen des ZIM sorgfältig und schonend zu behandeln;

(Umgang mit Authentifizierungsmedien)

4. ausschließlich mit den Authentifizierungsmedien zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung als Nutzerin oder Nutzer gestattet wurde;

5. dafür Sorge zu tragen, dass keine anderen Personen Kenntnis von bzw. Zugang zu den Authentifizierungsmedien erlangen, sowie Vorkehrungen zu treffen, damit unberechtigten Personen der Zugang zu den Ressourcen des ZIM verwehrt wird; dazu gehört auch der Schutz des Zugangs durch ein geheim zu haltendes und geeignetes, d.h. nicht einfach zu erratendes Passwort;

6. fremde Authentifizierungsmedien weder zu ermitteln noch zu nutzen;

7. keinen unberechtigten Zugriff auf Informationen anderer Nutzerinnen und Nutzer zu nehmen und bekanntgewordene Informationen anderer Nutzerinnen und Nutzer nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern;

(Softwarenutzung, Urheberrechte, Datenschutz)

8. bei der Benutzung von Software, Dokumentationen und anderen Daten die gesetzlichen Vorgaben, insbes. zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten seitens des ZIM zur Verfügung gestellt werden, zu beachten;

9. die vom ZIM bereitgestellten Software-Produkte, Dokumentationen und Daten weder ganz oder teilweise zu kopieren noch an Dritte weiterzugeben, sofern dies nicht ausdrücklich erlaubt ist, noch zu anderen als den erlaubten Zwecken zu nutzen;

10. bei der Benutzung von personenbezogenen Daten die gesetzlichen Vorgaben, insbesondere zum Datenschutz, zu beachten;

(Nutzung der Einrichtungen des ZIM)

11. in den Räumen des ZIM den Weisungen des Personals Folge zu leisten;

12. Störungen, Beschädigungen und Fehler an Datenverarbeitungsanlagen, Kommunikationssystemen, sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung und Datenträgern sowie Diensten des ZIM unverzüglich den Mitarbeiterinnen und Mitarbeitern des ZIM zu melden und sie nicht selbst zu beheben;

13. ohne ausdrückliche Einwilligung des ZIM keine Eingriffe in die Hardwareinstallation der Systeme des ZIM vorzunehmen und die Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Nutzerdateien und des Netzwerks nicht zu verändern;

(Sonstiges)

14. der Direktorin bzw. dem Direktor des ZIM auf Verlangen in begründeten Einzelfällen – insbes. bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung – zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu erteilen sowie Einsicht in die Programme zu gewähren.
    Von dieser Regelung werden nicht die Nutzerdaten erfasst, die durch das Telekommunikationsgeheimnis oder das Datengeheimnis geschützt sind, z.B. E-Mails, persönliche Dateien oder personenbezogene Daten Dritter;

15. eine Verarbeitung personenbezogener Daten mit dem ZIM und vorab mit dem bzw. der Datenschutzbeauftragten der HHU abzustimmen und – unbeschadet der eigenen datenschutzrechtlichen Verpflichtungen des Benutzers bzw. der Benutzerin – die vom ZIM vorgeschlagenen Datenschutz- und Datensicherheitsvorkehrungen zu berücksichtigen.

§ 8
Ausschluss von der Nutzung

(1) Nutzerinnen und Nutzer können vorübergehend oder dauerhaft in der Benutzung der Datenverarbeitungsanlagen, Kommunikationssysteme und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung eingeschränkt oder hiervon ausgeschlossen werden, wenn sie

1. schuldhaft gegen diese Benutzungsordnung, insbesondere gegen die in § 7 aufgeführten Pflichten, verstoßen (missbräuchliches Verhalten) oder

2. diese für strafbare Handlungen missbrauchen oder

3. der Universität durch sonstiges rechtswidriges Nutzungsverhalten Nachteile entstehen.

(2) Maßnahmen nach (1) sollen erst nach einer Abmahnung unter Hinweis auf die sonst eintretenden Folgen ergriffen werden. Bei sehr schwerwiegenden Verstößen ist die Abmahnung im Einzelfall entbehrlich. Der bzw. dem Betroffenen ist Gelegenheit zur Stellungnahme zu geben. Sie bzw. er kann die bzw. den CIO um Vermittlung bitten. In jedem Fall bleibt das Recht an ihren/ seinen Daten unberührt.

