AMTSBLATT
MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG

24. Jahrgang, Nr. 9 vom 9. Dezember 2014, S. 11

Kanzler

Dienstvereinbarung über die Nutzung von elektronischen Schließanlagen und Zugangskontrollsystemen an der Martin-Luther-Universität Halle-Wittenberg zwischen der Dienststelle Martin-Luther-Universität Halle-Wittenberg und dem Personalrat

vom 08.10.2014

§ 1
Zielsetzung und Allgemeines

(1) Ziel dieser Vereinbarung ist es, beim Einsatz von elektronischen Schließ- und Zugangskontrollsystemen den Schutz personenbezogener Daten vor unzulässigem Gebrauch und unberechtigtem Zugriff zu gewährleisten. Die technisch-organisatorischen Grundsätze zum Einsatz der oben genannten Systeme sind in der Schließordnung der Martin-Luther-Universität Halle-Wittenberg - Anlage 1 - (im folgenden SOMLU) geregelt.

(2) Ziel des Einsatzes der elektronischen Schließ- und Zugangskontrollsysteme ist ausschließlich die Erhöhung der Sicherheit für Personen, Betriebsabläufe und Gegenstände in den Gebäuden und beim Zugang zu den Gebäuden der Martin-Luther-Universität Halle-Wittenberg.

(3) Durch elektronische Schließanlagen und Zugangskontrollsysteme werden personenbezogene Daten erfasst. Dies sind Stammdaten, die zum Systembetrieb notwendig sind. Die Stammdaten umfassen folgenden Datensatz: Name / Vorname, Geburtsdatum, Struktureinheit, elektronische Identität je nach Schließsystem Transponder oder Chipkarte) Darüber hinaus werden, wenn technisch möglich und erforderlich, sogenannte Protokolldaten erfasst. Diese umfassen (teils systemabhängig) folgende Daten: Ident-Merkmal (Karte bzw. Transponder mit Nummer, Datum, gegebenenfalls Erfolgs / Fehlermeldung) zum Öffnen/Betätigen des elektronischen Schließmechanismus.

(4) Eine Leistungs- oder Verhaltenskontrolle findet nicht statt. Personenbezogene oder personenbeziehbare Daten, die für eine Leistungs- oder Verhaltenskontrolle (z. B. Anwesenheits- oder Bewegungsprofile) geeignet sind, dürfen nicht ausgewertet, in andere Systeme übertragen oder in sonstiger Weise dafür verwandt werden, individuelle Eigenschaften mit Anforderungsprofilen zu vergleichen.

(5) Die Dienststelle verpflichtet sich, die Bestimmungen zum Datenschutz einzuhalten.

(6) Eine Verknüpfung der Protokolldaten der elektronischen Schließ- und Zugangskontrollsysteme bzw. der von dort gelieferten Daten mit anderen IT-Systemen ist nicht zulässig.

§ 2
Geltungsbereich

(1) Der räumliche Geltungsbereich dieser Dienstvereinbarung umfasst alle Bereiche der Martin-Luther-Universität Halle-Wittenberg und deren Einrichtungen.

(2) Die Dienstvereinbarung gilt für alle Beschäftigten der Martin-Luther-Universität Halle-Wittenberg und deren Einrichtungen.

§ 3
Mitbestimmung/Rechte des Personalrates

(1) Diese Dienstvereinbarung regelt das Verfahren zur Nutzung elektronischer Schließ- und Zugangskontrollsysteme an der Martin-Luther-Universität Halle-Wittenberg. Die Erweiterung elektronischer Schließ- und Zugangskontrollsysteme sowie die Einrichtung weiterer solcher Systeme unterliegen der Mitbestimmung. Der jeweilige Ausrüstungsstand der Martin-Luther-Universität Halle-Wittenberg ist gemäß der SO-MLU dokumentiert.

(2) Zu seiner Information hat der Personalrat das Recht, an Besprechungen teilzunehmen, die aus Anlass beabsichtigter Änderungen der elektronischen Schließ- und Zugangskontrollsysteme durchgeführt werden.

(3) Der Personalrat hat im Rahmen seiner allgemeinen Aufgaben ein Informations- und Überwachungsrecht bezüglich der Einhaltung dieser Dienstvereinbarung. Der dazu erforderliche Zugang zu den entsprechenden Systemen und die erforderlichen Informationen sind nach vorheriger Absprache zu gewähren. Die Hochschulleitung ist verpflichtet, dem Personalrat alle Informationen und Kenntnisse, die sich aus dem Betreiben des Systems ergeben bzw. die zum Betreiben des Systems notwendig sind, zur Verfügung zu stellen. Details der Nutzung und Ansprechpartner regelt die SO-MLU.

