UNIVERSITÄT SIEGEN

Amtliche Mitteilungen

Datum 8. Dezember 2006 **Nr.** 41/2006

Inhalt:

Ordnung zum Datenschutz

an der Universität Siegen

Vom 6. Dezember 2006

Herausgeber: Rektorat der Universität Siegen
Redaktion: Dezernat 3, Herrengarten 3, 57068 Siegen, Tel. 0271/740-4813

Ordnung zum Datenschutz an der Universität Siegen

Vom 6. Dezember 2006

Aufgrund der §§ 2 Abs. 4, 10 und 22 Abs. 1 Nr. 3 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG) vom 14. März 2000 (GV.NRW. S. 190) zuletzt geändert durch Gesetz vom 21. März 2006 (GV.NRW. S.119), und des § 18 Abs. 3 Satz 3 Nr. 6 ihrer Grundordnung vom 08. Februar 2002 hat die Universität Siegen die folgende Ordnung erlassen:

Inhaltsverzeichnis

1 Einleitung

Diese Ordnung ergeht in Umsetzung der Empfehlungen der Datenschutz-AG vom 20. September 2000 zur Gestaltung des Datenschutzes an der Universität Siegen.
Aufgabe dieser Ordnung ist es, die grundlegenden organisatorischen Maßnahmen zu treffen, welche erforderlich sind, um den Schutz von personenbezogenen Daten sicherzustellen. Sofern notwendig, sind in den Organisationseinheiten weitergehende organisatorische Maßnahmen zu treffen, die in die Datenschutzkonzepte der einzelnen Einheiten aufzunehmen sind.
Technische Maßnahmen werden in dieser Ordnung wegen der hohen Komplexität nicht geregelt. Für sie wird eine zentrale Instanz eingerichtet, die sich ausschließlich mit den technischen Maßnahmen zum Datenschutz befasst und Unterstützung für alle Organisationseinheiten bietet.

Konkrete Verhaltensmaßnahmen zum Schutz personenbezogener Daten in den Organisationseinheiten sind im Anhang geregelt. Sie sind jährlich bzw. bei Bedarf von dem/der behördlichen Datenschutzbeauftragten unter vorheriger Absprache mit dem/der IT-Sicherheitsbeauftragten zu aktualisieren und zu veröffentlichen.

Diese Ordnung gilt für alle Organisationseinheiten und richtet sich an alle Mitglieder und Angehörigen der Universität Siegen sowie alle Nutzerinnen und Nutzer der IT-Struktur der Universität Siegen.

Bestehende und künftige Regelungen der einzelnen Organisationseinheiten sind, soweit sie den Datenschutz betreffende Bestimmungen enthalten, dieser Ordnung anzupassen.

Grundlagen:

- Grundgesetz für die Bundesrepublik Deutschland (GG)
- Bundesdatenschutzgesetz (BDSG)
- Teledienstegesetz (TDG)
- Teledienstedatenschutzgesetz (TDDSG)
- Datenschutzgesetz Nordrhein-Westfalen (DSG NRW)
- Hochschulgesetz (HG)
- Telekommunikationsgesetz (TKG)
- IT-Grundschutzhandbuch des BSI
- Empfehlungen der Datenschutz-AG vom 20. September 2000 zu Gestaltung des Datenschutzes an der Universität Siegen
- Entwurf der „Regelungen zur IV-Sicherheit in der Universität ..." des Arbeitskreises der Leiter Wissenschaftlicher Rechenzentren in NRW (ARNW)
- Dienstvereinbarung über die Einführung und den Betrieb eines Datenverarbeitungs-Kommunikationsnetzes und die Einführung und den Betrieb aller übrigen Datenverarbeitungsgeräte an der Universität Siegen

Begriffe:

Datenschutz

Datenschutz ist der Schutz des/r Einzelnen davor, dass er/sie durch die Verarbeitung personenbezogener Daten in unzulässiger Weise in seinem/ihrem Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner/ihrer Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

Datensicherung

Datensicherung umfasst alle Maßnahmen zur Sicherstellung der informationstechnischen Sicherheit und damit auch des technisch-organisatorischen Datenschutzes.

Datensicherheit

Datensicherheit ist das angestrebte Ergebnis der Maßnahmen zur Datensicherung.

Personenbezogene Daten

Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 DSG NW). Hierzu gehören z. B. Name, Alter, Familienstand, Wohnort, gesundheitliche Verhältnisse, Prüfungsnoten.

Datenverarbeitung

Unter Datenverarbeitung wird das Erheben, Speichern, Verändern, Übermitteln (einschließlich der Gewährung des Zugriffes), Sperren, Löschen (endgültige physische Vernichtung) sowie Nutzen von personenbezogenen Daten verstanden (§ 3 Abs. 2 Satz 1 DSG NW).

Einwilligung

Die Einwilligung ist die widerrufliche, freiwillige und eindeutige Willenserklärung der betroffenen Person, einer bestimmten Datenverarbeitung zuzustimmen. Sie bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die betroffene Person auf die Einwilligung schriftlich besonders hinzuweisen. Sie ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung über die Empfänger der Daten aufzuklären; sie ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass sie die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.
Die Einwilligung kann unter den Voraussetzungen des § 4 Abs. 1 Satz 6 DSG NRW auch elektronisch erstellt werden.

Anonymisieren

Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (§ 3 Abs. 7 DSG NRW).

