Musterbenutzungsordnung

Wichtiger Hinweis:

Der Mustertext soll ausschließlich als Formulierungsvorschlag dienen. Eine unveränderte Übernahme ist daher in der Regel nicht möglich. Vielmehr ist der Entwurfstext an die jeweiligen hochschulspezifischen Gegebenheiten anzupassen, wobei insbesondere die Eigenheiten und speziellen Anforderungen der jeweils angebotenen Dienste sowie vertragliche Vereinbarungen mit deren Anbietern beachtet werden müssen, was im Einzelfall separate Ordnungen für einzelne Dienste erforderlich machen kann. Überdies müssen - soweit vorhanden – landesrechtliche Besonderheiten berücksichtigt werden.

Eine Haftung für die Richtigkeit und Vollständigkeit des Mustertextes wird nicht übernommen.

Bei den grau hinterlegten Passagen handelt es sich um Anmerkungen, die nicht Teil des Mustertextes sind.

Ordnung des Hochschulrechenzentrums vom xx.xx.xxxx

Aufgrund des § XX des Landeshochschulgesetzes vom (GVBl. XXXX) hat der Senat der Hochschule XY die folgende Ordnung des Hochschulrechenzentrums [als Satzung] beschlossen:

Die Benennung des Regelungswerks als „Rechenzentrumsordnung", „Nutzungsordnung", „Betriebsordnung", „Netzordnung", „Benutzungsrichtlinien" etc. ist unerheblich. Ob die Benutzungsordnung als „Satzung" oder als förmliche „Ordnung" ergeht, richtet sich nach der jeweiligen landesrechtlichen Ermächtigungsgrundlage. Der Zusatz „als Satzung" dient lediglich der Klarstellung für den Normadressaten, dass die Benutzungsordnung eine allgemeinverbindliche Regelung für alle Nutzer darstellt.

Präambel

Diese Benutzungsordnung soll die möglichst störungsfreie, ungehinderte und sichere Nutzung der Kommunikations- und Datenverarbeitungsinfrastruktur des Hochschulrechenzentrums der Hochschule XY gewährleisten. Die Benutzungsordnung orientiert sich an den gesetzlich festgelegten Aufgaben der Hochschule XY sowie an ihrem Mandat zur Wahrung der akademischen Freiheit. Sie stellt Grundregeln für einen ordnungsgemäßen Betrieb der Informationsverarbeitungsinfrastruktur (IV-Infrastruktur) auf und regelt so das Nutzungsverhältnis zwischen den einzelnen Nutzern und dem Hochschulrechenzentrum.

Einer Präambel kommt in erster Linie die deklaratorische Funktion eines Programmsatzes zu, durch den einerseits der verbindliche Charakter des Regelwerks unterstrichen wird und andererseits die Regelungsziele der Benutzungsordnung vorangestellt werden. Zwar sind für die Ausgestaltung des Nutzungsverhältnisses in erster Linie die konkreteren Einzelregelungen der Benutzungsordnung maßgeblich. Auf eine Präambel sollte dennoch nicht verzichtet werden, da sie im Einzelfall bei Zweifeln über die Auslegung von konkreten Einzelregelungen Bedeutung erlangen kann.

§ 1 Geltungsbereich

Diese Benutzungsordnung gilt für die Nutzung der Informationsverarbeitungsinfrastruktur des Rechenzentrums der Hochschule XY, bestehend aus den Datenverarbeitungsanlagen, Kommunikationssystemen und sonstigen Einrichtungen zur rechnergestützten Informationsverarbeitung, die dem Hochschulrechenzentrum unterstellt sind.

§ 2 Rechtsstellung und Organisation des Hochschulrechenzentrums

(1) Das Rechenzentrum ist eine zentrale Betriebseinheit/Einrichtung der Hochschule XY. Es unterstützt die Hochschule bei der Durchführung von Datenverarbeitungsaufgaben und bei der rechnergestützten Informationsverarbeitung. SOFERN EINSCHLÄGIG: Im Rahmen bestehender Kooperationsvereinbarungen, nimmt das Rechenzentrum seine Aufgaben auch für die Fachhochschule XY sowie für die Kunst- und Musikhochschule XY wahr.

(2) Organisation des Rechenzentrums: Leitung des Rechenzentrums, interne Verwaltungsstruktur (z. B. Stellvertretung, Geschäftsverteilung, Arbeitsgruppen), DV-Kommission etc.

An dieser Stelle können die Organisation, der Aufbau des Rechenzentrums, die Eingliederung des Rechenzentrums in die Hochschule sowie alle sonstigen hochschulspezifischen Besonderheiten der Verwaltung des Rechenzentrums geregelt werden. Etwaige landesrechtliche Vorgaben, wie z. B. zur Einrichtung einer Datenverarbeitungskommission des Senats, sind zu berücksichtigen. Die Rechtsstellung, Organisation und Aufgaben des Rechenzentrums können auch in einem eigenen Abschnitt "Verwaltungsordnung" der Benutzungsordnung oder in einer separaten Verwaltungsordnung geregelt werden. Auf diese sollte ausdrücklich hingewiesen werden, z. B.: „(2) Rechtsstellung, Organisation und Aufgaben des Rechenzentrums ergeben sich aus der Verwaltungs- und Benutzungsordnung für das Hochschulrechenzentrum der Hochschule XY."

§ 3 Aufgaben des Hochschulrechenzentrums

(1) Dem Hochschulrechenzentrum obliegen [in Erfüllung der in § XX LHG zugewiesenen gesetzlichen Aufgaben] insbesondere folgende Aufgaben:

> Soweit dem Rechenzentrum durch das Landeshochschulgesetz bestimmte Aufgaben zugewiesen werden, sind diese bei der Aufgabenbeschreibung zu berücksichtigen. Sofern die Aufgaben des Rechenzentrums bereits in der allgemeinen Hochschulsatzung festgelegt sind, genügt in der Benutzungsordnung ein entsprechender Verweis. Der möglichst genauen Beschreibung der wesentlichen Aufgaben des Hochschulrechenzentrums kommt eine zentrale Bedeutung zu: Durch die exakte Aufgabenbestimmung wird nämlich der sog. "Anstaltszweck" festgelegt, nach dem sich das Nutzungsverhältnis bestimmt. Dies ist wichtig für Maßnahmen, die nicht von einer spezielleren Ermächtigungsgrundlage in der Benutzungsordnung gedeckt sind. Mit der Zweckbestimmung des Hochschulrechenzentrums korrespondieren allgemeine „Ordnungspflichten" der Nutzer, die ggf. auch ohne ausdrückliche Spezialermächtigung in der Benutzungsordnung mit (verhältnismäßigen) inneranstaltlichen Ordnungsmaßnahmen (im Betriebsverhältnis) durchgesetzt werden können. Aus Gründen der Rechtssicherheit sollte jedoch versucht werden, zumindest das „typische" Fehlverhalten der Nutzer in der Benutzungsordnung explizit zu regeln (z. B. bei der Festlegung der Nutzerpflichten durch nicht-abschließende Aufzählungen und Regelbeispiele).[1]

[Beispiele]

> Die nachfolgende Aufgabenbeschreibung soll lediglich als Beispiel dienen und ist ggf. den lokalen Besonderheiten anzupassen.

1. Planung, Realisierung und Betrieb der Datenverarbeitungsanlagen des Rechenzentrums für Aufgaben in Forschung, Lehre, Studium, Verwaltung [und Krankenversorgung].
2. Betreuung der für die Hochschule verfügbaren Datenverarbeitungsressourcen und die betriebsfachliche Aufsicht über alle Datenverarbeitungsanlagen in der Hochschule, soweit dies nicht Aufgabe anderer Organisationseinheiten oder Einrichtungen der Hochschule ist.
3. Koordinierung der Beschaffung von Datenverarbeitungsanlagen in der Hochschule, insbesondere Stellungnahme zu Investitionsmaßnahmen in Datenverarbeitungssysteme, Nutzungsanalyse vorhandener System-Komponenten und Bedarfsplanung.
4. Erwerb, Verwaltung, Dokumentation, Pflege und Weiterentwicklung von Standard- und Grundsoftware, insbesondere Hochschul- und Campuslizenzen sowie Auswahl, Einsatz und Betreuung der in der Hochschulverwaltung eingesetzten Software.
5. Unterweisung, Beratung und Unterstützung der Nutzer.
6. Durchführung von Schulungs- und Fortbildungsmaßnahmen für Angehörige der Hochschule sowie Unterstützung anderer Fachbereiche bei EDV-bezogenen Lehrveranstaltungen.