(4) Der Personalrat erhält von der Dienststelle eine aktuelle Liste der zentralen- und Bereichsadministratoren der Schließsysteme.

§ 4
Datenerhebung und -auswertung

(1) Die Zutrittsberechtigungen zu einzelnen Gebäuden und Räumen werden in elektronischer Form entsprechend der Architektur der jeweiligen Schließanlage geführt (u.a. Schließplan). Die Datenstrukturen und der Datenumfang sind in der Systemdokumentation beschrieben. Diese Stammdaten sind vor unbefugter Einsichtnahme zu schützen. Details sind im Verfahrensverzeichnis beschrieben.

(2) Die Beschäftigten, die im Rahmen ihrer Tätigkeit Zugriff auf diese Daten haben (lesend und schreibend), sind in der SO-MLU benannt und bei der Dienststelle hinterlegt.

(3) Das Auslesen und Auswerten der Protokolldaten der elektronischen Schließ- und Zugangskontrollsysteme ist nur aus besonderem Anlass (wie z. B. Störung, Havarie, oder Fehlfunktion) erlaubt.

(4) Die Befugnisse der in Abs. 2 genannten Personen regelt die SO-MLU.

(5) Alle aufgezeichneten Protokolldaten (sofern überhaupt technisch möglich) einschließlich etwaiger Kopien werden maximal 30 Tage vorgehalten und dann gelöscht. Sollten sie zur Aufklärung/Beweissicherung von konkreten Vorkommnissen (z. B. Einbruch/Diebstahl) weiterhin benötigt werden, so sind der bzw. die Datenschutzbeauftragte und der Personalrat zu informieren. Ausgenommen davon sind die Protokollinformationen auf den elektronischen Schließzylindern, wo eine automatisierte Löschung technisch nicht möglich ist.

§ 5
Rechte und Pflichten der Beschäftigten

Die Beschäftigten sind für den bestimmungsgemäßen Gebrauch ihrer elektronischen Schlüssel verantwortlich. Die Schlüssel (Transponder und/oder Chipkarte) dürfen nicht an Unbefugte weiter gegeben oder benutzt werden, um Unbefugten den Zutritt/Zugang zu ermöglichen. Details dazu regelt die SO-MLU.

§ 6
Inkrafttreten und Geltungsdauer

(1) Diese Dienstvereinbarung tritt einen Tag nach ihrer Veröffentlichung im Amtsblatt der Martin-Luther-Universität Halle-Wittenberg in Kraft.

(2) Die Dienstvereinbarung gilt für ein Jahr. Sie verlängert sich um jeweils ein weiteres Jahr, wenn sie nicht von einer der Vereinbarungsparteien mit einer Frist von 3 Monaten zum Ende des Jahres schriftlich gekündigt wird.

(3) Bis zum Abschluss einer neuen Dienstvereinbarung gilt diese Vereinbarung weiter.

Halle (Saale), 8. Oktober 2014

Horst-Dieter Foerster
Amt. Kanzler

Bertolt Marquardt
Personlrat

Anlage zur Dienstvereinbarung über die Nutzung von elektronischen Schließanlagen und Zugangskontrollsystem an der Martin-Luther-Universität Halle-Wittenberg

Schließordnung für die digitalen Türöffnungs-und Schließsysteme an der Martin-Luther-Universität Halle-Wittenberg

vom 08.10.2014

Im Rahmen der umfassenden Sanierung der universitären Gebäude werden für die meisten Gebäude moderne, vernetzte digitale Schließanlagen installiert. Zusätzlich oder ausschließlich können ausgewählte Türen (vorwiegend Außentüren und Türen in Funktionalbereichen) mit einem Türöffnungssystem ausgestattet werden, bei dem die Türen mit der Mitarbeiterkarte, dem Bibliotheksausweis in Chipkartenform oder dem Studierendenausweis in Chipkartenform zu öffnen sind. Eine aktuelle Übersicht der mit digitalen Schließsystemen ausgerüsteten

Gebäude und eine Übersicht der Türen, die mit Chipkarte zu öffnen sind, ist auf entsprechenden Webseiten des ITZ dokumentiert.