Pseudonymisieren

Pseudonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Die Daten verarbeitende Stelle darf keinen Zugriff auf die Zuordnungsfunktion haben; diese ist an dritter Stelle zu verwahren (§ 3 Abs. 8 DSG NRW).

2 Organisation des Datenschutzes

2.1 Behördliche/r Datenschutzbeauftragte/r

Gemäß § 32 a DSG NRW haben öffentliche Stellen, die personenbezogene Daten verarbeiten, eine/n interne/n Beauftragte/n für den Datenschutz sowie eine/n Vertreter/in zu bestellen. Der/die Beauftragte muss die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. Er/sie unterstützt die Stelle bei der Sicherstellung des Datenschutzes.
Der/die Datenschutzbeauftragte ist Ansprechpartner/in in allen Fragen des Datenschutzes und berät die datenverarbeitenden Stellen bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten.
Er/sie ist bei der Erarbeitung behördeninterner Regelungen und Maßnahmen zur Verarbeitung personenbezogener Daten frühzeitig zu beteiligen und hat die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen und die mit der Verarbeitung personenbezogener Daten befassten Personen mit den Bestimmungen des Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen.

Der/die Beauftragte ist in seiner/ihrer Eigenschaft als behördliche/r Datenschutzbeauftragte/r der Leitung der öffentlichen Stelle unmittelbar zu unterstellen und in dieser Funktion weisungsfrei. Er/sie darf wegen der Erfüllung seiner/ihrer Aufgaben nicht benachteiligt werden. Während seiner/ihrer Tätigkeit darf er/sie mit keiner Aufgabe betraut sein, deren Wahrnehmung zur Interessenkollision führen könnte.

2.2 Verfahrensverzeichnis

Gemäß § 8 DSG NRW hat jede datenverarbeitende Stelle, die für den Einsatz eines Verfahrens zur automatisierten Verarbeitung personenbezogener Daten verantwortlich ist, ein Verfahrensverzeichnis anzulegen, in dem mindestens die in § 8 Abs. 1 Nr. 1 bis 11 DSG NRW aufgeführten Angaben enthalten sein müssen. Das Verfahrensverzeichnis ist von dem/der Datenschutzbeauftragten zu führen.
Für Dateien, die bereits zum Register des/der Landesbeauftragten für den Datenschutz gemeldet sind, ist das Verzeichnis erstmals bei seit dem 31. Mai 2000 (In-Kraft-Treten des DSG NRW) eintretender Veränderung zu errichten. Die alten Dateibeschreibungen sind dem/der Datenschutzbeauftragten zu übergeben; Meldungen an den/die Landesbeauftragte/n für den Datenschutz erfolgen nicht mehr.
Sofern es für einen einheitlichen Überblick erforderlich ist, sind auch für ältere unveränderte Verfahren Verfahrensverzeichnisse aufzustellen. Die Entscheidung hierüber trifft der/die Datenschutzbeauftragte. Er/sie fordert die datenverarbeitenden Stellen hierzu gesondert auf.
Der/die Datenschutzbeauftragte und die datenverarbeitende Stelle gewähren jeder Person unentgeltlich nach Maßgabe der §§ 8 Abs. 2, 32a Abs. 3 DSG NRW Einsicht in die Verfahrensverzeichnisse.

2.3 Vorabkontrolle für automatisierte Verfahren

Nach § 10 Abs. 3 DSG NRW ist vor der Entscheidung über den Einsatz oder einer wesentlichen Änderung eines automatisierten Verfahrens, eine Vorabkontrolle hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung durchzuführen. Das Verfahren darf nur eingesetzt werden, wenn diese Gefahren nicht bestehen, oder durch technische und organisatorische Maßnahmen im Sinne des § 10 Abs. 1 und 2 DSG NRW verhindert werden können. Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklungen der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen. Die Vorabkontrolle ist Bestandteil des zu dokumentierenden Sicherheitskonzepts und ist aufzuzeichnen.

Zur Durchführung der Vorabkontrolle haben die für die Einführung verantwortlichen Administratoren in Zusammenarbeit mit der datenverarbeitenden Stelle ein Konzept zur Sicherung der personenbezogenen Daten, die in dem einzuführenden Verfahren verarbeitet werden, schriftlich zu erstellen und dem/der behördlichen Datenschutzbeauftragten vorzulegen. Das Konzept muss alle Angaben enthalten, die benötigt werden, um die Vorabkontrolle durchzuführen.

2.4 Datenschutzbericht

Der/die Datenschutzbeauftragte erstellt in regelmäßigen Abständen einen Datenschutzbericht, in dem die Mitglieder der Hochschule zu Fragen des Datenschutzes, die die Hochschule betreffen, informiert werden. Die jährlichen Fortschreibungen der Konzepte der Organisationseinheiten sollten, sofern sich Änderungen ergeben, in den Datenschutzbericht aufgenommen werden.

2.5 Interne Kontrolle

Die interne Kontrolle der Einhaltung dieser Ordnung und sonstiger zum Datenschutz und zur Datensicherheit bestehender Vorschriften und Anweisungen wird von dem/der jeweiligen Leiter/in der Organisationseinheit und dem/der Datenschutzbeauftragten wahrgenommen.
Berichte über Mängel/Feststellungen haben schriftlich zu erfolgen.
Die mit der internen Kontrolle beauftragten Beschäftigten haben im Rahmen ihrer Überwachungsfunktion Zugangsberechtigung zu allen Räumen, insbesondere zu Räumen, in denen DV-Geräte aufgestellt sind.

