Fachhochschule
Münster University of
Applied Sciences

Amtliche Bekanntmachungen

Herausgegeben vom
Rektor
der Fachhochschule Münster
Hüfferstraße 27
48149 Münster
Fon +49(0)2 51/83-6 40 19

17. Juli 2003
Nr. 31/2003
Seite 383 - 390

Inhalt:

Dienstvereinbarung

Einsatz von elektronischen Schließanlagen und Zugangskontrollsystemen

Zwischen dem Rektor der Fachhochschule Münster, dem Kanzler der Fachhochschule Münster, dem Personalrat der künstlerisch und wissenschaftlich Beschäftigten der Fachhochschule Münster und dem Personalrat der Fachhochschule Münster wird nach § 70 des Landespersonalvertretungsgesetzes (LPVG NW) nachfolgende Dienstvereinbarung zum Einsatz von elektronischen Schließanlagen und Zugangskontrollsystemen geschlossen:

Präambel

Ziel dieser Vereinbarung ist es, beim Einsatz elektronischer Schließanlagen und Zugangskontrollsysteme den Schutz personenbezogener Daten vor unzulässigem Gebrauch und unberechtigtem Zugriff zu gewährleisten. Ziel des Einsatzes der elektronischen Schließ- und Zugangskontrollsysteme ist die Erhöhung der Flexibilität in der Nutzung der Gebäude sowie die Erhöhung der Sicherheit für Personen, Anlagen und Gegenstände in den Gebäuden und beim Zugang zu den Gebäuden der Fachhochschule Münster. Bei Einsatz und Verwaltung elektronischer Systeme wird zugleich die Wirtschaftlichkeit, Flexibilität, Aktualität und Transparenz gegenüber herkömmlichen Systemen erhöht. Eine Kontrolle oder Überwachung des Verhaltens von Mitarbeiterinnen und Mitarbeitern findet, auch wenn dieses technisch möglich wäre, nicht statt.

§ 1
Geltungsbereich

(1) Diese Dienstvereinbarung gilt für alle Gebäude der Fachhochschule Münster.

(2) Diese Dienstvereinbarung gilt für die von den Personalräten vertretenen Beschäftigten der Fachhochschule Münster, unabhängig von der mit ihnen arbeitsvertraglich vereinbarten regelmäßigen Arbeitszeit.

(3) Gesetzliche und tarifvertragliche Vorschriften bleiben unberührt.

(4) Soweit diese Dienstvereinbarung personalvertretungsrechtliche Beteiligungstatbestände nicht erfasst, bleiben die Rechte der Personalräte auf Beteiligung nach den einschlägigen Bestimmungen des LPVG unberührt.

§ 2
Zuständigkeit und Betrieb

(1) Datenverarbeitende Stelle für den Einsatz elektronischer Schließanlagen und Zugangskontrollsysteme ist das Dez. 2 für alle Bediensteten der Hochschule. Die Fachbereiche und sonstigen Einrichtungen der Hochschule dürfen Chips lediglich an Studierende ausgeben, z.B. für die Benutzung der Pools. Nach Absprache mit den Personalräten legt die Verwaltung in Schriftform fest, wo genau die Anlagen installiert, wie sie technisch ausgestattet werden und wer für den ord-

nungsgemäßen Betrieb zuständig ist. Durch technische Vorkehrungen (z. B. Passwörter) ist sicherzustellen, dass nur die mit dem Betrieb betrauten Personen die Anlagen bedienen.

(2) Die anliegende Übersicht (Anlage 1) über die derzeit eingesetzten elektronischen Schließanlagen und Zugangskontrollsysteme wird von der Dienststelle einmal jährlich aktualisiert und den Personalräten unaufgefordert zur Verfügung gestellt.

(3) Die Zutrittsberechtigungen zu einzelnen Gebäuden und Räumen werden nach organisatorischen und arbeitstechnischen Notwendigkeiten vergeben.

(4) Der behördliche Datenschutzbeauftragte wirkt mit bei der Erstellung eines Sicherheitskonzepts gemäß § 10 Abs. 3 Datenschutzgesetzes NRW (DSG NW) und führt die Vorabkontrolle unter Beteiligung der Personalräte durch. Die Ergebnisse dokumentiert der behördliche Datenschutzbeauftragte in einer Stellungnahme zum Datenschutz und zur Datensicherheit (Anlage 2).

