23.6.2010

Dienstvereinbarung über den Einsatz von Elektronischen Zutrittssystemen der Ruhr-Universität Bochum

Zwischen dem

Personalrat der Ruhr-Universität Bochum vertreten durch den Vorsitzenden

und der

Ruhr-Universität Bochum vertreten durch den Kanzler

sowie zwischen dem

Personalrat der wissenschaftlich/künstlerisch Beschäftigten der Ruhr-Universität Bochum vertreten durch den Vorsitzenden

und der

Ruhr-Universität Bochum vertreten durch den Rektor

wird gemäß § 6 der Rahmendienstvereinbarung über Einführung und Anwendung von Systemen der Informationstechnik (IT-Rahmen-DV) vom 26.6.2009 und § 70 Personalvertretungsgesetz für das Land Nordrhein - Westfalen (Landespersonalvertretungsgesetz - LPVG -) folgende Dienstvereinbarung abgeschlossen:

§ 1
Geltungsbereich

Diese Dienstvereinbarung gilt für den Einsatz von elektronischen Zutrittssystemen an der Ruhr-Universität Bochum für Beschäftigte der Ruhr-Universität Bochum im Sinne der §§ 5 und 104 LPVG NW sowie für den Betrieb der dazu notwendigen Verwaltungssoftware. Die Ruhr-Universität Bochum wird die Regelungen dieser Dienstvereinbarung auch auf die Beschäftigten anwenden, die nicht von Personalräten vertreten werden.

§ 2

Begriffsbestimmungen

(1) Unter Verarbeitung wird gem. DSG NW die Erhebung (das Beschaffen von Daten), Speicherung, Veränderung, Übermittlung (das Bekanntgeben gespeicherter Daten an einen Dritten), Sperrung (das Verhindern der weiteren Verarbeitung), Löschung (das Unkenntlichmachen der gespeicherten Daten) sowie Nutzung von Daten verstanden.

(2) Unter Pseudonymisierung wird das Ersetzen aller personenbezogenen Daten durch eine Kennzahl gemäß einer Zuordnungsvorschrift verstanden, so dass der Personenbezug ohne Kenntnis der Zuordnungsvorschrift nicht mehr hergestellt werden kann. Ziel eines solchen Verfahrens ist es, nur bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug von einer dazu berechtigten Stelle wieder herstellen zu können (Re-Identifikation).

(3) Ein Zutrittsprofil ergibt sich aus der Festlegung von Türen und Zeiten, zu denen ein elektronischer Schlüssel Zugang gewährt. Standardprofile sind typischerweise in einem Bereich vorkommende Zutrittsprofile.

§ 3

Zweckbestimmungen

(1) Elektronische Zutrittssysteme werden zu den Zwecken eingesetzt,

(a) den Zutritt zu Gebäuden, Bereichen und Räumen der Ruhr-Universität zeitlich begrenzt auf berechtigte Personen einzuschränken,

(b) Unbefugten den Zutritt zu Gebäuden, Bereichen und Räumen der Ruhr-Universität zu verwehren, um die darin befindlichen Werte vor Diebstahl, Zerstörung oder Manipulation zu schützen.

(2) Alle Systemkomponenten dürfen ausschließlich die für den Zutritt notwendigen Informationen enthalten. Personenbezogene Daten sind innerhalb des gesamten Zutrittssystems in pseudonymisierter Form zu verarbeiten. Die Zuordnung zu Personen erfolgt getrennt vom Zutrittssystem. Die Re-Identifikation darf nur zum Zweck der Sperrung des elektronischen Schlüssels sowie zur Modifikation des Zutrittsprofils erfolgen.

(3) Für Bereiche, die nicht als sicherheitskritisch eingeschätzt werden, ist eine Datenaufzeichnung über Schließvorgänge unzulässig.

(4) Anfallende Daten im Sinne dieser Dienstvereinbarung dürfen gem. § 3 der IT-Rahmen-DV nur für die vereinbarten Zwecke verarbeitet werden. Sie dürfen nicht zu Zwecken einer Verhaltens- oder Leistungskontrolle oder zu Zwecken einer Ermittlung von Grundlagen für dienstliche Beurteilungen, Disziplinarmaßnahmen oder als Grundlage für die Feststellung des Gesundheitszustandes verarbeitet werden. Die Nutzung eines elektronischen Zutrittssystems für weitere Zwecke wird im gemeinsamen IT-Ausschuss mit dem Ziel der Einigung verhandelt und bedarf der Zustimmung durch die Personalräte.