2.6 Datenschutz-AG

Zur Aufdeckung und Erörterung der datenschutzrechtlichen Probleme der Universität Siegen und zur Erarbeitung von Lösungsmöglichkeiten sowie zur Beratung des/der Datenschutzbeauftragten und der Hochschulleitung ist eine Arbeitsgruppe für den Datenschutz eingerichtet. Diese setzt sich zusammen aus dem/der behördlichen Datenschutzbeauftragten, dem/der Sicherheitsbeauftragten, jeweils einem/r Vertreter/in des Verwaltungsrechenzentrums, des Hochschulrechenzentrums, des Medienzentrums, des nichtwissenschaftlichen Personalrates, des wissenschaftlichen und künstlerischen Personalrates sowie der Universitätsbibliothek. Weitere Mitglieder können bei Bedarf hinzugezogen werden.

2.7 Datenschutzkonzeption in den Einheiten

Die Leiter/innen der Organisationseinheiten haben jeweils für ihren Bereich die Ausführung und Einhaltung dieser Ordnung, die Einhaltung der im Anhang aufgeführten Maßnahmen zum Datenschutz in den Organisationseinheiten in der jeweils aktuellen Fassung sowie die Einhaltung der sonstigen Vorschriften zum Datenschutz sicherzustellen. Sie haben dafür Sorge zu tragen, dass alle Mitglieder und Angehörige, die in der Organisationseinheit arbeiten oder diese nutzen und personenbezogene Daten verarbeiten, Kenntnis vom Inhalt dieser Ordnung, deren Anhang in der jeweils gültigen Fassung und der sonstigen in der jeweiligen Organisationseinheit geltenden Regelungen zum Datenschutz nehmen.
In jeder Organisationseinheit sind Überlegungen darüber anzustellen, welche über diese Ordnung und deren Anhang hinaus gehenden Maßnahmen zur Sicherstellung des Datenschutzes erforderlich sind. Die Leiter/innen sind verpflichtet, diese Überlegungen in detaillierte Datenschutzkonzepte für ihre Bereiche zusammenzufassen und diese umzusetzen. Die Konzepte sind zu dokumentieren und dem/der Datenschutzbeauftragten mitzuteilen. Der/die Datenschutzbeauftragte kann Empfehlungen zur Erstellung der Konzepte herausgeben. Er/sie ist bei der Erarbeitung der Konzepte frühzeitig zu beteiligen.

Die Wirksamkeit der Konzepte ist ständig, mindestens jährlich unter Berücksichtigung sich verändernder Rahmenbedingungen und Entwicklung der Technik zu überprüfen. Das Ergebnis ist zu dokumentieren und dem/der Datenschutzbeauftragten mitzuteilen.
Die in dem nachfolgenden Unterabsatz genannten Maßnahmen sowie die Maßnahmen zum Problem Innentäter (siehe Anhang) sind in die Überlegungen einzubeziehen. Es ist zu begründen, warum im Einzelfall die dort genannten Maßnahmen als nicht erforderlich angesehen werden.

In den Organisationseinheiten sind erforderlichenfalls Ordnungen/Richtlinien und/oder Dienstanweisungen zu erlassen oder Dienstvereinbarungen zu treffen, die zur Regelung des Datenschutzes in dem jeweiligen Bereich erforderlich sind. Hierzu gehören zum Beispiel Regelungen zum Umgang mit personenbezogenen Daten, für die Benutzung der DV-Geräte, zu den Aufgaben der Systemadministratoren sowie die Änderung der Benutzungsordnung SIENET und Nutzungsregelungen des Internets für Studierende und Mitarbeiter/innen.

3 Organisation des IT-Sicherheitsprozesses

Voraussetzung für eine sinnvolle Umsetzung und Erfolgskontrolle von IT-Sicherheitsmaßnahmen ist wegen der Komplexität der Informationstechnik ein durchdachter und gesteuerter IT-Sicherheitsprozess. Wesentliche Teile dieses Prozesses sind die Erstellung eines IT-Sicherheitskonzeptes für die gesamte Hochschule und die Bestellung eines/r IT-Sicherheitsbeauftragten, dessen wichtigste Aufgabe es ist, das IT-Sicherheitskonzept zu errichten und umzusetzen.

3.1 Sicherheitsmanagement

3.1.1 IT-Sicherheitsbeauftragte/r

Die Leitung der Hochschule bestellt eine/n IT-Sicherheitsbeauftragte/n sowie eine/n Vertreter/in. Der/die IT-Sicherheitsbeauftragte muss die erforderliche Sachkenntnis und Zuverlässigkeit besitzen. Er/sie ist in seiner/ihrer Eigenschaft als IT-Sicherheitsbeauftragte/r der Leitung der Hochschule direkt zu unterstellen. Er/sie darf wegen der Erfüllung seiner/ihrer Aufgabe nicht benachteiligt werden.

