TECHNISCHE UNIVERSITÄT DRESDEN

Der Kanzler

Technische Universität Dresden, 01062 Dresden

Rektor, Prorektoren, Dekane, Sprecher der Fachrichtungen, geschäftsf. Leiter/Direktoren der Institute und Zentralen Einrichtungen, Dezernenten, Sachgebietsleiter, Personalrat, Studentenrat, Gleichstellungsbeauftragte, Schwerbehindertenvertretung, SLUB zur Beachtung

Bearbeiter: Herr Herber
Datenschutzbeauftragter
Mommsenstr. 12
Telelfon 0351 463 32881
Telefax: 0351 463 39718
E-Mail: Datenschutz@tu-dresden.de

Dresden, 30. Juni 2010

Rundschreiben D4/2/2010

Dienstvereinbarung über die Installation und den Betrieb elektromechanischer und/ oder elektronischer Schließanlagen sowie Zugangskontrollsysteme in Gebäuden der TU Dresden

Sachwörter:
Dienstvereinbarung (Installation und Betrieb von Schließanlagen und Zugangskontrollsystemen)
Schließanlagen (elektronische, elektromechanische, Dienstvereinbarung zum Schutz personenbezogener Daten)
Zugangskontrollsysteme (elektronische, elektromechanische, Dienstvereinbarung zum Schutz personenbezogener Daten)
Datenschutz (Schließanlagen, Zugangskontrollsysteme, Dienstvereinbarung)

Sehr geehrte Damen und Herren,

in der beigefügten Anlage finden Sie die o. a. Vereinbarung.
Ich bitte um Kenntnisnahme, Bekanntmachung und Beachtung in Ihrem Verantwortungsbereich.

Mit freundlichen Grüßen

gez. Wolf-Eckhard Wormser

Dienstvereinbarung
zwischen der
Technischen Universität Dresden
vertreten durch den Kanzler

und dem

Personalrat der Technischen Universität Dresden,
vertreten durch den Vorsitzenden

über die Installation und den Betrieb elektromechanischer und/oder elektronischer Schließanlagen sowie Zugangskontrollsysteme in Gebäuden der TU Dresden

§ 1 Zielsetzung und Allgemeines

(1) Ziel dieser Vereinbarung ist es, beim Einsatz elektronischer Schließanlagen und elektronischer Zugangskontrollsysteme den Schutz personenbezogener Daten vor unzulässigem Gebrauch und unberechtigtem Zugriff zu gewährleisten.

(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 Technischen Universität Dresden.

(3) Eine allgemeine Kontrolle oder Überwachung des Verhaltens der Nutzer elektronischer Schließ- und Zugangskontrollsysteme ist unzulässig und findet nicht statt.

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

§ 2 Geltungsbereich

(1) Der räumliche Geltungsbereich dieser Dienstvereinbarung umfasst den Bereich der Technischen Universität Dresden einschließlich aller von ihr genutzten Einrichtungen.

(2) Diese Dienstvereinbarung gilt nicht für die Medizinische Fakultät Dresden.

§ 3 Mitbestimmung

(1) Die Einrichtung und der Betrieb einer elektronischen Schließanlage bzw. eines Zugangskontrollsystems unterliegt in jedem einzelnen Fall der Mitbestimmung. Die Zustimmung des Personalrats und des Datenschutzbeauftragten ist in jedem Fall vor der Beschaffung der elektronischen Schließanlage bzw. des Zugangskontrollsystems einzuholen.

(2) Dem Mitbestimmungsantrag ist eine Verfahrensbeschreibung gemäß § 10 SächsDSG (für die TU Dresden umgesetzt in RS D4/02/04) sowie eine Betriebsordnung für die öffentliche Bekanntgabe und ein Sicherheitskonzept beizufügen.

(3) Änderungen und Erweiterungen der elektronischen Schließanlagen bzw. des Zugangskontrollsystems unterliegen ebenfalls der Mitbestimmung durch den Personalrat und bedürfen der Zustimmung des Datenschutzbeauftragten.

§ 4 Betreiberverantwortung

(1) Verantwortlich für die Vorgaben zur Installation, den Betrieb solcher Anlagen und den Zugriff auf die gespeicherten Daten ist das Dezernat Gebäudemanagement und Datenverarbeitung, im Folgenden Dezernat 4, der TU Dresden. Die Betreiberverantwortung kann mit Verfügung des Kanzlers auf andere Struktureinheiten übertragen werden. In jedem Fall ist durch geeignete technische Vorkehrungen sicherzustellen, dass nur Berechtigte die Anlagen bedienen.

(2) Im Dezernat 4 wird ein Verzeichnis aller elektronischen Schließanlagen und elektronischen Zugangskontrollsysteme geführt. Der Personalrat erhält mindestens einmal jährlich eine Kopie des jeweils aktuellsten Verzeichnisses.

(3) Schnittstellen zu anderen DV-Systemen sind gesondert datenschutzrechtlich zu genehmigen und mitzubestimmen.

§ 5 Erheben und Verarbeiten von Daten

(1) Die Zutrittsberechtigungen zu einzelnen Gebäuden und Räumen werden in Stammdaten der elektronischen Schließanlage bzw. dem Zugangskontrollsystem geführt. Die Stammdaten sind personenbezogene Daten im Sinne des Sächsischen Datenschutzgesetzes, die vor unbefugter Einsichtnahme zu schützen sind. Die Stammdaten können elektronisch verwaltet werden. Es sollen folgende Daten verarbeitet werden:

1. Titel
2. Name
3. Vorname
4. ein weiteres Merkmal zur eindeutigen Identifizierung der Person
5. Status (Mitarbeiter/Student/Gast)
6. Beschäftigungsstelle
7. Nutzungs-/Zugangsberechtigungen für Räume/Gebäude
8. Datum des Ablaufes der Nutzungsberechtigung
9. Nutzerkennung

Die Nutzerkennung (Nr. 9) soll alphanumerisch sein und darf ohne Kenntnis der Stammdatei keine Rückschlüsse auf eine natürliche Person erlauben.