(5) Eine Diskriminierung von Beschäftigten durch Festlegung oder Änderung von Zutrittsprofilen findet nicht statt. Bei der Vergabe von Zutrittsberechtigungen sollen funktionsbezogene Standardprofile benutzt werden.

§ 4

Systemdokumentation

(1) Ein Zutrittsystem arbeitet mit dezentralen Schließgeräten an den Eingängen, die mit einem kontaktlosen oder kontaktbehafteten elektronischen Schlüssel bedient werden. Die Schließgeräte können mit einem zentralen System vernetzt sein. Die Zutrittsprofile sind sowohl dezentral als auch zentral gespeichert und können folgende Angaben enthalten:

- Identifikationsnummer,
- Gültigkeit,
- räumliche und zeitliche Zutrittsbeschränkungen,
- Identifikationscode.

Findet ein kontaktloser Schlüssel Einsatz, so muss das Auslesen der Daten vom Nutzer kontrolliert werden können. Anderenfalls ist der Leseabstand aus Sicherheitsgründen auf unter 20 cm zu begrenzen.

(2) Für als sicherheitskritisch eingeschätzte Gebäude, Bereiche und Räume können zusätzliche Sicherungsmaßnahmen (z.B. die Eingabe eines persönlichen Identifikationscodes) vorgesehen werden. Die Einschätzung eines Gebäudes, Bereiches oder Raumes als sicherheitskritisch und die anzuwendenden Maßnahmen werden im IT-Ausschuss mit dem Ziel der Einigung verhandelt und bedürfen der Zustimmung durch die Personalräte.

(3) Nach Ablauf eines für das Einzelsystem festzulegenden Zeitraumes, der zum regulären Eintritt in einen geschützten Bereich angemessen ist, kann das fehlerhafte Offenstehen einer Tür über eine Anzeige an zentraler Stelle kenntlich gemacht werden. Das Verlassen der geschützten Bereiche erfolgt ohne erneute Identifikation durch mechanisches Öffnen einer Tür. Für den Notfall sind deutlich erkennbare Paniköffnungen von innen und Rettungszugänge von außen in ausreichendem Umfang vorzusehen.

(4) Jedes einzelne Zutrittssystem wird wie folgt dokumentiert:

- Auflistung der Hardwarekomponenten des Zutrittssystems einschließlich des Installationsplans,
- Bezeichnung der sicherheitskritischen Bereiche, für die zusätzliche Sicherungsmaßnahmen vorgesehen sind,
- Auflistung der Softwarekomponenten des Zutrittssystems,
- Bezeichnung der Administratoren des Zutrittssystems und deren Vertreter, Berechtigungen zur Vergabe von Zutrittsprofilen,
- Beschreibung der organisatorischen Maßnahmen zur Einführung und Administration des Systems und zur Umsetzung der Vorgaben dieser Dienstvereinbarung,
- Festlegung der Standardprofile,
- Abnahmeprotokoll der Feuerwehr.

§ 5
Inbetriebnahme

(5) Zur Inbetriebnahme eines elektronischen Zutrittssystems gemäß dieser Dienstvereinbarung sind die in § 4 Absatz 2 genannten Systemdokumentationen sowie eine Stellungnahme des behördlichen Datenschutzbeauftragten vorzulegen.

(6) Die Inbetriebnahme eines elektronischen Zutrittssystems erfolgt nach Einigung im IT-Ausschuss und bedarf der Zustimmung der Personalräte.

§ 6
Rechte und Pflichten der Beschäftigten

(1) Zutrittsberechtigte Beschäftigte erhalten einen elektronischen Schlüssel kostenfrei. Die Ausgabe des Schlüssels erfolgt nach Bestätigung durch die Beschäftigten. Mit Aushändigung des Schlüssels sind dem/der Beschäftigten das Zutrittsprofil, Rechte und Pflichten sowie Sperrwege mitzuteilen. Spätere Änderungen sind dem/der Beschäftigten umgehend anzuzeigen.