Zu den Aufgaben des/der IT-Sicherheitsbeauftragten gehören:
- Initiierung, Steuerung und Kontrolle des IT-Sicherheitsprozesses.
- Erarbeitung und Überwachung der Umsetzung eines IT-Sicherheitskonzeptes für die gesamte Hochschule.
- Erstellung eines Realisierungsplans für IT-Sicherheitsmaßnahmen.
- Erarbeitung und Überwachung der Umsetzung einer IT-Sicherheitsrichtlinie.
- Durchführung von IT-Sicherheitsüberprüfungen in den einzelnen Organisationseinheiten zur Kontrolle, ob die im IT-Sicherheitskonzept geplanten IT-Sicherheitsmaßnahmen wie beabsichtigt funktionieren und geeignet und wirksam sind.
- Erarbeitung eines Notfallkonzeptes.
- Aufstellung von Ausbildungs- und Schulungsprogrammen zur IT-Sicherheit für Benutzer/innen, Administratoren und Mitglieder des IT-Sicherheitsteams, die auch die Sensibilisierung für Maßnahmen der Verbesserung der IT-Sicherheit berücksichtigen.
- Ansprechpartner und Beratung der Hochschulleitung, der einzelnen Organisationseinheiten und des/der behördlichen Datenschutzbeauftragten in allen Fragen, die die IT-Sicherheit betreffen.
- Entgegennahme, Dokumentation und Untersuchung aller sicherheitsrelevanter Vorfälle.

- Bereitstellung der technischen Mittel, die für Verschlüsselung, Zertifizierung und digitaler Unterschrift notwendig sind.
- Erarbeitung von Vorgaben zur Protokollierung
- Leitung des IT-Sicherheitsteams

3.1.2 IT-Sicherheitsteam

Zur Unterstützung des/der IT-Sicherheitsbeauftragten wird ein IT-Sicherheitsteam aufgestellt. Das IT-Sicherheitsteam unterstützt den/die IT-Sicherheitsbeauftragte/n bei der Wahrnehmung seiner/ihrer Aufgaben. Die einzelnen Aufgaben sind zu Beginn der Arbeit des IT-Sicherheitsteams festzulegen. Die Geschäftsstelle des IT-Sicherheitsteams sollte beim ZIMT eingerichtet werden. Das IT-Sicherheitsteam und der/die IT-Sicherheitsbeauftagte arbeitet mit dem/der behördlichen Datenschutzbeauftragten, soweit es um den Schutz der personenbezogenen Daten geht, zusammen. Der/die behördliche Datenschutzbeauftragte ist regelmäßig über die Inhalte der Sitzungen des IT-Sicherheitsteams zu unterrichten. Er/sie kann jederzeit an den Sitzungen des IT-Sicherheitsteams teilnehmen.
Der/die IT-Sicherheitsbeauftragte ist Mitglied des IT-Sicherheitsteams. Weitere Mitglieder sollten mindestens ein/e IT-Beauftragte/n und mindestens ein/e Vertreter/in der IT-Benutzer/innen sein.

3.1.3 IT-Beauftragte/r

In den einzelnen Organisationseinheiten ist mindestens ein/e IT-Beauftragte/r zu benennen, der/die Ansprechpartner/in für die IT-Sicherheit ist. Bei der Bestellung der IT-Beauftragten soll darauf geachtet werden, dass diese über eine hohe IT-Kompetenz verfügen und dass die kontinuierliche Wahrnehmung der Aufgaben gewährleistet ist. Sofern organisationsübergreifend elektronische Dienste angeboten werden, kann ein/e IT-Beauftragte/r für die einzelnen Dienste benannt werden.
Der/die IT-Beauftragte hat folgende Aufgaben:

- Umsetzung der IT-Sicherheitsmaßnahmen und der IT-Sicherheitsrichtlinie nach den Vorgaben des IT-Sicherheitsteams.
- Ansprechpartner/in des IT-Sicherheitsteams und der IT-Benutzer/innen vor Ort.
- Meldung von sicherheitsrelevanten Vorfällen an den/die IT-Sicherheitsbeauftragte/n.
- Ermittlung und Weiterleitung des Schulungs- und Sensibilisierungsbedarfs von IT-Benutzern/innen in der jeweiligen Organisationseinheit.

3.2 Erstellung eines IT-Sicherheitskonzepts

3.2.1 Grundlagen

Die Erstellung eines IT-Sicherheitskonzeptes wird für Daten mit mittlerem Schutzbedarf anhand der Grundschutzbetrachtung nach dem IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik vorgenommen.
Für Daten mit hohem Schutzbedarf wird eine Bedrohungs- und Risikoanalyse durchgeführt. Es werden die Bedrohungen für diese Bestände bezüglich Vertraulichkeit, Integrität und Verfügbarkeit ermittelt und analysiert. Für jede Bedrohung werden die damit verbundenen Risiken bestimmt. Daraufhin werden für jede Bedrohung die technischen und organisatorischen Maßnahmen ermittelt, die zur Abwehr der Bedrohung geeignet sind und das verbleibende Restrisiko entsprechend dem Schutzbedarf vertretbar machen. Falls es zur Abwehr ein und derselben Bedrohung mehrere Maßnahmenalternativen gibt, werden die angemessenen Maßnahmen mittels einer Kosten/Nutzen-Analyse bestimmt.
Vor der oben genannten Vorgehensweise ist eine IT-Strukturanalyse und eine Schutzbedarfsfeststellung durchzuführen und zu dokumentieren.

Die Wirksamkeit der getroffenen IT-Sicherheitsmaßnahmen ist fortlaufend mit Blick auf sich wandelnde Bedrohungen, veränderte Rahmenbedingungen der Datenverarbeitung und Entwicklungen der Technik zu überprüfen. Sofern sich Anpassungsbedarf ergibt, sind die notwendigen Änderungen zeitnah umzusetzen. Vorgeschrieben ist eine mindestens jährliche Evaluierung der Konzepte und der Umsetzung.
Auf Sicherheitsvorfälle ist entsprechend zu reagieren.

