

# Rechtlicher Rahmen

## Ergänzendes Material zum Papier IT-Sicherheit an Hochschulen

Erarbeitet durch den AK-„IT-Sicherheit“ von Herbst 2004 bis Sommer 2005  
Version 1.0 - Stand Oktober 2005

Der rechtliche Rahmen der IT-Nutzung an Hochschulen ergibt sich im Wesentlichen aus den für die Kommunikation einschlägigen Spezialvorschriften (TDG, TDDSG, MDStV, TKG) und den hochschulspezifischen Vorschriften (meist Hochschulgesetze) auf Länderebene. Die kommunikationsbezogenen Spezialvorschriften beinhalten insbesondere Regelungen zur Haftung und zum Datenschutz. Daneben ergeben sich jedoch auch Anforderungen aus den allgemeinen Gesetzen wie zum Beispiel dem Strafgesetzbuch in Bezug auf strafbare Handlungen bei der Nutzung der Kommunikationstechnologie. Aus dem genannten Rechtsrahmen ergeben sich Anforderungen an die Hochschulen und die Nutzer. Nutzer sind in der Regel die Mitarbeiter und Studierenden der Hochschule. Aufgrund der zumeist großen Anzahl von Nutzern ist eine Zugangskontrolle verbunden mit einer Nutzungsordnung aus Sicherheitsgründen unerlässlich. Die Zugangskontrolle hat den Sicherheitsaspekt, dass nur autorisierte Nutzer die hochschulinterne Kommunikationstechnologie nutzen können. Die Nutzungsordnung dient der Konkretisierung der gegenseitigen Rechte und Pflichten und dient zugleich als Rechtsgrundlage für Ordnungsmaßnahmen. Im Folgenden wird ohne einen Anspruch auf Vollständigkeit ein Überblick über den rechtlichen Rahmen mit besonderem Bezug auf die IT-Sicherheit gegeben.

## 1 Verpflichtungen der Hochschule

- Die Hochschule hat ihren Studierenden bei Vorliegen der Zulassungsvoraussetzungen und vorhandener Ressourcen in der Regel die **Nutzungsberechtigung** zu erteilen, da mit der Entscheidung über die Berechtigung die Grundrechtsausübung des Studierenden (Art. 12 GG, Lernfreiheit) tangiert wird. Dies ist im Rahmen der Verhältnismäßigkeit auch bei einer nur partiellen Entziehung des Nutzungsrechts zu berücksichtigen. Bei Mitarbeitern sind hinsichtlich der Nutzungsrechte die arbeitsrechtlichen Grundsätze bzw. bei wissenschaftlichem Personal auch das Grundrecht der Freiheit von Wissenschaft, Forschung und Lehre aus Art. 5 Abs. 3 S. 1 GG zu beachten.
- Die Hochschule ist in der Regel aufgrund landesrechtlicher Datenschutzvorschriften im Rahmen der Verhältnismäßigkeit zu **technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes** verpflichtet. Hierzu gehören insbesondere Maßnahmen zur Sicherung von personenbezogenen Daten vor unerlaubten Zugriffen, etwa durch Hacker oder durch Schadsoftware. Eine speziellere und teilweise weiter gehende Verpflichtung im Hinblick auf den Datenschutz und das Telekommunikationsgeheimnis ergibt sich aus § 109 TKG, wenn die Hochschule als Telekommunikationsdiensteanbieter anzusehen ist. Dies ist in der Regel dann der Fall, wenn die Hochschule den Internetzugang und/oder den Mailedienst mit einer gewissen Nachhaltigkeit auch für private Zwecke gestattet.
- Die Hochschule hat **bei Sicherheitsmaßnahmen die Persönlichkeitsrechte der Nutzer zu beachten**. Eine fortdauernde Überwachung ohne begründbaren Verdacht verletzt das Persönlichkeitsrecht des betroffenen Nutzers. **Ist die Privatnutzung des Internetzugangs und/oder des Mailedienstes gestattet, hat die Hochschule zudem das Fernmeldegeheimnis aus Art. 10 GG (konkretisiert in § 88 TKG) und die providerspezifischen Datenschutzregelungen zu beachten**. Diese sind im TDDSG und im TKG enthalten und unterscheiden zwischen Bestands-, Nutzungs- und Verkehrsdaten. Unter den Begriff der **Bestandsdaten** nach § 5 TDDSG und § 3 Nr. 3 TKG fallen Daten eines Teilnehmers (Nutzers), die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses erhoben werden. Es handelt sich somit um Basisdaten wie Name, Anschrift und Teilnehmernummer. Diese Daten dürfen ohne Einwilligung erhoben, verarbeitet und genutzt werden, soweit sie für die Erbringung des Dienstes erforderlich sind. Darüber hinaus bedarf es einer Einwilligung. Gemäß § 113 TKG und § 5 S. 2 TDDSG ist die Hochschule auf Anfrage der Strafverfolgungsbehörden in der Regel zur Auskunfterteilung über Bestandsdaten gegenüber den Behörden verpflichtet. Eine Pflicht zur Speicherung bestimmter, über das erforderliche Maß hinausgehender Daten nach § 111 TKG zu Zwecken der

Strafverfolgung besteht im Wesentlichen nur dann, wenn geschäftsmäßig (nachhaltig, unabhängig von einer Gewinnerzielungsabsicht und damit nicht im Sinne von gewerblich zu verstehen) Telekommunikationsdienste erbracht werden und dabei Rufnummern vergeben werden. Aufgrund des Bezugs zu einer (Telefon-) Rufnummer besteht die Pflicht für IP-Adressen oder E-Mailadressen nicht.