(3) Vorübergehende Nutzungseinschränkungen, über die die Direktorin bzw. der Direktor des ZIM entscheidet, sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet erscheint.

(4) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss einer Nutzerin bzw. eines Nutzers von der weiteren Nutzung kommt nur bei schwerwiegenden oder wiederholten Verstößen i.S.v. (1) in Betracht, wenn auch künftig ein ordnungsgemäßes Verhalten nicht mehr zu erwarten ist. Die Entscheidung über einen dauerhaften Ausschluss trifft die Rektorin bzw. der Rektor auf Antrag der Direktorin bzw. des Direktors des ZIM. Mögliche Ansprüche der HHU aus dem Nutzungsverhältnis bleiben unberührt.

(5) Im Falle der Nutzungseinschränkung sind der zuständige Personalrat und weitere Interessensvertretungen zu beteiligen.

§ 9
Rechte und Pflichten des ZIM

(1) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerdaten erforderlich ist, kann das ZIM die Nutzung seiner Ressourcen vorübergehend einschränken oder einzelne Nutzungskennungen vorübergehend sperren. Sofern möglich sind die betroffenen Nutzerinnen und Nutzer hierüber im Voraus zu unterrichten.

(2) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass Nutzerinnen und Nutzer auf den Servern des ZIM rechtswidrige Inhalte zur Nutzung bereithalten, kann das ZIM die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.

(3) Das ZIM ist berechtigt, die Sicherheit der System-/Benutzerpasswörter bei Wahl und Änderung der Passwörter durch automatisierte Maßnahmen zu überprüfen, um zu verhindern, dass durch leicht zu erratende Passwörter die Sicherheit der Datenverarbeitungsanlagen und Benutzerdaten gefährdet werden.

(4) Das ZIM ist nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der Datenverarbeitungsanlagen, Kommunikationssysteme und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung durch die einzelnen Nutzerinnen und Nutzer zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist:

1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
2. zur Ressourcenplanung und Systemadministration,
3. zum Schutz der personenbezogenen Daten anderer Nutzerinnen und Nutzer,
4. zu Abrechnungszwecken,
5. zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

(5) Unter den Voraussetzungen von (4) 1. und 5. ist das ZIM auch berechtigt, unter Beachtung des Datengeheimnisses Einsicht in die Benutzerdateien zu nehmen, soweit dies erforderlich ist zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen, sofern hierfür tatsächliche Anhaltspunkte vorliegen. Eine Einsichtnahme in die Nachrichten- und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist. Die Einsichtnahme ist beschränkt auf Personen, die über die erforderlichen Rechte verfügen (Administratoren) oder die weisungsfrei sind. In jedem Fall ist die Einsichtnahme zu dokumentieren, und die betroffene Nutzerin bzw. der betroffene Nutzer ist nach Zweckerreichung unverzüglich zu benachrichtigen.

(6) Die personenbezogenen Verkehrs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Telediensten, die das ZIM zur Nutzung bereithält oder zu denen das ZIM den Zugang zur Nutzung vermittelt, sind frühestmöglich, spätestens unmittelbar am Ende der jeweiligen Nutzung, zu löschen, soweit es sich nicht um Abrechnungsdaten handelt. Für die zur Abrechnung erforderlichen Daten gelten die Fristen nach der jeweils gültigen Fassung des Telekommunikationsgesetzes bzw. des Telemediengesetzes. Hat die Teilnehmerin bzw. der Teilnehmer gegen die Höhe der in Rechnung ge-

stellten Entgelte vor Ablauf dieser Fristen Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

(7) Nach Maßgabe der gesetzlichen Bestimmungen ist das ZIM zur Wahrung des Telekommunikations- und Datengeheimnisses verpflichtet.

(8) Zu den Rechten und Pflichten des ZIM gehört auch das Ergreifen der gemäß § 8 gebotenen Maßnahmen.

§ 10
Besondere Bestimmungen zur Nutzung von Kommunikationsdiensten

(1) Mit der Zulassung erhalten alle Nutzerinnen und Nutzer eine personenbezogene dienstliche E-Mailadresse der HHU, die nach § 5 (10) ihren Namen enthält. Nachrichten an diese E-Mail-Adresse ersetzen den Postweg. Näheres regelt eine Dienstanweisung.