(2) Das Hochschulrechenzentrum ist überdies für die Planung, Installation und den Betrieb rechnergestützter Informations- und Kommunikationsnetze einschließlich der erforderlichen

[1] Vgl. zum Ganzen auch Gurlit, in: Ehlers/Pünder, Allg. VerwR, § 35 Rn. 33 ff. (S. 788 ff.).

zentralen Server sowie der Datenkommunikations- und Telekommunikationssysteme zuständig. Diesbezüglich obliegen dem Rechenzentrum insbesondere folgende Aufgaben:

Hier sollte eine spezifische Aufgabenbeschreibung vorgenommen werden, die den Gegebenheiten des jeweiligen Hochschulrechenzentrums entspricht.

1. Bereitstellung und Aufrechterhaltung eines möglichst störungsfreien und ununterbrochenen Betriebes des Kommunikationsnetzes.
2. Koordination des Ausbaus und der Wartung des Kommunikationsnetzes.
3. Verwaltung der Adress- und Namensräume.
4. Bereitstellung von Netzwerkdiensten und zentralen Netzwerk-Servern.
5. Unterstützung der Nutzer bei der Anwendung der Dienste.

(3) Zur Gewährleistung eines ordnungsgemäßen Betriebes des Informations- und Kommunikationsnetzes sowie der Datenverarbeitungssysteme, die dem Hochschulrechenzentrum zugeordnet sind, kann der Leiter des Rechenzentrums weitere Regeln für die Nutzung der DV-Anlagen des Hochschulrechenzentrums erlassen, wie z. B. Nutzungsbedingungen für die Nutzung des CIP-Pools, technisch-organisatorische Vorgaben zum Betrieb des Datennetzes oder Betriebsregelungen für Veröffentlichungen auf Servern des Rechenzentrums.

Diese Ermächtigungsgrundlage ermächtigt den Leiter des Rechenzentrums zum Erlass weiterer Detailregelungen über Fragen des Betriebsalltags, die in der Betriebsordnung als grundlegendem Regelungswerk nicht geregelt werden können. Inhaltlich sind hierbei die o.g. Einschränkungen zur Regelungskompetenz zu beachten, d. h. es können ausschließlich Fragen des „Anstaltsalltags" geregelt werden. Überdies müssen sich die nachrangigen Richtlinien am Anstaltszweck orientieren, so dass eine entsprechende Betriebsregelung nur der näheren Ausgestaltung des Anstaltszwecks im Betriebsverhältnis dienen kann.[2] Auch deshalb kann eine möglichst konkrete Beschreibung der Aufgaben des Hochschulrechenzentrums wichtig sein, wobei abstrakte Beschreibungen der Hauptfunktionen ausreichen.

§ 4 Nutzungsberechtigung und Zulassung zur Nutzung

(1) Zur Nutzung der Dienste des Hochschulrechenzentrums können, soweit nicht spezielle Regelungen für einzelne Dienste oder DV-Ressourcen oder vertragliche Verpflichtungen der Hochschule dem entgegenstehen, zugelassen werden

1. Mitglieder, Angehörige und Einrichtungen einschließlich der Verwaltung der XY Universität SOFERN EINSCHLÄGIG: sowie der Fachhochschule XY;
2. Beauftragte der Hochschule zur Erfüllung ihrer Dienstaufgaben;
3. Mitglieder und Angehörige anderer Hochschulen des Landes XY oder staatlicher Hochschulen außerhalb des Landes XY aufgrund besonderer Vereinbarungen;
4. sonstige staatliche Forschungs- und Bildungseinrichtungen und Behörden des Landes XX aufgrund besonderer Vereinbarungen;
5. Studierendenwerke im Land XY.

[2] Vgl. Gurlit, in: Ehlers/Pünder, Allg. VerwR, § 35 Rn. 33 ff. (S. 788 ff.).

Die Hochschule behält sich ausdrücklich vor, den Nutzerkreis allgemein oder begrenzt auf einzelne Dienste einzuschränken. Dies kann insbesondere aufgrund vertraglicher Verpflichtungen der Hochschule beim Bezug einzelner Dienste erfolgen, die eine Beschränkung des Nutzerkreises erforderlich machen.

> Bei den hier angeführten Nutzergruppen handelt es sich nur um Beispiele. Unbedingt zu beachten sind jedoch vertragliche Verpflichtungen der Hochschule, die eine Einschränkung des Nutzerkreises vorsehen. Die Reihenfolge der Nutzungsberechtigten ist von Bedeutung, da diese gemäß § 4 Abs. 8 dieses Entwurfs für die Rangfolge im Rahmen einer Kontingentierung bei Ressourcenmangel ausschlaggebend ist.

(2) Die Zulassung erfolgt ausschließlich zu wissenschaftlichen Zwecken in Forschung, Lehre und Studium, zu Zwecken der Bibliothek und der universitären Verwaltung, zur Aus- und Weiterbildung sowie zur Erfüllung sonstiger Aufgaben der Hochschule XY. Eine hiervon abweichende Nutzung bedarf der ausdrücklichen Zulassung, die erteilt werden kann, wenn die abweichende Nutzung geringfügig ist, sie keinen gesetzlichen oder vertraglichen Verpflichtungen der Hochschule zuwiderläuft und die Zweckbestimmung des Hochschulrechenzentrums sowie die Belange der anderen Nutzer nicht beeinträchtigt werden.

> An dieser Stelle können auch eine kommerzielle Anwendung und die Nutzung der Rechenzentrumsdienste für private Zwecke ausgeschlossen werden. Sofern abweichende Nutzungen, insbesondere eine geringfügige Privatnutzung, zugelassen werden, sollten diese mit einem ausdrücklichen Widerrufsvorbehalt versehen und mit dem Hinweis auf die Freiwilligkeit dieser Leistungsausweitung des Hochschulrechenzentrums kombiniert werden. Weiterhin zu beachten ist allerdings, dass ein Ausschluss der Privatnutzung bei Studierenden mangels rechtssicherer Abgrenzung schwerlich durchzusetzen ist.

(3) Die Zulassung zur Nutzung der Einrichtungen und Dienste des Hochschulrechenzentrums erfolgt durch Erteilung einer Nutzungserlaubnis. Diese wird vom Rechenzentrum schriftlich auf Antrag des Nutzers erteilt.

> Diese sowie die nachfolgenden Regelungen beschreiben ein „klassisches" Zulassungsverfahren auf schriftlichen Antrag des Nutzers. Natürlich sind auch andere Anmeldeverfahren denkbar, wie z. B. eine Online-Anmeldung oder die automatische Zulassung von Studierenden bei ihrer Immatrikulation. Sofern derartige Verfahren bereits praktiziert werden, müssen die Regelungen über das Zulassungsverfahren entsprechend modifiziert und ergänzt werden.

(4) Der Antrag soll unter Verwendung eines vom Rechenzentrum vorgegebenen Formblatts folgende Angaben enthalten:

[Beispiele]

> Die erforderlichen Angaben auf dem Nutzerantrag sind an die jeweiligen hochschulinternen Besonderheiten anzupassen: Wenn z. B. gesonderte Antragsformulare für die Internetnutzung durch Studierende verwendet werden sollen, entfallen naturgemäß Angaben z. B. über die Finanzierung des DV-Projekts, den Auftraggeber oder die Dauer und den Umfang des DV-Vorhabens.