3.2.2 IT-Strukturanalyse

Die Struktur der Informationstechnologie in der Hochschule ist durch das IT-Sicherheitsteam zu analysieren und zu dokumentieren.

3.2.3 Schutzbedarfsfeststellung

Bei der Erstellung eines IT-Sicherheitskonzepts ist die erste und wichtigste Aufgabe festzustellen, welcher Schutz für die IT-Systeme, IT-Anwendungen und Informationen ausreichend und angemessen ist. Dazu wird der Schutzbedarf ermittelt. Er gibt an, welche möglichen Schäden beim IT-Einsatz entstehen können, und wie wichtig es daher ist, den Eintritt solcher Schäden zu verhindern. Da anhand der Feststellung des Schutzbedarfs über die weitere Vorgehensweise der IT-Sicherheitskonzeption entschieden wird, ist dieser Schutzbedarfsfeststellung große Bedeutung beizumessen. Entsprechend sorgfältig und gründlich muss sie durchgeführt werden. Werden bei der Schutzbedarfsfeststellung bereits Fehler gemacht, so pflanzen sich diese im weiteren Verfahren fort und sind kaum noch zu korrigieren.

3.2.4 Behandlung von Sicherheitsvorfällen

Um die IT-Sicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Sicherheitsvorfällen konzipiert und eingeübt zu haben. Als Sicherheitsvorfall wird dabei ein Ereignis bezeichnet, das Auswirkungen nach sich ziehen kann, die einen großen Schaden anrichten können. Um Schäden zu verhüten bzw. zu begrenzen, muss die Behandlung der Sicherheitsvorfälle zügig und effizient ablaufen. Wenn hierbei auf ein vorgegebenes Verfahren aufgesetzt werden kann, können Reaktionszeiten minimiert werden. Die möglichen Schäden bei einem Sicherheitsvorfall können dabei sowohl die Vertraulichkeit oder die Integrität von Daten als auch die Verfügbarkeit betreffen.

4 Haftung

Wird einer Person durch die unrichtige oder unzulässige Verarbeitung ihrer personenbezogenen Daten durch ein Mitglied oder eine/n Angehörige/n der Universität Siegen ein Schaden zugefügt, so haftet das Mitglied oder der/die Angehörige bei Erfüllung der Haftungsvoraussetzungen des § 84 LBG bzw. § 14 BAT für alle Nachteile, die der Hochschule daraus entstehen.

Auf die §§ 33 und 34 DSG NRW wird hingewiesen.

5 In-Kraft-Treten

Diese Ordnung tritt am Tage nach der Veröffentlichung in dem Verkündungsblatt „Amtliche Mitteilungen der Universität Siegen“ in Kraft. Sie gilt zunächst für die Dauer eines Jahres. Der Senat entscheidet über ihre Fortgeltung.

Ausgefertigt aufgrund des Beschlusses des Senats der Universität Siegen vom 19. Dezember 2005.

Siegen, den 6. 12. 2006

Der Rektor

(Universitätsprofessor Dr. Ralf Schnell)

ANHANG

Maßnahmen zum Datenschutz in den Organisationseinheiten/ Konkrete Maßnahmen zum Schutz personenbezogener Daten

Personenbezogene Daten sind vor unberechtigtem Zugriff zu schützen und gegen jegliche Form des Missbrauchs zu sichern. Missbräuchliche Verarbeitung liegt vor, wenn sie gegen Datenschutzbestimmungen oder andere zum Schutz personenbezogener Daten erlassene Vorschriften verstößt. Die nachfolgend aufgeführten Maßnahmen sind in jeder Organisationseinheit mindestens zu treffen, um den Schutz der personenbezogenen Daten zu gewährleisten.

Die nachfolgend genannten Maßnahmen sind Mindestmaßnahmen, die in allen Organisationseinheiten einzuhalten sind. Sofern im begründeten Einzelfall diese Regelungen nicht eingehalten werden können, können durch die Hochschulleitung Ausnahmen zugelassen werden. Der/die Datenschutzbeauftragte ist vor der Entscheidung zu hören.

1. Zulässigkeit der Datenverarbeitung

Personenbezogene Daten dürfen nur verarbeitet werden, wenn die Verarbeitung durch die Datenschutzgesetze oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder angeordnet ist oder der/die Betroffene eingewilligt hat.
Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.
Wenn die Speicherung der personenbezogenen Daten unzulässig ist oder ihre Kenntnis für die speichernde Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist, sind sie zu löschen.

2. Datenvermeidung

Personenbezogene Daten dürfen nur insoweit erhoben werden, als ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.
Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben und weiterzuverarbeiten. Soweit möglich, sind Verfahren anonym zu gestalten oder Pseudonyme zu verwenden.

3. Schutzmaßnahmen bei automatisierter Verarbeitung personenbezogener Daten

Für Daten bis mittlerer Schutzstufe, z. B. die Anschrift in den Personal- und Studierendendaten, die Daten in UnivIS, Reisekostendaten, Logdaten (Rechner, Netz), Maildaten, Adressdaten, Ausleihdaten, Telefondaten, Schlüsseldaten, Preise, interne Dokumente, Mailinhalte, Forschungsdaten (Drittmittel), Haushaltsmittel (MBS) oder urheberrechtlich geschützte Daten, sind mindestens folgende Schutzmaßnahmen zu ergreifen:

- Der Zugriff darf nur berechtigten Nutzern/innen mittels Passwort ermöglicht werden. Passwörter für administrative Zwecke müssen verschlüsselt übertragen werden.