(2) Bewegungsdaten im Sinne dieser Vereinbarung sind:

1. Ort
2. Datum
3. Zeit
4. Aktion
5. Nutzerkennung (Nr. 9 aus Abs. 1)

(3) Die Datenbestände nach Abs. 1 und Abs. 2 sind physisch zu trennen.

(4) Einsichtsberechtigt in Daten nach Abs. 1 und Abs. 2 sind:

1. der verantwortliche Betreiber sowie dessen Beauftragter (Administrator),
2. der Vorsitzende des Personalrats sowie
3. der Datenschutzbeauftragte

bzw. deren jeweilige Vertreter.

(5) Eine Zusammenführung und Auswertung ist nur bei besonderen Vorkommnissen von strafrechtlicher Relevanz oder auf schriftlichen Antrag des Nutzers der Anlage zulässig. Dabei müssen mindesten zwei Personen nach Abs. 4 anwesend sein. Jedwede Auswertung dient ausschließlich der Klärung des konkreten Anlasses. Über die Auswertung wird ein Protokoll erstellt. Entsprechende Aufzeichnungsdaten können auf Anforderung den Strafverfolgungsbehörden durch den Rektor im Einvernehmen mit dem Personalrat in angemessener Weise zur Verfügung gestellt werden. Andere Auswertungen und Berichte sind unzulässig.

(6) Der Zugriff auf die Bewegungsdaten nach Abs. 2 zu Zwecken der Administration, insbesondere zur Überprüfung der Funktionsfähigkeit der Anlage oder zur Störungsbeseitigung durch den zuständigen Betreiber nach Abs. 4 Nr. 1 ist jederzeit zulässig und in geeigneter Form zu dokumentieren.

(7) Die in den Sicherheitsanlagen gespeicherten Daten, die sich auf die Nutzung dieser Anlagen beziehen (Bewegungsdaten), werden spätestens nach Ablauf von 7 Werktagen nach Erhebung gelöscht. In den Fällen nach Abs. 5 ist eine längere Speicherfrist bis zur Klärung des Sachverhaltes möglich.

§ 6 Rechte und Pflichten der Nutzer

(1) Alle betroffenen Nutzer der Anlagen werden rechtzeitig umfassend und in geeigneter Weise über die Wirkungsweise des Systems (z. B. Verwendung ihrer Daten und die Auswertungsmöglichkeiten) informiert.

(2) Weiterhin erhalten die Nutzer, die am Zugangskontrollsystem teilnehmen, eine schriftliche Mitteilung über alle ihre Person betreffenden gespeicherten Daten zu Beginn des Systembetriebes sowie bei jeder Änderung, wenn sie davon betroffen sind.

(3) Jeder Beschäftigte hat das Recht, sich die auf seinem elektronischen Zugangsmedium gespeicherten Daten bei einer Person, die mit der Administration der Zugangsberechtigungsdaten betraut ist, darstellen zu lassen. Die Darstellung erfolgt in einer für die Nutzer nachvollziehbaren und verständlichen Form.

(4) Die Nutzer sind für den bestimmungsgemäßen Gebrauch ihres elektronischen Zugangsmediums verantwortlich. Dieses darf nicht weitergegeben und in unzulässiger Weise, z.B. um Unbefugten einen Zugang zu ermöglichen, genutzt werden.

(5) Ein Verlust ist unverzüglich beim zuständigen Betreiber sowie dem zuständigen Administrator anzuzeigen.

(6) Für die Ausgabe des Zugangsmediums kann ein Pfand erhoben werden.

§ 7 Bestandsanlagen / Übergangsvorschriften

(1) Bestandsanlagen sind den Bestimmungen dieser Dienstvereinbarung bis spätesten 6 Monate nach Unterzeichnung anzupassen. Dem Personalrat sowie dem Datenschutzbeauftragten sind hierfür die erforderlichen Unterlagen nach § 3 Abs. 2 vorzulegen.

§ 8 Inkrafttreten, Änderung und Kündigung

(1) Diese Dienstvereinbarung tritt mit ihrer Unterzeichnung in Kraft.

(2) Die Dienstvereinbarung kann mit einer Frist von drei Monaten zum Ende eines Jahres gekündigt werden. Nach Eingang der Kündigung sind Verhandlungen über eine neue Vereinbarung aufzunehmen. Bis zum Zustandekommen einer neuen Dienstvereinbarung gilt die bisherige weiter.

(3) Einvernehmliche Änderungen sind jederzeit unter Wahrung der Schriftform möglich.

(4) Sollten einzelne Punkte der Vereinbarung ungültig sein oder ihre Gültigkeit aufgrund neuer Gesetzgebung oder Rechtssprechung verlieren, so bleiben die übrigen Bestimmungen hiervon unberührt und weiterhin in Kraft.

Dresden, 20.10.2009

Kanzler
der Technische Universität Dresden

gez. Wolf-Eckhard Wormser

Vorsitzender des Personalrates
der Technischen Universität Dresden

gez. Dr. Michael Hochmuth