1. Name, Anschrift und Unterschrift des Antragstellers sowie seinen Status als Studierender, Mitarbeiter, Einrichtung oder sonstiger Benutzer im Sinne von § 4 Abs. 1;
2. Beschreibung des Nutzungszwecks bzw. des geplanten Vorhabens;

3. Gewünschte DV-Ressourcen;
4. Erklärung zur Verarbeitung personenbezogener Daten durch den Nutzer;
5. Erklärung, dass der Antragsteller sich mit seiner Unterschrift einverstanden erklärt, dass das Rechenzentrum die Sicherheit der System-/Benutzerpasswörter und der Nutzerdaten durch regelmäßige manuelle oder automatisierte Maßnahmen überprüfen und notwendige Schutzmaßnahmen, wie z. B. Änderung leicht zu erratender Passwörter, durchführen wird, um die DV-Ressourcen und Benutzerdaten vor unberechtigten Zugriffen Dritter zu schützen. Erklärung, dass der betroffene Nutzer unverzüglich über die erforderliche Änderung seines Nutzerpassworts, der Zugriffsberechtigung auf seine Nutzerdateien und sonstige nutzungsrelevante Schutzmaßnahmen in Kenntnis gesetzt wird;

Die Einverständniserklärung in die Datenveränderung ist einzuholen, um eine mögliche Strafbarkeit wegen Datenveränderung nach § 303a StGB abzuwenden. Näheres hierzu unter § 7 Abs. 4 dieser Musterbenutzungsordnung. Unabhängig davon ist aber stets eine Änderung des Passworts durch den Nutzer selbst vorzugswürdig.

6. Anerkennung dieser Benutzungsordnung sowie der nach § 3 Abs. 3 erlassenen Betriebsregelungen als Grundlage des Nutzungsverhältnisses;

Ggf. ist hier noch eine evtl. bestehende Kosten- und Entgeltordnung zu ergänzen. Die ausdrückliche Anerkennung der Benutzungs- und Kostenordnung auf dem Nutzerantrag ist vor allem für die Zulassung externer Nutzer von Bedeutung, soweit diese im Rahmen eines privatrechtlichen Nutzungsverhältnisses erfolgt: Die Zulassung als solche, d. h. die Begründung des Nutzungs- bzw. Grundverhältnisses, kann entweder privatrechtlich durch Abschluss eines Vertrages (vor allem bei externen Nutzern) oder - nach der hier vorgesehen Konzeption (vgl. § 4 Abs. 3) - bei allen Nutzern als öffentlich-rechtlicher Akt erfolgen. Demgegenüber ist die Nutzung selbst (sog. Leistungsverhältnis), insbesondere die Regelung des Nutzungsentgelts, bei externen Nutzern i.d.R. privatrechtlich ausgestaltet (sog. Zwei-Stufen-Theorie). Letzteres ist jedoch abhängig vom Nutzerkreis und der landesrechtlichen Ausgestaltung des Nutzungsverhältnisses, z. B. durch eine landesweite Gebührenverordnung für alle Rechenzentren. Dann ist u. U. auch für Nicht-Hochschulangehörige ein öffentlich-rechtlicher Gebührenbescheid möglich. Sofern dies nicht der Fall ist, bestimmt sich die nähere Ausgestaltung des Nutzungsverhältnisses bei externen Nutzern - auch hinsichtlich der Kostenregelung - nach den getroffenen privatrechtlichen Vereinbarungen. Damit die Benutzungs-/Betriebs- und Entgeltordnung auch Bestandteil eines privatrechtlich ausgestalteten Nutzungsverhältnisses wird, ist hierauf im Zulassungsantrag ausdrücklich hinzuweisen (vgl. § 305 Abs. 2 BGB). Nach Möglichkeit ist der Text der Benutzungs- und sonstiger Ordnungen dem Antrag beizufügen bzw. es ist zumindest deutlich darauf hinzuweisen, auf welche Weise sich der Nutzer vom Inhalt der Benutzungsordnung Kenntnis verschaffen kann (z. B. Aushang im Rechenzentrum, Abruf im WWW über öffentlich zugängliche PC unter Angabe der genauen URL).

7. Schriftliche oder elektronische Einverständniserklärung des Nutzers zur Verarbeitung seiner personenbezogenen Daten;

Der Inhalt einer derartigen „Datenschutzklausel" bestimmt sich in erster Linie nach den Vorgaben der Datenschutzgrundverordnung (DSGVO). Die Voraussetzungen einer wirksamen Einwilligung ergeben sich aus Art. 7 DSGVO. Zwar ist hier grundsätzlich keine Form vorgeschrieben, nach Art. 7 Abs. 1 DSGVO muss der Nachweis der Einwilligung aber vom Verantwortlichen erbracht werden, was faktisch zu einer Dokumentationspflicht führt.

Grundsätzlich ist hier auch eine elektronische Dokumentation denkbar. Ausnahmen gelten für Beschäftigte der Hochschule. Hier sind über Art. 88 DSGVO bereichsspezifische Sonderregelungen im nationalen Recht zulässig. Diese finden sich in den Landesdatenschutzgesetzen (bspw. § 18 DSG NRW) und schreiben oftmals eine Schriftform vor. Unzulässig ist in jedem Fall eine „erzwungene" Einwilligung des Nutzers in eine generelle Protokollierung seiner Aktivitäten oder in eine uneingeschränkte Einsicht in seine Benutzerdateien. Diese Unzulässigkeit ergibt sich aus dem Gebot, dass die Einwilligung stets freiwillig sein muss (vgl. Art. 7 Abs. 4 DSGVO). Auch aus Gründen der Verhältnismäßigkeit sollte auf eine solche allumfassende Einwilligung verzichtet werden. Dabei ist zu berücksichtigen, dass der Nutzer einen grundrechtlich gesicherten Zulassungsanspruch bzw. zumindest einen Anspruch auf ermessensfehlerfreie Entscheidung über seinen Zulassungsantrag hat. Im Rahmen dieser Ermessensentscheidung über die Zulassung scheidet aber eine sachwidrige Koppelung des Zulassungsbegehrens an eine „erzwungene" Einwilligung als Zulassungsbedingung wegen der dann fehlenden Freiwilligkeit und des Vorliegens der Gefahr einer Umgehung des Datenschutzes grundsätzlich aus. Die Zulassung zum Dienst darf also nicht von einer Einwilligung abhängig gemacht werden, wenn der Nutzer zu Studien-, Forschungs- oder Arbeitszwecken auf den Dienst angewiesen ist. Davon ist u.a. angesichts der fortschreitenden Digitalisierung von Forschung und Lehre und der von einer Zulassung abhängigen Zugriffsberechtigung auf fachspezifische Datenbanken i.d.R. auszugehen. Eine Einschränkung der Dienste auf das notwendige Minimalmaß bei Verweigerung der Einwilligung dürfte aber zulässig sein, wenn dadurch Interessen der Hochschule (z. B. Gewährleistung von Systemsicherheit) verfolgt werden. Des Weiteren ist darauf zu achten, dass eine informierte Einwilligung vorliegt. Zu diesem Zwecke sind die Informationspflichten der Art. 12, 13 DSGVO einzuhalten. Regelmäßig werden sich entsprechende Informationen auf der Website des Rechenzentrums finden lassen. Ist dies der Fall, bietet sich ein Verweis auf die Website an entsprechender Stelle an.

8. Hinweis auf die Möglichkeiten einer Dokumentation des Nutzerverhaltens und der Einsichtnahme in die Nutzerdateien nach Maßgabe dieser Benutzungsordnung (vgl. § 7).

Diese Angaben verweisen auf § 7 Abs. 2 ff. dieses Entwurfs. Die Regelung kann ggf. mit dem Hinweis verbunden werden, dass sich der Nutzer nötigenfalls auch selbst um die Sicherheit seiner Daten bemühen sollte (z. B. durch geeignete Kryptographie-Verfahren etc.). Auch hier bietet sich ein Verweis auf die Website des Rechenzentrums zur Wahrung der datenschutzrechtlichen Informationspflichten an.