Bei Daten, deren Schutzstufe hoch bis sehr hoch ist, z. B. Daten der Laufbahn aus den Personaldaten, die Daten zum Studium aus den Studierendendaten, Beihilfedaten, Daten der betriebsärztlichen Vorsorgedatei, personenbezogene Daten für Forschungszwecke, Zeiterfassungsdaten und Fehltage, Prüfungsdaten, personenbezogen Daten in der Forschungs-Transferstelle, sind folgende Schutzmaßnahmen zu ergreifen:

- Die Rechner, auf denen die Dateien verarbeitet werden, sind permanent physikalisch von allen Netzen abzutrennen oder die Daten dürfen auf vernetzten Rechnern nur verschlüsselt abgelegt und übertragen werden.

Die dargestellten Maßnahmen sind Mindestanforderungen, die zur Realisierung des Datenschutzes zu erfüllen sind. Eine umfassende Maßnahmenempfehlung ist wegen der spezifischen Besonderheit jeder datenverarbeitenden Stelle nicht sinnvoll. Die Anwender/innen werden jedoch ausdrücklich darauf hingewiesen, dass es wünschenswert ist, für ihren Bereich weitergehende Schutzvorkehrungen einzurichten.

Dokumente, die sensible Daten enthalten, dürfen nicht allgemein zugänglich sein. Zu beachten ist, dass nicht nur auf die allgemeine Zugänglichkeit der Ablage geachtet werden muss, sondern auch auf die Zugänglichkeit der Drucker, wenn z. B. mehrere Personen einen gemeinsamen Drucker benutzen.
Zur revisionssicheren Archivierung von Dokumenten und zur Einhaltung der vorgeschriebenen Aufbewahrungsfristen sollte eine Software eingesetzt werden, die neben der reinen Archivierung auch auf die Einhaltung der Aufbewahrungsfristen achtet.

4. Zugangsberechtigung und Zugangskontrolle

Räume, in denen personenbezogene Daten verarbeitet werden, und in Räumen mit DV-Ausstattung sind beim - nicht nur kurzzeitigen - Verlassen grundsätzlich zu verschließen. Räume mit mehr als einem Arbeitsplatz sind von der letzten Person, die den Raum verlässt, zu verschließen. DV-Endgeräte sind bei Abschluss der Arbeiten nach vorschriftsmäßiger Programmbeendigung abzuschalten. Bei kurzfristiger Abwesenheit ist der Bildschirmarbeitsplatz softwaremäßig zu sperren.
Benutzer/innen haben dafür Sorge zu tragen, dass bei Darstellung von personenbezogenen Daten auf Bildschirmen und Druckern Unbefugten die Einsicht verwehrt wird.
Das Betreten von Räumen, in denen personenbezogene Daten verarbeitet werden oder sich DV-Geräte befinden, ist nur Berechtigten gestattet.
Reinigungspersonal und Wartungsdienste sind darauf hinzuweisen, dass sie keine Kenntnis von den in ihrem Bereich vorhandenen Daten nehmen dürfen und falls die Kenntnisnahme unumgänglich ist, sie zur Geheimhaltung verpflichtet sind.
Die für die Systeme notwendigen zentralen Komponenten (Server, Hubs, Switch, etc.) sind im System-/Technikraum unterzubringen. Zugangsberechtigt ist nur die Systemadministration. Anderen Personen ist der Zugang nur in Anwesenheit der Systemadministration gestattet.

5. Zugriffsberechtigung

Die Benutzer/innen dürfen nur Zugriff zu den Daten und Programmen erhalten, die sie im Rahmen der (ihnen übertragenen) Aufgaben benötigen. Die Festlegung der Zugriffsberechtigung - unterteilt nach Benutzer/in oder Nutzungsgruppen sowie der Art der Zugriffsberechtigung (Lesen, Schreiben, Löschen, Ausführen) - erfolgt schriftlich durch den/die Leiter/in der Organisationseinheiten. Sofern erforderlich, kann der/die Leiter/in der Organisationseinheit diese Aufgabe auf eine Person innerhalb der Organisationseinheit übertragen. Die Übertragung hat schriftlich zu erfolgen.

Die Einrichtung von Berechtigungen einschließlich der Übernahme der zugewiesenen Zugriffsrechte erfolgt durch die Systemadministration, die eine aktuelle Übersicht über die vergebenen Berechtigungen schriftlich zu führen hat.