1.
Geltungsbereich

Die nachstehende Schließordnung gilt für alle universitären Gebäude, bei denen eine digitale Schließ- oder Öffnungsanlage bereits installiert ist oder die in Zukunft mit solchen Systemen ausgestattet werden. Sie regelt u. a. die Verantwortlichkeiten, Grundsätze der Administration und die Ausgabe und Rücknahme von digitalen Schlüsseln, den sogenannten Transpondern.

2.
Transponderverwaltung

Organisatorisch verantwortlich für die ordnungsgemäße bereichsbezogene Transponderverwaltung sind die Hausbeauftragten gemäß § 2 (3) Ziffer 1-3 der Hausordnung der Martin-Luther-Universität Halle-Wittenberg (ABl. 2000, Nr. 6, S. 46), der Kanzler, die Dekane bzw. Leiter der zentralen Einrichtungen für die ihnen zur Nutzung zugewiesenen jeweiligen Einrichtungen (im weiteren Leiter der Einrichtung).

Das Rektorat wird auf Vorschlag der Leiter der Einrichtungen einen hauptverantwortlichen Administrator (im weiteren Administrator) nebst Stellvertretung für die jeweilige Schließanlage bestellen. Die Bestellung durch das Rektorat gilt bis auf Widerruf.

Die Hausbeauftragten können sich bei der Ausübung des Hausrechtes über die Transponderverwaltung durch andere Mitarbeiter (z. B. Institutsdirektoren, Referatsleiter etc.) vertreten lassen. Den Leitern der Einrichtung bzw. ihren Vertretern obliegt es, für ihren Bereich jeweils transponderverantwortliche Bereichsadministratoren (im weiteren Bereichsadministrator) zu benennen, die für die Programmierung, die Transponderaushändigung und Transponderrücknahme sowie für die Pflege der entsprechenden (elektronischen) Dokumentation innerhalb des Bereiches zuständig sind und die operative Verantwortung tragen. Die Bestimmung eines Vertreters im Krankheits- oder Urlaubsfall obliegt den Bereichsadministratoren im Einvernehmen mit dem Leiter der Einrichtung. Die Bestellung durch den Leiter der Einrichtung gilt bis auf Widerruf. Die Bestellung/Abbestellung ist dem Kanzler zu melden.

3.
Verwaltung des Türöffnungssystems mit Universitätschipkarte

Vom Begriff der Universitätschipkarte werden folgende Karten umfasst:

- Personalkarte,
- Studentenausweis,
- elektronischer Bibliotheksausweis für externe Bibliotheksnutzer.

Das Türöffnungssystem mit der Universitätschipkarte wird ebenfalls durch den vom Rektor bestellten hauptverantwortlichen Administrator aus dem Bereich des ITZ (siehe Ziffer 2, Abs. 2) betreut. Diesem obliegt damit die organisatorische Verantwortung der Verwaltung der zulässigen Universitätschipkarten und der allgemeinen Regelungen zur Türöffnung. Auf Antrag einer Einrichtung kann die Verwaltung einzelner Türen in die Hoheit von Hausbeauftragten übergeben werden. Den Hausbeauftragten bzw. ihren Vertretern obliegt es, für ihren Bereich den jeweils verantwortlichen Administrator für die Universitätschipkarten zu benennen. Die Zutrittsregelungen zu den einzelnen Türen werden über die Webseiten des ITZ veröffentlicht.

Die Ausgabe der Chipkarten regelt sich über die einzelnen Hauptanwendungen: Studierendenausweis (über ZUV/Abteilung 1), Personalkarte/Zeiterfassung (über ZUV/Abteilung 3) und der ULB (Gästeausweis für externe ULB-Nutzer).

4.
Aufgaben des Administrators / Bereichsadministrators für die digitalen Schließsysteme

4.1.
Aufgaben im Zusammenhang mit dem Türöffnungssystem mittels Transponder

Der Administrator ist zuständig für die IT-Infrastruktur seines/seiner Verwaltungsarbeitsplatzes/plätze im Bereich des jeweiligen Schließsystems, die Klärung bereichsübergreifender Fragen sowie Ansprechpartner gegenüber dem Systemhersteller bzw. dem Lieferanten und den Bereichsadministratoren.