Weitere Angaben dürfen aus datenschutzrechtlichen Gründen nur erhoben werden, soweit dies zur Entscheidung über den Zulassungsantrag erforderlich ist.

(5) Die Nutzungserlaubnis ist auf das beantragte Vorhaben beschränkt und kann zeitlich befristet werden.

(6) Zur Gewährleistung eines ordnungsgemäßen und störungsfreien Betriebs kann die Nutzungserlaubnis überdies mit einer Begrenzung der Rechen- und Onlinezeit sowie mit anderen nutzungsbezogenen Bedingungen und Auflagen verbunden werden.

(7) Das Hochschulrechenzentrum kann die Zulassung zur Nutzung überdies vom Nachweis bestimmter Kenntnisse über die Benutzung der gewünschten Datenverarbeitungssysteme und DV-Dienste abhängig machen.

(8) Wenn die Kapazitäten der DV-Ressourcen nicht ausreichen, um allen Nutzungsberechtigten gerecht zu werden, können die Betriebsmittel für die einzelnen Nutzer entsprechend der Reihenfolge in § 4 Abs. 1 kontingentiert werden, da die Zulassung nur im Rahmen der verfügbaren Kapazitäten erfolgen kann.

(9) Die Nutzungserlaubnis kann ganz oder teilweise versagt, widerrufen oder nachträglich beschränkt werden, insbesondere wenn

1. kein ordnungsgemäßer Antrag vorliegt oder die Angaben im Antrag nicht oder nicht mehr zutreffen;
2. die Voraussetzungen für eine ordnungsgemäße Benutzung der DV-Einrichtungen nicht oder nicht mehr gegeben sind;
3. die nutzungsberechtigte Person nach § 6 von der Benutzung ausgeschlossen worden ist;
4. das geplante Vorhaben des Nutzers nicht mit den Aufgaben des Rechenzentrums und den in § 4 Abs. 2 genannten Zwecken vereinbar ist;
5. die vorhandenen DV-Ressourcen für die beantragte Nutzung ungeeignet oder für besondere Zwecke reserviert sind;
6. die Kapazität der Ressourcen, deren Nutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die geplante Nutzung nicht ausreicht;
7. die zu benutzenden DV-Komponenten an ein Netz angeschlossen sind, das besonderen Datenschutzerfordernissen genügen muss und kein sachlicher Grund für die geplante Nutzung ersichtlich ist;
8. zu erwarten ist, dass durch die beantragte Nutzung andere berechtigte Vorhaben in unangemessener Weise beeinträchtigt werden.

§ 5 Rechte und Pflichten der Nutzer

(1) Die nutzungsberechtigten Personen (Nutzer) haben das Recht, die Einrichtungen, Datenverarbeitungsanlagen und Informations- und Kommunikationssysteme des Hochschulrechenzentrums im Rahmen der Zulassung und nach Maßgabe dieser Benutzungsordnung sowie der nach § 3 Abs. 3 erlassenen Regeln zu nutzen. Eine hiervon abweichende Nutzung bedarf einer gesonderten Zulassung. Ein Anspruch auf ununterbrochenen und störungsfreien Zugang zu den Einrichtungen, Datenverarbeitungsanlagen und Informations- und Kommunikationssystemen des Hochschulrechenzentrums sowie auf unveränderte Fortführung des Leistungsangebots erwächst daraus nicht.

(2) Die Nutzer sind verpflichtet,

(Allgemein)

1. die Vorgaben der Benutzungsordnung zu beachten und die Grenzen der Nutzungserlaubnis einzuhalten, insbesondere die Nutzungszwecke nach § 4 Abs. 2 zu beachten;
2. alles zu unterlassen, was den ordnungsgemäßen Betrieb der DV-Einrichtungen des Hochschulrechenzentrums stört;
3. alle Datenverarbeitungsanlagen, Informations- und Kommunikationssysteme und sonstigen Einrichtungen des Rechenzentrums sorgfältig und schonend zu behandeln;

(Umgang mit Benutzungskennungen)

4. ausschließlich mit den Benutzungskennungen zu arbeiten, deren Nutzung ihnen im Rahmen der Zulassung gestattet wurde;
5. Benutzerpasswörter nicht an Dritte weiterzugeben und dafür Sorge zu tragen, dass keine anderen Personen Kenntnis von den Benutzerpasswörtern erlangen, sowie Vor-

kehrungen zu treffen, damit unberechtigten Personen der Zugang zu den DV-Ressourcen des Rechenzentrums verwehrt wird; dazu gehört auch der Schutz des Zugangs durch ein geheim zu haltendes und geeignetes, d. h. nicht einfach zu erratendes Passwort, das möglichst regelmäßig geändert werden sollte;

6. fremde Benutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen;
7. keinen unberechtigten Zugriff auf Informationen anderer Nutzer zu nehmen und bekanntgewordene Informationen anderer Nutzer nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern;
8. Durch diese Regelung werden insbesondere die strafrechtlichen Verbote nach § 202a StGB (Ausspähen von Daten) und § 303a StGB (Datenveränderung) ausdrücklich in das Benutzungsverhältnis aufgenommen. Diese Relativierung der an sich absolut wirkenden Strafvorschriften ist für den Ausschluss einzelner Nutzer ohne rechtskräftiges Strafurteil von Bedeutung, z. B. wenn zwar der Straftatbestand rechtswidrig und schuldhaft verwirklicht wurde (und deshalb ein Interesse am Ausschluss des Täters besteht), aber der zur Strafverfolgung erforderliche Strafantrag nicht gestellt wurde oder sonstige Strafverfolgungshindernisse bestehen.

(Softwarenutzung, Urheberrechte, sonstige Schutzrechte Dritter)

9. bei der Benutzung von Software, Dokumentationen und anderen Daten die gesetzlichen Vorgaben, insbesondere zum Urheberrechtsschutz, einzuhalten und die Lizenzbedingungen, unter denen Software, Dokumentationen und Daten vom Rechenzentrum zur Verfügung gestellt werden, zu beachten;
10. die nationalen und internationalen Urheber-, Marken-, Patent-, Namens- und Kennzeichenrechte sowie sonstige gewerbliche Schutzrechte und Persönlichkeitsrechte Dritter bei der Nutzung der Dienste zu wahren;
11. das Abrufen, Anbieten, Hochladen oder Verbreiten von rechtswidrigen Inhalten, insbesondere solchen, die gegen strafrechtliche, datenschutzrechtliche, persönlichkeitsrechtliche, lizenzrechtliche, oder urheberrechtliche Bestimmungen verstoßen, zu unterlassen;
12. vom Rechenzentrum bereitgestellte Software sowie die Software, die zum Betrieb der Dienste dient, Dokumentationen und Daten weder zu kopieren noch an Dritte weiterzugeben, sofern dies nicht ausdrücklich erlaubt ist, noch zu anderen als den erlaubten Zwecken zu nutzen;

(Nutzung der Rechenzentrumseinrichtungen, CIP-Pool)

13. in den Räumen des Hochschulrechenzentrums den Weisungen des Personals Folge zu leisten und die Hausordnung des Rechenzentrums zu beachten; Diese Regelung ist Ausdruck des Hausrechts des Leiters des Rechenzentrums, der die Ausübung auch auf Mitarbeiter übertragen kann.
14. die Benutzungsberechtigung auf Verlangen nachzuweisen;
15. Störungen, Beschädigungen und Fehler an DV-Einrichtungen und Datenträgern des Rechenzentrums nicht selbst zu beheben, sondern unverzüglich dem Rechenzentrumspersonal zu melden;

16. ohne ausdrückliche Einwilligung des Rechenzentrums keine Eingriffe in die Hardwareinstallation des Rechenzentrums vorzunehmen und die Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Nutzerdateien und des Netzwerks nicht zu verändern;
17. Hiermit sollen Veränderungen an den Nutzerdateien untersagt werden, die systembedingt bei der Einrichtung des User-Accounts mit Schreibrechten für den User angelegt werden und aus Gründen des Systemschutzes nicht manuell vom Nutzer verändert werden sollten (z. B. Shell-Befehlsprotokolldateien oder Konfigurationsdateien).