(2) Außer im Falle des § 9 (5) hat ausschließlich die Nutzerin bzw. der Nutzer Zugang zu seinem bzw. ihrem personenbezogenen Nachrichten- und E-Mail-Postfach. Auch eine Weiterleitung von Nachrichten, die an personenbezogene E-Mailadressen adressiert wurden, darf ausschließlich von der Nutzerin bzw. dem Nutzer veranlasst werden.

(3) Die HHU kann spezielle E-Mailadressen für den Dienstgebrauch, die keinen Bezug auf den Namen einzelner Personen enthalten, einrichten (Funktions-E-Mailadressen). Mit diesen Mailadressen ist ausschließlich die Nutzung zu dienstlichen Zwecken erlaubt. Der Zugriff auf die betreffenden Nachrichten- und E-Mail-Postfächer sowie die Weiterleitung von Nachrichten, die an diese E-Mailadressen adressiert wurden, kann von der Dienststelle festgelegt und jederzeit verändert werden. Ausgenommen hiervon sind die Postfächer der Personalräte, des Datenschutzbeauftragten und der weiteren Interessensvertretungen.

(4) Mitglieder der HHU sind im E-Mailverkehr im Rahmen ihrer Dienstaufgaben zur Nutzung von E-Mailadressen der HHU verpflichtet. Näheres regelt eine Dienstanweisung.

§ 11
Haftung der Nutzerinnen und Nutzer

(1) Nutzerinnen und Nutzer haften für alle Nachteile, die der Universität durch missbräuchliche oder rechtswidrige Verwendung der Datenverarbeitungsanlagen, Kommunikationssysteme, sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung und der Nutzungsberechtigung oder dadurch entstehen, dass die Nutzerin bzw. der Nutzer schuldhaft ihren bzw. seinen Pflichten aus dieser Benutzungsordnung nicht nachkommt.

(2) Nutzerinnen und Nutzer haften auch für Schäden, die im Rahmen der ihnen zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn sie diese Drittnutzung zu vertreten haben, insbesondere im Falle einer Weitergabe einer Nutzungskennung an Dritte.

(3) Nutzerinnen und Nutzer haben die Universität von allen Ansprüchen freizustellen, wenn Dritte die Universität wegen eines missbräuchlichen oder rechtswidrigen Verhaltens der Nutzerin bzw. des Nutzers auf Schadensersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Die Universität wird der Nutzerin bzw. dem Nutzer den Streit verkünden, sofern Dritte aufgrund dieser Ansprüche gegen das ZIM gerichtlich vorgehen.

(4) Für die Mitarbeiterinnen und Mitarbeiter gelten die einschlägigen Vorschriften des Landesbeamtengesetzes und des jeweiligen Tarifvertrages.

§ 12
Haftung der Universität

(1) Die Universität übernimmt keine Garantie dafür, dass die Datenverarbeitungsanlagen, Kommunikationssysteme und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung fehlerfrei und jederzeit ohne Unterbrechung laufen. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.

(2) Die Universität übernimmt keine Verantwortung für die Richtigkeit der zur Verfügung gestellten Programme. Die Universität haftet auch nicht für den Inhalt, insbesondere für die Richtigkeit, Vollständigkeit und Aktualität der Informationen, zu denen sie lediglich den Zugang zur Nutzung vermittelt.

(3) Die Universität haftet gegenüber Dritten nur bei Vorsatz und grober Fahrlässigkeit ihrer Mitarbeiterinnen oder ihrer Mitarbeiter.

(4) Mögliche Amtshaftungsansprüche gegen die Universität bleiben von den vorstehenden Regelungen unberührt.

§ 13
In-Kraft-Treten

Diese Ordnung tritt am Tag nach Ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Heinrich-Heine-Universität Düsseldorf in Kraft. Die Verwaltungs- und Benutzungsordnung für das Universitätsrechenzentrum der Heinrich-Heine-Universität Düsseldorf vom 21. Februar 1995 (Amtliche Bekanntmachungen Nr. 3/1995 vom 07. März 1995) tritt gleichzeitig außer Kraft.

Ausgefertigt aufgrund des Beschlusses des Senats der HHU vom 28.06.2016.

Düsseldorf, den 28.06.2016

Die Rektorin
der Heinrich-Heine-Universität Düsseldorf

Anja Steinbeck
(Univ.-Prof. Dr. iur.)