(5) Der behördliche Datenschutzbeauftragte prüft die getroffenen technischen und organisatorischen Maßnahmen gemäß § 10 DSG NW und gibt der Dienststelle bei auftretenden Mängeln Anregungen und Empfehlungen zur Abhilfe.

§ 3
Erheben und Verarbeiten von Daten

(1) Die Zutrittsberechtigungen zu einzelnen Gebäuden und Räumen werden in einer Stammdatei der elektronischen Schließanlage bzw. dem Zugangskontrollsystem geführt. Die Stammdatei ist eine Datei im Sinne des DSG NW. Die Einsichtnahme in die Dateien und Protokolle ist nur zur Fehlerbeseitigung und in den in Abs. 2 genannten Fällen zulässig. Die Einsichtnahme ist auf die erforderlichen Daten zu beschränken; eine Verknüpfung von Dateien und Protokollen mit anderen Dateien ist nicht zulässig.

(2) Bestehen konkrete Anhaltspunkte für einen Missbrauch der Schließ- und Zugangssysteme oder besteht der Verdacht eines strafbaren Verhaltens beim Einsatz der Schließ- und Zugangssysteme, kann das Protokoll ausgewertet werden.

(3) Jede Auswertung eines nach Abs. 2 erstellten Protokolls erfolgt unter Beteiligung der Personalräte. Die oder der Datenschutzbeauftragte wird vor der Auswertung über den konkreten Anlass unterrichtet. Eine Weitergabe von Auswertungen an Dritte ist nur zulässig, wenn eine rechtliche Verpflichtung dazu besteht.

(4) Der behördliche Datenschutzbeauftragte unterrichtet die mit der Verarbeitung personenbezogener Daten befassten Personen über die Bestimmungen des DSG NW sowie die sonstigen Vorschriften über den Datenschutz.

(5) Die erhobenen Daten werden nach sieben Tagen gelöscht.

§ 4
Dynamisierungsklausel, Konfliktregelung und Verstöße gegen diese Dienstvereinbarung

(1) Bei Planungen hinsichtlich neuer oder zu ändernder elektronischer Schließanlagen und Zugangskontrollsysteme wird von Dienststelle und Personalräten gemeinsam überprüft, ob die geltenden Bestimmungen zum Daten- und Persönlichkeitsschutz eingehalten sind.

(2) Will die Dienststelle von den vereinbarten Grundsätzen abweichen, oder macht der betreffende Personalrat geltend, dass Abweichungen von diesen Grundsätzen zu erwarten sind, so wird hierüber mit dem Ziel einer einvernehmlichen Regelung verhandelt. Diese Regelung wird neuer Bestandteil der Dienstvereinbarung.

(3) Verstöße gegen diese Dienstvereinbarung werden umgehend abgestellt.

(4) Die Dienststelle und die Personalräte verpflichten sich, bei Streitigkeiten, die Auslegung und Anwendung dieser Dienstvereinbarung betreffen, unverzüglich Verhandlungen mit dem Ziel einer einvernehmlichen Regelung aufzunehmen.

(5) Ist über einzelne Fragen der Auslegung dieser Dienstvereinbarung kein Einvernehmen zu erzielen, so wird die Einigungsstelle angerufen. Die Einigungsstelle besteht aus zwei Vertreterinnen oder Vertretern der Dienststelle und zwei der Personalräte sowie der oder dem Vorsitzenden der Einigungsstelle. Die oder der Vorsitzende der Einigungsstelle wird in gegenseitigem Einvernehmen bestellt.

(6) Bis zu einer Entscheidung durch die Einigungsstelle darf eine beabsichtigte Maßnahme nicht vorgenommen werden. Die Einigungsstelle ist angerufen, sobald eine der beiden Vertragsparteien dies schriftlich fordert. Der Spruch der Einigungsstelle ersetzt die einvernehmliche Einigung.

§ 5
Inkrafttreten, Kündigung, Weitergeltung

(1) Diese Dienstvereinbarung tritt am Tag nach der Amtlichen Bekanntmachung in Kraft.

(2) Die Dienstvereinbarung kann einvernehmlich geändert werden. Änderungen bedürfen der Schriftform.

(3) Die Dienstvereinbarung kann von jeder Vertragspartei mit einer Frist von drei Monaten zum Ende eines Kalenderjahres gekündigt werden. Die Kündigung bedarf der Schriftform.

(4) Nach Eingang der Kündigung sind unverzüglich Verhandlungen über eine neue Dienstvereinbarung aufzunehmen.