(Sonstiges)

18. der Rechenzentrumsleitung auf Verlangen in begründeten Einzelfällen - insbesondere bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung - zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu erteilen sowie Einsicht in die Programme zu gewähren;
19. 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 (z. B. Patientendaten). Vgl. hierzu die speziellere Regelung in § 7 Abs. 5 ff. dieses Entwurfs.
20. eine Verarbeitung personenbezogener Daten mit dem Rechenzentrum abzustimmen und - unbeschadet einer eigenen datenschutzrechtlichen Verpflichtungen des Nutzers - die vom Hochschulrechenzentrum vorgeschlagenen Datenschutz - und Datensicherheitsvorkehrungen zu berücksichtigen.

(3) Auf die folgenden Straftatbestände wird besonders hingewiesen:

1. Ausspähen von Daten (§ 202a StGB),
2. Abfangen von Daten (§ 202b StGB),
3. Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB),
4. Datenhehlerei (§ 202d StGB),
5. Datenveränderung (§ 303a StGB) und Computersabotage (§ 303b StGB),
6. Computerbetrug (§ 263a StGB),
7. Verbreitung pornographischer Darstellungen (§§ 184 ff. StGB), insbesondere Verbreitung, Erwerb und Besitz kinderpornographischer Schriften (§ 184b StGB) und die Verbreitung pornographischer Darbietungen durch Rundfunk oder Telemedien (§ 184d StGB),
8. Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB) und Volksverhetzung (§ 130 StGB),
9. Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB),
10. strafbare Urheberrechtsverletzungen, z. B. durch urheberrechtswidrige Vervielfältigung von Software (§§ 106 ff. UrhG).

Entsprechende Hinweise auf spezifische Straftatbestände sind in fast allen Benutzungsordnungen zu finden. Grundsätzlich haben Verweise und Hinweise auf Straftatbestände

jedoch nur eine deklaratorische Funktion, da die aufgeführten Straftatbestände selbstverständlich auch ohne ausdrücklichen Hinweis in der Benutzungsordnung gelten. Aus diesem Grund kann auf diesen Absatz auch verzichtet werden.

§ 6 Ausschluss von der Nutzung

Mit den nachfolgenden Grundtatbeständen werden alle Missbräuche erfasst, die im Verhältnis zum Rechenzentrum einen Nutzungsausschluss rechtfertigen können. So wird z. B. die kommerzielle Nutzung als Verstoß gegen die Benutzungsordnung (§ 5 Abs. 1, 2 lit. a i.V.m. § 4 Abs. 2) erfasst, weil sich eine kommerzielle Nutzung nicht mehr im Rahmen der Nutzungszulassung hält. Sämtliche Hacker-Aktivitäten innerhalb der Systeme des Rechenzentrums stellen einerseits einen Verstoß gegen § 5 Abs. 2 lit. d, f, g der Benutzungsordnung und andererseits i.d.R. gegen §§ 202a, 202b, 303a StGB dar. Fraglich erscheint hingegen, ob auch unberechtigte Zugriffe auf fremde Daten, die sich außerhalb des Verantwortungsbereichs des Rechenzentrums befinden, also z. B. Hacker-Attacken auf fremde Internet-Server, als Verstoß gegen die Benutzerordnung einen Ausschluss einzelner Nutzer rechtfertigen können. Hierdurch ist nämlich das relative Nutzungsverhältnis zwischen Rechenzentrum und Nutzer nicht unmittelbar betroffen. Etwas Anderes gilt allerdings dann, wenn bei unberechtigten Zugriffen auf externe Daten die IP-Adresse der Hochschule verwendet wird. In diesem Fall können sich auch Konsequenzen für das vermeintlich unbeteiligte Rechenzentrum ergeben. Jedenfalls können Hacker-Angriffe auf externe Systeme aber als strafbare Handlungen (§§ 202a, 303a StGB) einen Ausschluss nach § 6 Abs. 1 lit. b begründen.

Eine "Beschränkung" der Nutzungsmöglichkeiten im Sinne dieser Vorschrift kann auch durch die Sperrung nur einzelner Dienste erfolgen.

(1) Nutzer können vorübergehend oder dauerhaft in der Benutzung der DV-Ressourcen beschränkt oder hiervon ausgeschlossen werden, wenn

1. sie schuldhaft gegen diese Benutzungsordnung, insbesondere gegen die in § 5 aufgeführten Pflichten, verstoßen oder
2. sie die DV-Ressourcen des Rechenzentrums für strafbare Handlungen missbrauchen oder

   Sofern die Strafbarkeit der jeweiligen Handlung nicht offenkundig ist, kommt aufgrund der grundgesetzlich verankerten Unschuldsvermutung ein dauerhafter Ausschluss grundsätzlich nur bei rechtskräftiger Verurteilung des Nutzers in Betracht. Dies gilt insbesondere für Ehrverletzungsdelikte und alle sonstigen Tatbestände, die dem Schutzbereich der Meinungsfreiheit unterfallen. Zur kurzfristigen Sperrung bei unklarer Rechtslage vgl. § 7 Abs. 3 dieses Entwurfs.

3. der Hochschule durch sonstiges rechtswidriges Nutzerverhalten Nachteile entstehen.

   Hierdurch werden alle sonstigen rechtswidrigen Verhaltensweisen auch außerhalb des Strafrechts erfasst, z. B. Urheberrechts- oder Markenrechtsverletzungen. Ein Nutzungsausschluss wegen eines entsprechenden (rein zivilrechtswidrigen) Verhaltens kommt jedoch nur in Betracht, wenn die Hochschule hiervon selbst betroffen ist, z. B. in Form einer Abmahnung, Unterlassungserklärung oder Schadensersatzforderung.

(2) Maßnahmen nach Abs. 1 sollen erst nach vorheriger erfolgloser Abmahnung erfolgen. Dies gilt nicht bei Gefahr im Verzug. Hierüber ist der Betroffene unverzüglich zu informieren. Dem Betroffenen ist Gelegenheit zur Stellungnahme zu geben. In jedem Fall ist ihm Gelegenheit zur Sicherung seiner Daten einzuräumen.

Das Erfordernis einer vorherigen Abmahnung in Abs. 1 ist als Soll-Vorschrift konzipiert, da eine Abmahnung bei sehr schwerwiegenden Verstößen im Einzelfall entbehrlich sein kann. Demgegenüber garantiert Absatz 2 als zwingende Ist-Vorschrift einen verfahrensrechtlichen Mindestschutz des Betroffenen, indem ihm bei allen „Sanktionen" die Möglichkeit gewährt wird, sich zu den Vorwürfen zu äußern. Die Vorgaben des Absatz 2 gelten für alle Maßnahmen nach Absatz 1, also sowohl für vorübergehende Beschränkungen als auch für einen dauerhaften Ausschluss. Demgegenüber enthalten die Absätze 3 und 4 jeweils Sonderregelungen für die unterschiedlichen Sanktionsmöglichkeiten.

(3) Vorübergehende Nutzungseinschränkungen, über die der Leiter des Rechenzentrums entscheidet, sind aufzuheben, sobald eine ordnungsgemäße Nutzung wieder gewährleistet erscheint.

(4) Eine dauerhafte Nutzungseinschränkung oder der vollständige Ausschluss eines Nutzers von der weiteren Nutzung kommt nur bei schwerwiegenden oder wiederholten Verstößen i.S.v. Abs. 1 in Betracht, wenn auch künftig ein ordnungsgemäßes Verhalten nicht mehr zu erwarten ist. Die Entscheidung über einen dauerhaften Ausschluss trifft der Kanzler auf Antrag des Leiters des Rechenzentrums und nach Anhörung durch eine dafür eingerichtete Kommission durch Bescheid. Mögliche Ansprüche des Rechenzentrums aus dem Nutzungsverhältnis bleiben unberührt.