6. Benutzungskennwort

Es sind die Voraussetzungen dafür zu schaffen, dass die von den DV-Systemen gebotenen technischen Möglichkeiten des Kennwortschutzes genutzt werden.
Benutzungskennworte müssen mindestens 6-stellig sein und dürfen nicht aus einer zu einfachen Ziffern- und/oder Buchstabenkombination, aus einfach abzuleitenden Begriffen oder leicht zu erratenden Namen (beispielsweise Namen von Angehörigen, Monatsnamen) bestehen. Es sollte möglichst eine Kombination aus Buchstaben und Ziffern ohne erkennbare Gesetzmäßigkeit gewählt werden.
Benutzungskennworte dürfen nur dann eingegeben werden, wenn die Eingabe nicht von Unbefugten beobachtet werden kann.
Es ist unzulässig, das Benutzungskennwort anderen Personen mitzuteilen oder zur Kenntnis gelangen zu lassen. Die Geheimhaltungspflicht gilt auch gegenüber Vorgesetzten und Lehrenden.
Benutzungskennworte sollten nach Möglichkeit nicht aufgeschrieben werden. Falls dies dennoch geschieht, ist dafür zu sorgen, dass keine andere Person die Möglichkeit erhält, diese Aufzeichnung einzusehen.
Um die Vertraulichkeit der Benutzungskennworte zu gewährleisten, sind sie spätestens nach Ablauf der von der Systemadministration festzulegenden Gültigkeitsintervalle (systemabhängig) zu ändern. Die Gültigkeitsintervalle sollen drei Monate nicht überschreiten. Die Änderung des Benutzungskennwortes soll möglichst in unregelmäßigen Abständen erfolgen.
Soweit technisch möglich, sind alle Versuche, sich mittels falscher Benutzungskennworte Zugang zum DV-System zu verschaffen, vom DV-System zu protokollieren. Nach dreimaligem fehlerhaftem Zugangsversuch sollte die Arbeitsstation gesperrt werden. Die Sperre kann nur durch die Systemadministration aufgehoben werden.

7. Nachrichtenübermittlung

Elektronische Nachrichten, die personenbezogene Daten beinhalten (E-Mail), sind zur Wahrung der Vertraulichkeit und Integrität zu verschlüsseln.

8. Aufbewahrung von Datenträgern

Datenträger, die der System- und Datensicherung dienen, sind verschlossen im Datentresor aufzubewahren. Die zuständigen Stellen haben jeweils ein aktuelles Verzeichnis über den zur System- und Datensicherung erforderlichen Datenträgerbestand zu führen.
Kopien wichtiger System- und Anwendungsdateien sind an geeigneter Stelle auszulagern.

9. Löschung, Vernichtung und Entsorgung von Datenträgern

Auf maschinell einsetzbaren Datenträgern (beispielsweise Disketten, Festplatten), die an Herstellerfirmen zurückgehen, verkauft werden sollen oder nicht mehr verwendbar sind, sind noch vorhandene personenbezogene oder vertrauliche Daten physikalisch zu löschen. Hierzu sind die kompletten Datenträger oder zumindest die genutzten Bereiche mit einem bestimmten Muster zu überschreiben. Die Überschreibung darf nicht mit gleichförmigem Muster erfolgen und muss zwei- bis dreimal wiederholt werden. Der zweite Durchlauf ist mit einem zum ersten Durchlauf komplementären Muster durchzuführen, damit möglichst jedes Bit einmal geändert wird. Falls eine physikalische Löschung nicht mehr möglich sein sollte, sind die Datenträger in geeigneter Weise für die Verarbeitung unbrauchbar zu machen. Schreibgeschützte oder nicht mehrfach beschreibbare Datenträger sind ebenfalls zu

vernichten. Sofern möglich, sollte die Vernichtung durch geeignete Vernichtungsgeräte erfolgen.
Ist die Löschung der Daten technisch nur durch die Herstellerfirma möglich, ist eine Weitergabe der Datenträger an diese zulässig, wenn der sichere Transport gewährleistet, eine missbräuchliche Nutzung der Daten ausgeschlossen und ihre unverzügliche vollständige Löschung in oben genannter Weise garantiert wird. Dies ist durch eine schriftliche Vereinbarung mit der Herstellerfirma zu gewährleisten.
Auszusondernde Datenträger sind an die ausgebende Stelle zurückzugeben. Diese sorgt für eine sachgerechte Vernichtung.

10. Pflicht zur Geheimhaltung / Datengeheimnis

Den Personen, die Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren; dies gilt auch nach Beendigung ihrer Tätigkeit. Mit der schriftlichen Erteilung der Zugriffsberechtigung gemäß Ziffer 4.5 ist der/die Zugriffsberechtigte über die Pflicht zur Geheimhaltung aufzuklären. Die Kenntnisnahme von der Pflicht zur Geheimhaltung ist von dem/der Zugriffsberechtigten schriftlich zu bestätigen.

11. Übermittlung von Daten und Auskunftserteilung

Eine Datenübermittlung/-weitergabe an Stellen innerhalb der Hochschule (z. B. innerhalb eines Dezernates oder von Dezernat zu Dezernat oder von einem Dezernat an einen Fachbereich) ist zulässig, wenn dies zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist.

Eine Datenübermittlung/-weitergabe an Behörden oder sonstige öffentliche Stellen ist grundsätzlich nur erlaubt, wenn eine Rechtsvorschrift oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen einzelnen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt oder der/die Betroffene schriftlich eingewilligt hat. Die Auskunft ersuchende Behörde oder sonstige Stelle hat ihr Auskunftsbegehren schriftlich zu begründen. Die Auskunft soll schriftlich erfolgen.

Sollte in dringendem Einzelfall eine fernmündliche Auskunft an eine Behörde oder sonstige öffentliche Stelle notwendig sein, ist hierfür der Dezernent/die Dezernentin oder der/die Leiter/in der Organisationseinheit zuständig. Dieser/diese hat die sachlichen und gesetzlichen Voraussetzungen zu prüfen und über die Auskunft zu entscheiden. Die Entscheidungsgründe sind schriftlich festzuhalten und zu den Akten zu nehmen.
Datenauskünfte an den/die Betroffene/n sollen in der Regel schriftlich erfolgen. Weitergehende Verfahren (z. B. Akteneinsicht etc.) sind durch den Dezernenten/die Dezernentin oder den/die Leiter/in der Organisationseinheit zu entscheiden. Mündliche Datenauskünfte dürfen im Einzelfall nur nach einwandfreier Identifizierung des/der Betroffenen an diese/n gegeben werden. Das Recht der Beschäftigten auf Einsicht in ihre Personalakte bleibt unberührt.
Die Weitergabe von personenbezogenen Daten an Dritte, insbesondere an Privatpersonen, ist ohne schriftliches Einverständnis des/der Betroffenen nicht statthaft.