Die Bereichsadministratoren sind zuständig für die Verwaltung der dem Bereich zugeordneten Türen (i. d. R. durch eine Software) und der Transponder. Die Bereichsadministratoren führen den Nachweis über die Ausgabe von Transpondern und sind Ansprechpartner für Mitarbeiter des jeweiligen Zuständigkeitsbereiches. Der Verlust eines Transponders ist umgehend dem Bereichsadministrator anzuzeigen und zu dokumentieren. Die Bereichsadministratoren sind für den Ersatz von verlustigen (oder gegebenenfalls defekten) Transpondern zuständig.

4.2.
Aufgaben des/der Administrators(en) für das Türöffnungssystem mittels Universitätschipkarte

Der Administrator ist zuständig für die komplette zentrale Infrastruktur des Öffnungssystems (Hard-und Software), die Klärung aller bereichsübergreifender Fragen sowie Ansprechpartner gegenüber dem Systemhersteller bzw. dem Lieferanten und den jeweiligen Hausbeauftragten. Einzelne Türen oder Türgruppen können bei Bedarf durch die Bereiche selbst administriert werden.

Die Bereichsadministratoren sind dabei zuständig für die Verwaltung der dem Bereich zugeordneten Türen (i. d. R. durch eine Software). Diese können jede einzelne Mitarbeiter / Studierenden / Bibliothekschipkarte zulassen oder sperren. Die Bereichsadministratoren führen den Nachweis über die von ihnen vergebenen Berechtigungen und sind Ansprechpartner für Mitarbeiter des jeweiligen Zuständigkeitsbereiches. Sie klären dabei für alle in ihrem Zuständigkeitsbereich befindlichen Türen die allgemeinen Öffnungsregeln (z. B. Zeitfenster der Öffnung usw.)

Der Verlust einer Universitätschipkarte ist umgehend dem ITZ (in seiner Funktion als Administrator des gesamten Universitätschipkartensystems der MLU) anzuzeigen und zu dokumentieren, da die Universitätschipkarten neben der Türöffnungsfunktion noch viele weitere Funktionen erfüllen und eine Sperrung auch in anderen Funktionalbereichen der Universitätschipkarte notwendig ist (siehe entsprechende Webseiten des ITZ).

4.3.
Datengeheimnis

Alle Administratoren und Bereichsadministratoren von digitalen Schließsystemen sind nach § 5 des Landesdatenschutzgesetzes auf das Datengeheimnis zu verpflichten.

5.
Empfangsberechtigung für Transponder

Die Bereitstellung von Transpondern erfolgt auf der Basis von schriftlichen Anträgen im Rahmen der dienstlichen Notwendigkeit. Sie sind den Leitern der Einrichtung oder der von ihnen beauftragten Personen zur Entscheidung vorzulegen und von dort an den Bereichsadministrator zur weiteren Veranlassung weiter zu leiten. Die Ausgabe von Transpondern und die Zutrittserlaubnis für bestimmte Räume erfolgt personenbezogen im Rahmen der dienstlichen Notwendigkeit.

Zugangsberechtigte zu mindestens einem Raum erhalten automatisch die Zutrittsberechtigung für die Eingangstüren zu dem jeweiligen Gebäude. Das dazu notwendige Antragsformular (mit Empfangsbescheinigung) wird über die Webseiten des ITZ bereitgestellt.
Eine Änderung dieser Berechtigung kann ausschließlich durch den zuständigen Leiter oder von ihm beauftragter Personen der Einrichtung veranlasst werden. Dies kann z. B. dann der Fall sein, wenn der Berechtigte den Transponder unberechtigt an Dritte zur Nutzung weiter gibt oder in sonst einer Weise unsachgemäß handelt (z. B. gültige Sicherheitsvorschriften missachtet).

6.
Ausgabe und Pflichten nach Erhalt eines Transponders

Die Transponderausgabe erfolgt generell nur gegen persönliche Unterschrift des Empfängers auf der Empfangsbestätigung. Das vollständig ausgefüllte Antragsformular muss dem Bereichsadministrator vorab im Original vorliegen.

Mit der Unterschrift des Empfängers eines Transponders werden die Bedingungen dieser Schließordnung und gegebenenfalls weiterer orts- und aufgabenbezogener Sicherheitsordnungen (z. B. in Laboren) anerkannt. Auf die speziellen orts- und aufgabenbezogenen Sicherheitsordnungen ist der Antragsteller ausdrücklich hinzuweisen.