Eine Anhörung sollte an dieser Stelle gewährleistet werden, um den Eingriff in die Berufsfreiheit (Art. 12 Abs. 1 GG) durch ein entsprechendes Verfahren zu begleiten. Eine dafür zuständige Kommission muss von der Hochschule eingerichtet werden und kann in der Norm mit ihrer Bezeichnung eingesetzt werden.

§ 7 Rechte und Pflichten des Hochschulrechenzentrums

(1) Das Hochschulrechenzentrum führt über die erteilten Benutzungsberechtigungen eine Nutzerdatei mit den erforderlichen Bestandsdaten, in der insbesondere die Benutzer- und Mailkennungen sowie der Name und die Anschrift der zugelassenen Nutzer aufgeführt werden.

Seit dem 25. Mai 2018 haben sich die Rechtsgrundlagen für die Verarbeitung von Bestandsdaten der Nutzer geändert. Es muss nunmehr danach differenziert werden, aus welcher Personengruppe die Nutzer stammen. Soweit es um Beschäftigte der Hochschule geht und die Nutzung des Accounts für dienstliche Zwecke erforderlich ist, ergibt sich die Erlaubnis zur Nutzung aus Art. 88 DSGVO in Verbindung mit entsprechenden Normen der Landesdatenschutzgesetze zur Verarbeitung von Daten zur Durchführung des Beschäftigungsverhältnisses (z.B. § 18 DSG NRW). Hierzu gehören auch die dienstlich genutzte Nutzerkennung sowie die damit verbundenen Informationen zum Mitarbeiter.

Handelt es sich bei den Nutzern um Studierende oder Gäste aus Wissenschaft und Forschung, so wird die Einrichtung des Accounts der Ermöglichung des Studiums und somit einer Aufgabe dienen, die im öffentlichen Interesse liegt. Mit Inkrafttreten des TTDSG sind die Regelungen der §§ 95 Abs. 1 TKG und § 14 Abs. 1 TMG weggefallen. Die Zulässigkeit der Verarbeitung richtet sich nunmehr nach Art. 6 Abs. 1 lit. e DSGVO (in Verbindung mit den Normen des jeweiligen Landeshochschulgesetzes oder Landesdatenschutzgesetzes).

Die Aufzählung in § 7 Abs. 1 ist nur beispielhaft, da sich die Erforderlichkeit aus den jeweiligen Gegebenheiten und Erfordernissen der Einrichtung ergibt.

(2) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerdaten erforderlich ist, kann das Hochschulrechenzentrum die Nutzung seiner Ressourcen vorübergehend einschränken oder

einzelne Nutzerkennungen vorübergehend sperren. Sofern möglich sind die betroffenen Nutzer hierüber im Voraus zu unterrichten.

(3) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass ein Nutzer auf den Servern des Rechenzentrums rechtswidrige Inhalte zur Nutzung bereithält, kann das Rechenzentrum die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.

Hierdurch soll gewährleistet werden, dass das Rechenzentrum Internet-Seiten (WWW) oder sonstige Dateien (z. B. per FTP), die von Nutzern über die Server des Rechenzentrums zum allgemeinen Abruf angeboten werden, bis zur Klärung der Rechtslage sperren kann, wenn die Inhalte zweifelhaft erscheinen oder die Rechtswidrigkeit in einer Abmahnung gerügt wird. Die Einsichtnahme oder Sperrung „normaler" Benutzerdaten, die vom Nutzer nicht zum allgemeinen Abruf freigegeben sind, wird von der vorstehenden Regelung jedoch nicht erfasst. Vielmehr ist die Kontrolle der „privaten" Nutzerdateien allein unter den in Abs. 5 ff. genannten Voraussetzungen oder aufgrund einer richterlichen bzw. polizeilichen/staatsanwaltlichen Aufforderung (z. B. „Beschlagnahme der Dateien" als Beweismittel) möglich.

(4) Das Rechenzentrum ist berechtigt, die Sicherheit der System-/Benutzerpasswörter und der Nutzerdaten durch regelmäßige manuelle oder automatisierte Maßnahmen zu überprüfen und notwendige Schutzmaßnahmen, z. B. Änderungen leicht zu erratender Passwörter, durchzuführen, um die DV-Ressourcen und Benutzerdaten vor unberechtigten Zugriffen Dritter zu schützen. Bei erforderlichen Änderungen der Benutzerpasswörter, der Zugriffsberechtigungen auf Nutzerdateien und sonstigen nutzungsrelevanten Schutzmaßnahmen ist der Nutzer hiervon unverzüglich in Kenntnis zu setzen.

Durch diese Ermächtigungsgrundlage wird eine Rechtfertigung für den Einsatz von sog. „Crack-Software" geschaffen, die automatisch Passwörter ermittelt, bei Bedarf (z. B. einfach zu erratende Begriffe) ersetzt und den Nutzer hiervon in Kenntnis setzt. Da die Änderung eines vom Benutzer selbst eingerichteten Passworts u. U. den Straftatbestand der Datenveränderung (§ 303a StGB) erfüllen kann, ist eine entsprechende Ermächtigungsgrundlage erforderlich. Dennoch sollte nach Möglichkeit einer Aufforderung des Nutzers zur Änderung des Passworts der Vorzug gegeben werden, damit dieser innerhalb einer bestimmten Frist selbst tätig werden kann.

Auch aus datenschutzrechtlicher Sicht sind Schutzmaßnahmen erforderlich. So gehört die Integrität und Vertraulichkeit der Datenverarbeitung nach Art. 5 Abs. 1 lit. f DSGVO zu den Datenschutzgrundsätzen. Es ist eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten, welche den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen sicherstellt. Diese werden in Art. 32 DSGVO weiter konkretisiert, wobei Maßnahmen gemeint sind, die ein dem Risiko angemessenes Schutzniveau gewährleisten. Dies umfasst auch geeignete Zugangs-, Benutzer- und Zugriffskontrollen, die durch passwortgeschützte Systemzugänge zu realisieren sind. Insoweit ist eine regelmäßige Überprüfung der Benutzerpasswörter aus Gründen der Systemsicherheit datenschutzrechtlich geboten. Hierbei ist jedoch zu beachten, dass eine Befugnis zur Passwortänderung im Rahmen von Art. 32 DSGVO nur zur Sicherung der gespeicherten Nutzer- und Telekommunikationsdaten vor unberechtigten Zugriffen Dritter besteht. Eine verdeckte Sanktion des fahrlässigen Nutzerverhaltens, z. B. durch ein für ihn umständliches Wiederfreischaltungsverfahren, ist hingegen nicht zulässig. Wichtig ist daher, dass der Nutzer möglichst vor, z. B. in Form einer Abmahnung, oder unmittelbar nach der Änderung seiner Passwörter und Zugriffsrechte hierüber informiert wird, damit er - nach Eingabe des neuen Passworts - weiterhin auf seine Daten zugreifen kann.

(5) Das Hochschulrechenzentrum ist nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme durch die einzelnen Nutzer zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist:

Die Dokumentation und Auswertung aus Sicherheitsgründen erfolgt aufgrund eines „öffentlichen Interesses“ der Hochschule an der Wahrung der Funktionsfähigkeit der informationstechnischen Systeme. Grundsätzlich kann sich die Hochschule deshalb auf Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO (in Verbindung mit den Normen des jeweiligen Landeshochschulgesetzes oder Landesdatenschutzgesetzes) berufen. Von besonderer Bedeutung ist ferner die Formulierung „soweit dies erforderlich ist". Hierdurch wird das Verhältnismäßigkeitsprinzip betont, das bei jeder Überwachungsmaßnahme zwingend zu beachten ist. Es bezieht sich sowohl auf den Zweck der Kontrollmaßnahme als auch auf die Intensität. Insbesondere im Rahmen der „telekommunikationsrechtlichen" Nutzeraktivitäten (Login-Zeiten, Mail-Nutzung, Verbindungsdaten im Netzverkehr) aber auch bei der Kontrolle des nicht-telekommunikationsspezifischen Nutzerverhaltens sollte eine Einsicht in personenbezogene Daten sowie in die Inhalte der Benutzerdateien nur als letztes Mittel in Erwägung gezogen werden. So kann es z. B. ausreichen, wenn das Benutzerverhalten in anonymisierter Form dokumentiert wird. Eine Einsicht in die E-Mails der Nutzer dürfte wegen Art. 10 GG und § 3 Abs. 3 S. 1 TDDDG generell ausscheiden („Es dürfen nur die näheren Umstände der Telekommunikation erhoben werden"). Auch die detaillierte, d. h. personen- und inhaltsbezogene Protokollierung der Online-Aktivitäten (clickstream) dürfte nicht dem Erforderlichkeitsmaßstab genügen.