**Nutzungsdaten** gem. § 6 TDDSG sind Daten, die erforderlich sind, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen. Dies sind insbesondere Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Teledienste. Die Daten dürfen im Rahmen der Erforderlichkeit ohne Einwilligung zum Zweck der Ermöglichung der Inanspruchnahme von Telediensten und zum Zweck der Abrechnung erhoben, verarbeitet und genutzt werden. **Verkehrsdaten** nach § 3 Nr. 30 TKG sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Hierzu gehören beispielsweise Nummer oder Kennung der beteiligten Anschlüsse, Beginn und Ende der jeweiligen Verbindung und übermittelte Datenmengen. Soweit die Hochschule die Privatnutzung des Internetzugangs und des Mailedienstes zulässt, sind die Vorgaben für Verkehrsdaten in §§ 96 ff. TKG zu beachten. Die Daten dürfen nach Ende der Verbindung nur mit Einwilligung oder für die in §§ 97, 99, 100 und 101 TKG genannten Zwecke verwendet werden. Für den Hochschulbereich sind im Wesentlichen die Befugnisse aus §§ 97 und 100 TKG von Bedeutung. § 97 TKG erlaubt die Verwendung, soweit die Daten zur Ermittlung eines Entgelts und zur Abrechnung mit den Nutzern benötigt werden. Nach § 100 Abs. 1 TKG darf der Diensteanbieter, soweit erforderlich, zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen auch die Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden. Aufgrund des Kriteriums der Erforderlichkeit ist hiervon jedoch zurückhaltend Gebrauch zu machen. Nach § 100 Abs. 3 TKG darf der Diensteanbieter, soweit erforderlich, bei Vorliegen zu dokumentierender tatsächlicher Anhaltspunkte auch die Verkehrsdaten erheben und verwenden, die zum Aufdecken sowie Unterbinden von Leistungserschleichungen und sonstigen rechtswidrigen Inanspruchnahmen des Dienstes erforderlich sind. Eine Pflicht zur Erhebung und Speicherung von Verkehrsdaten besteht grundsätzlich nur unter den Voraussetzungen von §§ 100g, 100h StPO, die eine richterliche Anordnung vorsehen. Unter den gleichen Voraussetzungen ist die Hochschule zur Auskunfterteilung verpflichtet.

Unter das Telekommunikationsgeheimnis fallen vor allem die **Nachrichteninhalte**. Eine Einsichtnahme in Nachrichteninhalte ist tunlichst zu vermeiden. Sollte keine andere Möglichkeit zur Störungsbeseitigung bestehen, ist die Einsichtnahme in jedem Fall zu dokumentieren und der betroffene Nutzer nach Zweckerreichung unverzüglich zu benachrichtigen. Eine Pflicht zur Aufzeichnung und Auskunft über Nachrichteninhalte besteht nur unter den Voraussetzungen von §§ 100a, 100b StPO, die eine richterliche Anordnung vorsehen.

**Hinweis:** Die vorgenannten datenschutzrechtlichen Erlaubnisnormen sind eng auszulegen und erfassen nur die Erhebung und Verwendung zu dem jeweiligen Zweck in dem hierzu erforderlichen Maß und der hierzu erforderlichen Dauer. Die Daten müssen nach Wegfall der Erforderlichkeit bei Fehlen einer abweichenden gesetzlichen Regelung grundsätzlich gelöscht werden. Darüber hinausgehend ist eine Einwilligung erforderlich. Im Zusammenhang mit dem Telekommunikationsgeheimnis ist regelmäßig die Einwilligung aller an dem konkreten Telekommunikationsvorgang Beteiligten erforderlich.

## 2 Haftungsgrundsätze

Gemäß § 8 Abs. 1 TDG sind die Hochschulen für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich. Dies gilt beispielsweise für Inhalte auf der Webseite der Hochschule oder für im Rahmen der Hochschultätigkeit (und damit eigene) übermittelte Informationen. Für fremde Informationen (etwa eine private E-Mail), die über das Kommunikationsnetz der Hochschule übermittelt werden, ist die Hochschule nach § 9 TDG grundsätzlich nicht verantwortlich. Werden fremde (nutzereigene) Informationen gespeichert (z.B. Homepages von Studierenden oder persönliche Laufwerke), ist die Hochschule nach § 11 TDG nicht verantwortlich, sofern sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben (allerdings reicht für Schadenersatz die Kenntnis von Umständen, aus denen dies offensichtlich wird) oder die Hochschule nach Kenntnis unverzüglich tätig geworden ist, um die Information zu entfernen oder den Zugang zu ihr zu sperren. In diesem Zusammenhang ist darauf hinzuweisen, dass die Hochschule nach § 8 Abs. 2 S. 1 TDG **nicht** verpflichtet ist, von ihr übermittelte oder gespeicherte fremde Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

### **3 Verpflichtungen der Nutzer**

- Die Nutzer sind zur Einhaltung der Benutzungsregelungen in einer bestehenden Benutzungsordnung und zur Einhaltung der Gesetze verpflichtet.
- Dies gilt insbesondere für die Beachtung von Urheberrechten und die Unterlassung strafbarer Handlungen im Zusammenhang mit der Nutzung der IT-Ressourcen.
- Im Hinblick auf die Nutzungsordnung gilt dies insbesondere für die Verhinderung des Missbrauchs der Nutzungsberechtigung etwa durch Weitergabe des Passworts an Dritte, die pflegliche Behandlung der technischen Einrichtungen, die Unterlassung von Eingriffen in die Systemkonfiguration und die Meldung sicherheitsrelevanter Ereignisse an das Rechenzentrum.