Münster, den 30.6.2003

Der Rektor
der Fachhochschule Münster
für die Dienststelle

Münster, den 30.06.2003

Der Kanzler
der Fachhochschule Münster
für die Dienststelle

Münster, den 11.07.2003

Der Personalrat der
wissenschaftlich und
künstlerisch Beschäftigten
der Fachhochschule Münster

Münster, den 11.07.2003

Der Personalrat
der Fachhochschule Münster

Anlage 1 zur Dienstvereinbarung Schließanlagen

An folgenden Türen werden elektronische Schließanlagen eingesetzt:

Stand: 01.07.2003

Steinfurt:

Stegerwaldstr.

Bauteil A	Raum 163a (Postraum)
Bauteil B	Raum 200 (FB 4, PC-Pool)
	Raum 201 (FB 4, PC-Pool)

Münster:

Hüfferstift

Untergeschoss	Eingang Hofseite
Erdgeschoss	Eingang Hüfferstr.
	Raum 0.01 (Hausmeisterraum)
4. Obergeschoss	Raum 4.14 (Gästezimmer)

Leonardo-Campus

Gebäude 5	Hauseingangstür
	Raum 110.108 (FB 5, Stud.-Arbeitsplätze)
	Raum 110.109 (FB 5, Stud.-Arbeitsplätze)
	Raum 110.112 (FB 5, Stud.-Arbeitsplätze)
	Raum 110.114 (FB 5, Stud.-Arbeitsplätze)

Protokoll
über die Vorabkontrolle der Dienstvereinbarung über den Einsatz elektronischer Schließanlagen und Zugangskontrollsystemen

Am 10.04.2003 fand die nach dem Datenschutzgesetz-NW vorgesehene Vorabkontrolle statt.

Teilnehmer waren: Herr Winkler, Dezernat 2
Herr Tolksdorf, Dezernat 2
Herr Hansen, Dezernat 2
Herr Overmann, PR
Herr Espelage, PR-Wiss.
Herr Schmidtke als stellvertretender Datenschutzbeauftragter
Herr Lange als Datenschutzbeauftragter

Einhalten des Datenschutzes aus rechtlicher Sicht:

Die datenverarbeitende Stelle für den Einsatz elektronischer Schließanlagen und Zugangskontrollsystemen ist die Fachhochschule Münster, Dezernat 2, für alle Bediensteten der Hochschule. Die Fachbereiche und sonstigen mit Lehraufgaben betrauten Einrichtungen der Hochschule dürfen Chips lediglich an Studierende ausgeben z.B. für die Benutzung der Pools.

Rechtsgrundlage für die Einführung elektronischer Schließanlagen und Zugangskontrollsysteme ist das Eigentums- oder Hausrecht der Hochschule.

Die gespeicherten Daten bestehen aus dem Namen des Bediensteten, der Zuordnung des Chips zu diesem Namen, der Kennzeichnung der Räumlichkeit, für die der Chip genutzt werden kann und dem Erfassen des Zeitpunktes des Öffnens eines Raumes (nicht des Verlassens). Der Öffnungschip kann auch so programmiert werden, dass die Zutrittsmöglichkeit auf bestimmte Zeiten beschränkt wird (z.B. für Gäste der Fachhochschule, die das Gästezimmer benutzen).

Es erfolgt grundsätzlich nur eine Erhebung und Protokollierung der Daten, jedoch keine Regelverarbeitung. Eine Einsichtnahme in die Protokolldaten ist auf die Behebung von Fehlfunktionen und Fehlern des Systems zulässig.

Es wurde eingehend erörtert, unter welchen Voraussetzungen die Personalräte Einsicht in die Protokolle erhalten.
Erörtert wurde auch, dass die Bestimmung des § 3 Abs. 2 der Dienstvereinbarung im Hinblick auf das verfassungsrechtliche Bestimmtheitsgebot rechtlich nicht unbedenklich ist, weil nicht näher konkretisiert ist, wann ein Ausnahmefall bei sicherheits- oder betriebstechnisch relevanten Ereignissen und bei besonderen Vorkommen strafrechtlicher Relevanz vorliegt.