In Zweifelsfällen ist vor der Entscheidung über die Übermittlung/Weitergabe der Daten der/die behördliche Datenschutzbeauftragte zu hören.

12. Rechte der Betroffenen

Jeder hat das Recht auf :

- Auskunft, Einsichtnahme (§ 18 DSG NRW),
- Widerspruch aus besonderem Grund (§ 4 Abs. 5 DSG NRW),
- Unterrichtung (§§ 12 Abs. 2, 13 Abs. 2 Satz 2, 16 Abs. 1 Satz 2 und 3 DSG NRW),
- Berichtigung, Sperrung oder Löschung (§ 19 DSG NRW),
- Schadensersatz (§ 20 DSG NRW),
- Anrufung des Landesbeauftragten für den Datenschutz (§ 25 Abs. 1 DSG NRW),
- Auskunft aus dem bei dem/der zuständigen behördlichen Datenschutzbeauftragten geführten Verfahrensverzeichnis (§ 8 DSG NRW).

Erforderlichenfalls ist die Durchsetzung dieser Rechte durch geeignete organisatorische und technische Maßnahmen sicher zu stellen. Diese Verfahren sollten so beschaffen sein, dass auf rationelle Weise die Rechtswahrnehmung der Betroffenen rasch umgesetzt wird.

Diese Rechte können auch durch die Einwilligung der betroffenen Person nicht ausgeschlossen oder beschränkt werden.

13. Systemadministration

Zentrale Aufgabe der Systemadministration ist die Sicherstellung eines ordnungsgemäßen Betriebsablaufs. Die Beschreibung der Aufgaben und Abläufe sowie die notwendigen Dokumentationen sind in einem Dienstbetriebshandbuch festzulegen. Soweit erforderlich, sind zusätzliche schriftliche Weisungen der Vorgesetzten zu erteilen. Die in der Systemadministration tätigen Beschäftigten dürfen, soweit sie nicht ausdrücklich zugriffsberechtigt sind, auf Anwendungen oder Dateien der Benutzerinnen und Benutzer nur in besonders begründeten Fällen zugreifen. Jeder Zugriff ist unter Angabe der Gründe zu dokumentieren. Soweit auf Dateien der Benutzerinnen und Benutzer zugegriffen wurde, sind die betroffenen Beschäftigten davon zu unterrichten.
Sofern mehrere Administratoren für einen oder mehrere Server zuständig sind, ist eine klare Aufgabenzuweisung durch eine schriftlich zu dokumentierende Anweisung des/der Leiters/in der Organisationseinheit festzulegen. Es ist sicherzustellen, dass die einzelnen Administratoren/innen nur in dem erforderlichen Umfang Zugriff auf personenbezogene Daten haben. Die Aktivitäten der Systemadministratoren sind zu protokollieren.

14. Wartung / Fernwartung

Wartung sind alle Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Datenverarbeitungssysteme.
Bei Wartungsarbeiten darf nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann.
Eine Wartung durch externe Stellen darf nur aufgrund schriftlicher Vereinbarungen erfolgen. Darin sind die im Rahmen der Wartung notwendigen technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit festzulegen. Die mit den Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.
Bei Wartung durch Externe ist sicherzustellen, dass nur dafür autorisiertes Personal die Wartung vornimmt, alle Wartungsvorgänge während der Durchführung kontrolliert und nach der Durchführung nachvollzogen werden können.
Eine Fernwartung ist in jedem Einzelfall freizuschalten. Während der Fernwartung hat die zuständige Stelle besonders darauf zu achten, dass nur erlaubte Funktionen ausgeführt

werden. Erforderlichenfalls ist die Fernwartung abzubrechen. Soweit möglich, sind technische Ablaufprotokolle zu erstellen und für Kontrollzwecke zu sichern.
Wartungstechniker und sonstige Dritte dürfen grundsätzlich nicht mit den von ihnen eingebrachten Datenträgern arbeiten. Statt dessen stellt die zuständige Stelle erforderlichenfalls Datenträger zur Verfügung, auf die der Inhalt des eingebrachten Datenträgers übertragen werden kann. Kann nur mit den eingebrachten Datenträgern gearbeitet werden, ist vor deren Einsatz eine Virenprüfung vorzunehmen.
Änderungen der Betriebssysteme bzw. systemnaher Software während der Wartung sind erst nach Freigabe zu übernehmen. Die Änderungen sind schriftlich zu dokumentieren.

15. Problem Innentäter/in

Das Problem Innentäter/in besteht neben der Gefahr durch Dritte, z.B. Hacker. Es sind daher Regelungen zu treffen, die die Sicherheit von innen gewährleisten und Maßnahmen zum Umgang mit dem „Problem Innentäter/in" enthalten. Hierzu gehört die Verbesserung der IT-Kompetenz der Mitarbeiter/innen durch entsprechende Schulungen, die Sensibilisierung der Mitarbeiter/innen für IT-Sicherheit, der Aufbau deutlicher und einfacher Sicherheitsstrukturen, die erkennen lassen, wie und mit wem unklare Situationen zu klären sind.