1. Zur Gewährleistung eines ordnungsgemäßen Systembetriebs,
2. zur Ressourcenplanung und Systemadministration,
3. zum Schutz der personenbezogenen Daten anderer Nutzer,

Durch diesen Tatbestand wird den Anforderungen der Datenschutzgesetze an einen „technisch-organisatorischen" Datenschutz entsprochen. Insbesondere können die zum Schutz personenbezogener Daten erforderlichen Schutzmaßnahmen eine Zugangs-, Benutzer-, Übermittlungs- und Zugriffskontrolle beinhalten (vgl. Art. 32 DSGVO). Wichtig ist hierbei jedoch, dass die Maßnahmen sich stets auf das für die Wahrung der Sicherheit notwendige Maß beschränken, um der Erforderlichkeit aus Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO i.V.m. dem Landeshochschul- oder - datenschutzgesetz zu genügen. Es muss also eine beschränkte datenbezogene Protokollierung stattfinden, während eine nutzerbezogene Überwachung aller Nutzeraktivitäten unzulässig ist, wenn hierdurch ein Benutzerprofil entstünde, das auch die Online-Aktivitäten umfasst. Dies bedeutet, dass z. B. eine möglichst lückenlose Protokollierung der Zugriffe und Zugriffsversuche auf die Benutzerdatenbank (Benutzeraccount und Passwörter) geboten sein kann, die freilich auch alle Zugriffe durch den Systemadministrator erfassen muss. Demgegenüber dürfte es unzulässig sein, für alle Nutzer generell ein Nutzer-Protokoll zu erstellen, um im Nachhinein unberechtigte Zugriffe auf die Daten anderer Nutzer nachvollziehen zu können. Sofern die Erhebung sonstiger Daten technisch erforderlich ist, um Dateizugriffe zu erfassen, müssen diese sonstigen Daten unverzüglich nach Erhebung, spätestens jedoch nach einer - möglichst automatisierten - Auswertung der Protokolle wieder aus den Logfiles gelöscht oder anonymisiert werden.

4. zu Abrechnungszwecken,
5. für das Erkennen und Beseitigen von Störungen sowie
6. zur Aufklärung und Unterbindung rechtswidriger oder missbräuchlicher Nutzung.

Diese Regelung orientiert sich an § 9 Abs. 1 S. 3 TDDDG i.V.m. §§ 10, 12 TDDDG, die über Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO weiterhin für Hochschulrechenzentren gelten, da es sich für geschäftsmäßige Anbieter von Telekommunikationsdiensten aus dem ö entlichen Bereich um speziellere Regelungen als die allgemeine Erlaubnisnorm aus dem jeweiligen Landes-datenschutzgesetz handelt. Die vorliegende Regelung bezieht sich nicht nur auf mentation der Benutzeraktivitäten, die als Telekommunikation dem besonderen Schutz des Telekommunikationsgeheimnisses unterliegen. Vielmehr wird auch die Protokollierung sonstiger Nutzeraktivitäten, z. B. die Inanspruchnahme von CPU-Rechenzeit oder von Speicherplatz durch einfache Nutzerdateien, erfasst. Beide Verhaltensbereiche werden zunächst zusammen behandelt, wobei für die spezifisch geschützte Telekommunikation eine Einschränkung der Kontrollbefugnisse geboten ist (vgl. die Einschränkungen in Abs. 6ff.).

(6) Unter den Voraussetzungen von Abs. 5 ist das Rechenzentrum 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.

Durch diese Regelung soll die Einsicht in „normale", d. h. nicht als Telekommunikationsinhalt besonders geschützte Dateien geregelt werden. Wichtig ist bei einem Missbrauchsverdacht, dass „tatsächliche Anhaltspunkte" vorliegen müssen, die in den Akten dokumentiert werden sollten. Besondere Relevanz kommt dem Erfordernis der tatsächlichen Anhaltspunkte für einen Missbrauch bei der „Verfolgung" von Straftaten zu, die an sich nicht in den Aufgabenbereich des Rechenzentrums fallen. Deshalb geht es bei der Missbrauchsaufdeckung (nicht präventive, verdachtsunabhängige Verhinderung bei bloß unbestimmten Missbrauchsgefahren) vor allem um Missbräuche im Verhältnis Nutzer zu Rechenzentrum. Freilich stellen auch strafbare Handlungen einen solchen „relativen" Missbrauch dar, da sie weder von der Benutzungsordnung noch von der Zulassung oder vom Anstaltszweck gedeckt sind. Problematisch ist jedoch die Frage, ab wann „tatsächliche Anhaltspunkte" für eine strafbare Handlung vorliegen. Diese Bewertung sollte daher grundsätzlich der Staatsanwaltschaft überlassen werden, da nur diese für die Verfolgung von Straftaten zuständig ist. Bei Verdachtsmomenten sollte deshalb nicht „auf eigene Faust" durch detaillierte Einsichtnahme in die Benutzerdateien weiter ermittelt werden, sondern das weitere Vorgehen sollte mit der Staatsanwaltschaft abgesprochen werden.

Eine Einsichtnahme in die Nachrichten- und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist.

Diese Einschränkung trägt dem besonderen Schutz der Nachrichteninhalte durch Art. 10 GG und § 3 TDDDG Rechnung. Eine Einsichtnahme der Mailbox-Inhalte kommt deshalb nur dann in Betracht, wenn dies zur Behebung einer Störung im Maildienst zwingend erforderlich ist, z. B. bei der Wiederherstellung automatisch gesicherter Nachrichten im Falle eines Ausfalls des systeminternen Zustelldienstes. Das Erfordernis der „Unerlässlichkeit" ist als Ausdruck des „ultima ratio"-Prinzips aufgrund des u. U. schwerwiegenden Eingriffs in die Privatsphäre des Betroffenen wörtlich zu nehmen. Es ist stets zu prüfen, ob nicht ein „milderes" Mittel gleich geeignet ist. Sofern möglich sollte daher die Beseitigung der Störung automatisch erfolgen, wenn eine manuelle Wiederherstellung mit der Kenntniserlangung der Mail-Inhalte verbunden wäre.

In jedem Fall ist die Einsichtnahme zu dokumentieren und der betroffene Benutzer ist nach Zweckerreichung unverzüglich zu benachrichtigen.

(7) Unter den Voraussetzungen von Abs. 5 können auch die Verkehrs- und Nutzungsdaten im Nachrichtenverkehr (insbesondere Mail-Nutzung) dokumentiert werden. Es dürfen jedoch nur

die näheren Umstände der Telekommunikation - nicht aber die nicht öffentlichen Kommunikationsinhalte - erhoben, verarbeitet und genutzt werden.

Da bereits veröffentlichte News-Beiträge nicht vom Telekommunikationsgeheimnis erfasst sind, betrifft die vorliegende Einschränkung nur „nicht-öffentliche" Kommunikationsinhalte. Im Übrigen orientiert sich die Regelung an §§ 9, 2 Abs. 1 TDDDG, 3 Nr. 30 TKG und 3 Abs. 3 S. 1 TDDDG, wonach nur die näheren Umstände der Telekommunikation liert und ausgewertet werden dürfen. Jedoch müssen auch hier in jedem Fall die Voraussetzungen für eine Protokollierung (vgl. Abs. 5) vorliegen.