Es wird nach Diskussion vorgeschlagen, § 3 der Dienstvereinbarung wie folgt abzufassen bzw. zu ändern:

(1) Die Zutrittsberechtigungen zu einzelnen Gebäuden und Räumen werden in einer Stammdatei der elektronischen Schließanlage bzw. dem Zugangskontrollsystem geführt. Die

Stammdatei ist eine Datei im Sinne des DSG NW. Die Einsichtnahme in die Dateien und Protokolle ist nur zur Fehlerbeseitigung und in den in Abs. 2 genannten Fällen zulässig. Die Einsichtnahme ist auf die erforderlichen Daten zu beschränken; eine Verknüpfung von Dateien und Protokollen mit anderen Dateien ist nicht zulässig.

(2) Bestehen konkrete Anhaltspunkte für einen Missbrauch der Schließ- und Zugangssysteme oder besteht der Verdacht eines strafbaren Verhaltens beim Einsatz der Schließ- und Zugangssysteme kann das Protokoll ausgewertet werden.

(3) Jede Auswertung eines nach Abs. 2 erstellten Protokolls erfolgt unter Beteiligung der Personalräte. Der Datenschutzbeauftragte wird vor der Auswertung über den konkreten Anlass unterrichtet. Eine Weitergabe von Auswertungen an Dritte ist nur zulässig, wenn eine rechtliche Verpflichtung oder eine sonstige Ermächtigung dazu besteht.

Anschließend wurde erörtert, wie lange die erhobenen Daten gespeichert sein bzw. wann sie gelöscht werden sollen. Die Dienstvereinbarung selbst enthält keine unmittelbare Regelung. Nach kurzer Diskussion ist man sich einig, dass eine Speicherung von sieben Werktagen ausreichend ist, um entscheiden zu können, ob konkrete Anhaltspunkte für einen Missbrauch oder sogar eines strafbaren Verhaltens vorliegen.

Es sollte folgende Regelung in die Dienstvereinbarung aufgenommen werden:

Die erhobenen Daten bleiben sieben Tage gespeichert und werden anschließend gelöscht.

Diese Ergänzung sollte als Abs. 5 in den § 3 der Dienstvereinbarung eingefügt werden.
Die Bediensteten der Hochschule sollen durch ein Informationsschreiben über den Einsatz des digitalen Zugangs- und Kontrollsystems informiert werden. Es ist weiterhin beabsichtigt, entsprechende Richtlinien zu erarbeiten.

Es besteht die Möglichkeit, dass Betroffene auf Antrag Einsicht in die über sie protokollierten Daten nehmen können.

Die Gefahr unberechtigter Zugriffe auf die Protokolle und Daten wird von den Anwesenden als gering eingeschätzt, weil die Daten - Erfassen von Öffnen von Räumen - kaum von wirtschaftlichem oder sonstigem Interesse für Dritte sein können.

Es ist zwar möglich, dass anhand eines Verfolgens von Öffnen der Türen mittels digitaler Zugangssysteme ein Verhaltensprofil erstellt wird; es handelt sich jedoch nur um ein grobes und nicht um ein Detailprofil, welches geeignet wäre, das Verhalten der Nutzer so zu erfassen, dass von einem Eingriff in die Persönlichkeitssphäre gesprochen werden könnte.

Insgesamt ist festzustellen, dass - bei Umsetzung der Empfehlungen für die Ergänzung und Änderung der Dienstvereinbarung - gegen die Einführung des digitalen Zugangs- und Kontrollsystems aus datenschutzrechtlicher Sicht keine Bedenken bestehen.

Stellungnahme aus technischer Sicht:

Für den Datentransfer zwischen dem Schließanlagenserver und den Clients wird das LAN der Fachhochschule genutzt. Innerhalb dieses Netzes wird ein VLAN (virtuelles LAN) die Datensicherheit nach dem heutigen Stand der Sicherheitsrichtlinien gewährleisten. Die Clientarbeitsstationen zur Programmierung des Servers bilden mit diesem ein privates Netzwerk, das keinen öffentlichen Zugang hat. Aus diesem Grund sollten die Clients keinen Internetzugang haben. Physikalisch werden die Clients und der Server über Switches verbunden, bei denen nur bestimmte Ports für dieses VLAN freigegeben sind.
Der Server und die Clients sollten gegen Stromausfall abgesichert werden.
Zu empfehlen sind hierfür unterbrechbare Stromversorgungen (USV), die an das Notstromversorgungssystem der Fachhochschule angeschlossen werden.

Münster, im April 2003

gez. Lange	gez. Schmidtke
Heinz-Dieter Lange	Dipl.-Ing. Klaus-Dieter Schmidtke
Datenschutzbeauftragter	Vertreter des Datenschutzbeauftragten