(2) Jede/r Beschäftigte erhält auf Wunsch schriftliche Informationen über alle auf dem Schlüssel und in der Verwaltungssoftware zu ihrer/seiner Person aktuell gespeicherten Daten.

(3) Die Beschäftigten sind verpflichtet, nach Kenntnisnahme des Verlustes eines elektronischen Schlüssels dessen Sperrung unverzüglich zu veranlassen.

(4) Die Beschäftigten sind verpflichtet, mit persönlichen Identifikationscodes sorgfältig umzugehen und diese nicht weiterzugeben.

(5) Personelle Maßnahmen, die auf Informationen beruhen, die unter Verletzung dieser Dienstvereinbarung gewonnen wurden, sind unwirksam und rückgängig zu machen.

(6) Es erwachsen der/dem Beschäftigten keine dienstrechtlichen Nachteile, wenn die/der Beschäftigte keinen Zutritt zu einem Dienstraum hat, weil die Tür nicht öffnet.

§ 7
Rechte der Personalräte

(1) Die Personalräte und der behördliche Datenschutzbeauftragte (bDSB) haben das Recht, die Einhaltung dieser Dienstvereinbarung zu überprüfen und zu diesem Zweck Stichproben zu machen. Dazu ist ihnen der erforderliche Zugang zu allen Stellen zu gewähren, an denen Komponenten des Zutrittssystems installiert sind und/oder Daten für das Zutrittssystem erhoben, gespeichert, verarbeitet und/oder genutzt werden. Die Personalräte können erforderlichenfalls dazu externe Sachverständige ihrer Wahl hinzuziehen. Unter Beachtung der sparsamen Haushaltsführung werden die Kosten hierfür von der Dienststelle getragen.

(2) Die Personalräte können auf allen Ebenen des Systems die vereinbarte Verwendung und die Einhaltung des Datenschutzes kontrollieren. Dazu können sie auch in alle vom System gespeicherten Daten und Protokolle Einblick nehmen. Alle zum System gehörenden Handbücher und Systemunterlagen einschließlich der Vorabkontrolle sind ihnen auf Wunsch in der aktuellen Version zeitweise zu überlassen

(3) Die Personalräte haben das Recht, alle Personen, die mit der Verarbeitung und Nutzung von Daten des Systems beschäftigt sind, bezüglich der rechtmäßigen, vereinbarten Verwendung zu befragen. Diese sind gegenüber den Personalräten zur wahrheitsgemäßen Auskunft berechtigt und verpflichtet. Auf Verlangen haben Sie Funktionen zu Prüfzwecken vorzuführen.

(4) Die Personalräte erhalten einen elektronischen Schlüssel mit einem Zutrittprofil zu allen Fluren und Gängen, soweit diese nicht aus besonderen Gründen für die Öffentlichkeit gesperrt sind. Über das Vorliegen besonderer Gründe (z.B. bei Gentechnikbereichen oder bei IT-Sicherheitsbereichen) entscheidet der IT-Ausschuss.

§ 8

Datenschutz

(1) Die Dienststelle stellt sicher, dass die organisatorischen und technischen Maßnahmen zur Umsetzung der im Landesdatenschutzgesetz geforderten Ziele getroffen werden.

(2) Unzulässig gespeicherte Daten sind aus allen Speichern zu löschen. Falsche Daten sind zu berichtigen. Ist die Richtigkeit der Daten strittig, so muss die Dienststelle die Richtigkeit innerhalb eines Monats nach Bekanntwerden der Bedenken nachweisen, andernfalls sind die Daten unverzüglich zu löschen. Die betroffenen Beschäftigten sind über diese Änderungen zu informieren.

(3) Der Kreis der zugriffsberechtigten Personen für die Verwaltungsdaten des Zutrittsystems wird unter Beachtung der Zweckbestimmung festgelegt. Veränderungen werden den Personalräten mitgeteilt.

§ 9

Schlussbestimmungen

Diese Vereinbarung tritt am Tage ihrer Unterzeichnung in Kraft. Sie kann von jeder Seite mit sechsmonatiger Frist gekündigt werden. In diesem Fall wirkt sie bis zum Abschluss einer neuen Vereinbarung insgesamt nach.

Sollte sich ein Teil dieser Dienstvereinbarung als rechtsunwirksam herausstellen, bleiben die anderen Teile in Kraft.