Die Verkehrs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Telemediendiensten, die das Rechenzentrum zur Nutzung bereithält oder zu denen das Rechenzentrum den Zugang zur Nutzung vermittelt, sind frühestmöglich, spätestens unmittelbar am Ende der jeweiligen Nutzung, zu löschen, soweit es sich nicht um Abrechnungsdaten handelt.

Vgl. Art. 17 DSGVO.

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

§ 8 Haftung des Nutzers

(1) Der Nutzer haftet für alle Nachteile, die der Hochschule durch missbräuchliche oder rechtswidrige Verwendung der DV-Ressourcen und der Nutzungsberechtigung oder dadurch entstehen, dass der Nutzer schuldhaft seinen Pflichten aus dieser Benutzungsordnung nicht nachkommt.

(2) Der Nutzer haftet auch für Schäden, die im Rahmen der ihm zur Verfügung gestellten Zugriffs- und Nutzungsmöglichkeiten durch Drittnutzung entstanden sind, wenn er diese Drittnutzung zu vertreten hat, insbesondere im Falle einer Weitergabe seiner Benutzerkennung an Dritte. In diesem Fall kann die Hochschule vom Nutzer nach Maßgabe der Entgeltordnung ein Nutzungsentgelt für die Drittnutzung verlangen.

Eine Klausel über die Entgeltzahlungspflicht des Nutzers für eine unbefugte Nutzung durch Dritte verstößt gegen § 307 Abs. 1, 2 Nr. 1 und § 309 Nr. 12 lit. a, b BGB, soweit sie eine verschuldensunabhängige Haftung des Nutzers für alle Fälle der Drittnutzung vorsieht.[3] Erforderlich ist daher die Einschränkung, dass der Nutzer für die unbefugte Nutzung seines Zugangs nur haftet, soweit er diese zu vertreten hat.

(3) Der Nutzer stellt die Hochschule von allen Ansprüchen frei, wenn Dritte die Hochschule wegen eines missbräuchlichen oder rechtswidrigen schuldhaften Verhaltens des Nutzers auf Schadensersatz in Anspruch nehmen. Die Hochschule wird dem Nutzer den Streit verkünden, sofern Dritte auf Grund dieser Ansprüche gegen das Rechenzentrum gerichtlich vorgehen.

§ 9 Haftung der Hochschule

(1) Die Hochschule übernimmt keine Garantie dafür, dass das System fehlerfrei und jederzeit ohne Unterbrechung läuft. Eventuelle Datenverluste infolge technischer Störungen sowie die Kenntnisnahme vertraulicher Daten durch unberechtigte Zugriffe Dritter können nicht ausgeschlossen werden.

[3] vgl. LG Köln v. 13.3.96, 26 O 217/94, VuR 96, 349 (352 f.).

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

(3) Im Übrigen haftet die Hochschule für entstehende Schäden lediglich, soweit diese auf einer schuldhaften Verletzung einer wesentlichen Pflicht aus dem Nutzungsverhältnis oder auf einem vorsätzlichen oder grob fährlässigen Verhalten durch ihre gesetzlichen Vertreter, Mitarbeiter oder sonstigen Erfüllungsgehilfen beruht. Wird eine wesentliche Pflicht aus dem Nutzungsverhältnis leicht fahrlässig verletzt, so ist die Haftung der Hochschule auf typische, bei Begründung des Nutzungsverhältnisses vorhersehbare Schäden begrenzt. Eine wesentliche Pflicht aus dem Nutzungsverhältnis ist bei Verpflichtungen gegeben, deren Erfüllung die ordnungsgemäße Durchführung des Nutzungsverhältnisses erst möglich macht oder auf deren Einhaltung der Nutzer vertraut hat und vertrauen durfte. Eine darüberhinausgehende Haftung auf Schadensersatz ist ausgeschlossen. Die Haftung wegen schuldhafter Verletzung von Leben, Körper oder Gesundheit nach den gesetzlichen Bestimmungen bleibt unberührt. Dies gilt auch für die zwingende Haftung nach dem Produkthaftungsgesetz. Soweit die Haftung ausgeschlossen oder begrenzt wird, gilt dies auch für die persönliche Haftung der Organe, Mitarbeiter und Erfüllungsgehilfen der Hochschule.

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

Die vorstehenden Regelungen, insbesondere Abs. 3, orientieren sich an § 309 Nr. 7 lit. a und b und § 309 Nr. 8 lit. a BGB. Hierbei ist zu beachten, dass sich die Haftungsbeschränkung nur auf die quasi-schuldrechtliche Haftung der Hochschule beziehen kann. Eine derartige Verantwortlichkeit kann sich aus einem verwaltungsrechtlichen Sonderschuldverhältnis aus §§ 276, 280 Abs. 1 und 3, 283, 280 Abs. 1 und 2, 286 BGB analog ergeben. Mögliche Amtshaftungsansprüche aus § 839 BGB i.V.m. Art. 34 GG stehen hierzu in Anspruchskonkurrenz, d. h. die Hochschule kann im Falle eines schuldhaften Verhaltens ihrer Mitarbeiter grundsätzlich sowohl nach Amtshaftungsgrundsätzen als auch wegen der Verletzung quasi-vertraglicher Pflichten aus dem verwaltungsrechtlichen Sonderverhältnis haften. Die vorliegende Haftungsbeschränkung kann sich wegen des grundgesetzlich garantierten Amtshaftungsanspruchs jedoch grundsätzlich nur auf die schuldrechtsähnliche Haftung der Hochschule beziehen (vgl. Abs. 4). Überdies sind hierbei die Vorgaben der §§ 305 ff. BGB zur Haftungsbeschränkung bei grobem Verschulden und bei der Verletzung wesentlicher (Kardinal-)Pflichten zu beachten (Vgl. *Gurlit*, in Ehlers/Pünder, Allgemeines Verwaltungsrecht, § 35, Rn. 38 f. (S. 791 f.)). Eine mit §§ 305 ff. BGB konforme Beschränkung der quasi-vertraglichen Haftung der Hochschule ist trotz der Anspruchskonkurrenz zur unbeschränkbaren Amtshaftung sinnvoll, da für beide Anspruchsgrundlagen unterschiedliche Voraussetzungen erfüllt sein müssen. So gilt im Rahmen der Amtshaftung z. B. nicht die erweiterte Verschuldensvermutung nach § 280 Abs. 1 S. 2 BGB analog, so dass der Anspruchsteller insoweit beweispflichtig bleibt. Dies hat wiederum zur Folge, dass bei leicht fahrlässigem Verhalten eines Mitarbeiters des Rechenzentrums eine Haftung der Hochschule regelmäßig ausscheidet, wenn der Anspruchsteller das Verschulden nicht nachweisen kann: In diesem Fall kommt nämlich eine Amtshaftung der Hochschule nicht in Betracht, da hier der Gläubiger für das Verschulden des Amtsträgers beweispflichtig ist. Überdies entfällt auch eine quasivertragliche Haftung, z. B. aus einem schuldrechtsähnlichen „Datenverwahrungsvertrag". Hier braucht der Schuldner wegen der Beweislastumkehr des § 280 Abs. 1 S. 2 BGB analog zwar das Verschulden nicht nachzuweisen, doch greift nun der vorliegende Haftungsausschluss für leicht fahrlässiges Verhalten der Mitarbeiter des Rechenzentrums.

§ 10 [Entgeltordnung]

An dieser Stelle kann ggf. eine Entgeltordnung als Anhang zur Benutzungsordnung eingefügt werden, die im Hinblick auf § 305 Abs. 2 BGB - insbesondere bei externen Nutzern - dem Antragsformular beigefügt werden sollte.

§ 11 Inkrafttreten

Die Ordnung des Hochschulrechenzentrums tritt am Tage nach ihrer Veröffentlichung in Kraft.