Der Inhaber des Transponders ist verpflichtet, diesen sorgfältig gegen den Zugriff von Dritten gesichert aufzubewahren und vor Verlust zu schützen. Eine Weitergabe an Dritte ist nicht gestattet. Bei Zuwiderhandlungen kann der Transponder eingezogen werden. Jeder Inhaber eines Transponders einer digitalen Schließanlage ist für die ihm über die erteilte Schließberechtigung zugeordneten Räume hinsichtlich der Gewährleistung der Verschlusssicherung und für den ordnungsgemäßen Gebrauch des Transponders verantwortlich. Er haftet bei vorsätzlichem oder grob fahrlässigem Gebrauch des erhaltenen Transponders und trägt die Folgen, die sich aus dem Verlust des Transponders ergeben.

7.
Verfahren und Haftung bei Verlust des Transponders

Der Verlust eines Transponders ist unverzüglich schriftlich (E-Mail, Fax oder Brief) an den Bereichsadministrator zu melden. Dieser sperrt den verlustig gegangenen Transponder sofort, um eine unberechtigte Nutzung auszuschließen. Bei Verlust eines Transponders fallen Ersatzkosten in Höhe der Materialersatzkosten an.

Für Schäden infolge einer verspäteten Verlustmeldung kann der Inhaber bei grobfahrlässigem Verhalten zur Haftung herangezogen werden.

Werden als verloren gemeldete Transponder wieder gefunden, sind diese unverzüglich an den zuständigen Bereichsadministrator zurück zu geben. Die gegebenenfalls gezahlten

Materialersatzkosten werden im Falle der Funktionstüchtigkeit des Transponders zurück erstattet.

8.
Rückgabe der Transponder

Die Transponder sind Eigentum der Universität. Bei Umzug in andere Diensträume, Ausscheiden aus dem Beschäftigungsverhältnis, Beurlaubung oder Freistellungen sonstiger Art sind alle dienstlich erhaltenen Transponder an den Bereichsadministrator zurück zu geben. Die Rückgabe hat spätestens am letzten Arbeitstag zu erfolgen und wird aktenkundig bestätigt. Ausnahmen sind in begründeten Einzelfällen möglich und können durch die Leitung der Einrichtung genehmigt werden.

9.
Beschaffung von Transpondern

Die Bereiche erhalten eine an der Personalstärke angepasste Erstausstattung mit Transpondern. Transpondernachforderungen, die über die Grundausstattung hinausgehen, sind über den jeweiligen Bereichsadministrator anzumelden und aus den Mitteln der bestellenden Einrichtungen zu finanzieren.

10.
Datenschutz

Alle einschlägigen Bestimmungen und Regelungen des Datenschutzes sind beim Umgang und der Steuerung von digitalen Schließ- und Öffnungssystemen strikt einzuhalten.

11.
Wartung/Reparatur

Zur Wartung und gegebenenfalls Reparatur an der Infrastruktur der digitalen Schließsysteme werden Wartungsverträge abgeschlossen. Ansprechpartner im Bereich der durch Transponder zu öffnenden Türen ist hierfür die Abteilung 4, Referat 4 (Technik) der ZUV, welche gleichzeitig für notwendige Batteriewechsel bei Transpondern und Zylindern – eingeschlossen die Finanzierung und Abrechnung – zuständig ist.

Die Notwendigkeit eines Batteriewechsels bei den Transpondern ist den jeweiligen Bereichsadministratoren per E-Mail, Fax oder Brief anzuzeigen. Die Bereichsadministratoren entscheiden je nach Verfügbarkeit bzw. Dringlichkeit in Abstimmung mit dem Referat 4.4, ob sofort ein Batteriewechsel erfolgt oder ein neuer Transponder mit identischer Schließberechtigung ausgegeben wird.

Die Wartung und gegebenenfalls Reparatur der Infrastruktur des digitalen Türöffnungssystems mittels Universitätschipkarte liegt in der Verantwortung des ITZ.

12.
Bezeichnungen

Personen- und Funktionsbezeichnungen in dieser Ordnung gelten jeweils in männlicher und weiblicher Form.

13.
Inkrafttreten

Diese Schließordnung tritt einen Tag nach ihrer Veröffentlichung im Amtsblatt der Martin-Luther-Universität Halle-Wittenberg in Kraft.

Halle (Saale), 8. Oktober 2014

Prof. Dr. Udo Stäter
Rektor