TECHNISCHE UNIVERSITÄT DRESDEN

Der Kanzler

Rektor, Prorektoren, Dekane
Vors. der Fachkommissionen u. Fachausschüsse, geschäftsf. Leiter/Direktoren der Institute, Zentralen Einrichtungen, Dezernenten, Sachgebietsleiter, Personalrat, Studentenrat, Gleichstellungsbeauftragte, Schwerbehindertenvertretung

Bearbeiter: Herr Dr. Zeimer
Mommsenstr. 15, Zi.: 7-105
Telefon: 0351 463-34766
Telefax: 0351 463-37701
E-Mail: dezernat2@tu-dresden.de
AZ:

Dresden, 16. November 2009

Rundschreiben D2/ 3 /2009

Dienstvereinbarung zwischen der TU Dresden und dem Personalrat der TU Dresden über die Nutzung eines Personaldateninformationssystems an der TU Dresden vom 7./17. September 2009 (Neufassung)

Sachwörter: Personaldateninformationssystem
(Dienstvereinbarung, Datenschutz, Datensicherheit)
Datenschutz (Personaldateninformationssystem, Dienstvereinbarung)
Datensicherheit (Personaldateninformationssystem, Dienstvereinbarung)
Dienstvereinbarung (Personaldateninformationssystem)

Sehr geehrte Damen und Herren,

die o.b. Dienstvereinbarung dient der Ausgestaltung der Beteiligungsrechte des Personalrates im Zusammenhang mit dem Schutz personenbezogener Daten (Personaldaten) der Mitglieder und Angehörigen der TU Dresden bei der Einführung und Anwendung eines Personaldateninformationssystems an der TU Dresden.

Die Neufassung ist der Umstellung des Personaldatensystems von HISSVA-UNIX auf die neuere Version HISSVA-GX geschuldet.

Ich bitte um Kenntnisnahme, Bekanntgabe und Beachtung in Ihrem Verantwortungsbereich.

Das Rundschreiben D2/6/98 tritt außer Kraft.

gez. Wolf-Eckhard Wormser

Anlagen

D i e n s t v e r e i n b a r u n g

zwischen der

TECHNISCHEN UNIVERSITÄT DRESDEN

vertreten durch den Kanzler

und dem

PERSONALRAT DER TECHNISCHEN UNIVERSITÄT DRESDEN

vertreten durch den Vorsitzenden

über die Nutzung eines Personaldateninformationssystems

P r ä a m b e l

Die nachstehende Dienstvereinbarung wird zur Ausgestaltung der Beteiligungsrechte des Personalrates im Zusammenhang mit der Wahrung des Rechts auf informationelle Selbstbestimmung der Mitglieder und Angehörigen der Technischen Universität Dresden (TUD) bei der Nutzung eines Personaldateninformationssystems an der TUD (außer Medizinischer Fakultät) getroffen.

§ 1
Allgemeine Regelungen

(1) Die Dienstvereinbarung gilt für die Verarbeitung personenbezogener und personenbeziehbarer Daten von gegenwärtigen oder ehemaligen Mitgliedern und Angehörigen der TUD (im weiteren Beschäftigte genannt) mit einem Personaldateninformationssystem (im weiteren System genannt).

(2) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, die auf der Grundlage der Einhaltung des Datenschutzes und der einschlägigen rechtlichen Bestimmungen erhoben werden.

(3) Die Verarbeitung von Daten ist das Erheben, Speichern, Verändern, Übermitteln, Nutzen, Sperren und Löschen i.S. des Sächsisches Datenschutzgesetzes (SächsDSG).

§ 2
Zulässigkeit der Verwendung von Personaldaten

(1) Die Daten der Beschäftigten werden nur im Rahmen der Zweckbestimmung des Beschäftigungsverhältnisses verwendet und ausgewertet.

(2) Die im System erfassten bzw. mit dem System oder anderweitig gewonnenen Daten werden nicht für Persönlichkeits- und Leistungsprofile verwendet. Arbeits- und personenbezogene Daten und Erkenntnisse aus dem System dürfen nicht alleinige Grundlage personalrechtlicher Entscheidungen sein.

(3) Zur individuellen Leistungs- und Verhaltenskontrolle der Beschäftigten werden Programme weder entwickelt noch eingesetzt. Der Inhalt von Dateien, einschließlich derer, die aus Gründen der Datensicherung erstellt werden, wird nicht als Hilfsmittel zur individuellen Leistungs- und Verhaltenskontrolle verwendet.

(4) Beurteilungen sowie medizinische und psychologische Befunde der Beschäftigten dürfen nicht im System gespeichert und verarbeitet werden. Das System darf ebenfalls nicht dazu benutzt werden, um personenbezogene Daten auf Vorrat, d.h. für einen noch nicht bestimmten oder noch nicht bestimmbaren Zweck zu erheben, zu speichern, zu verarbeiten oder auszuwerten.

(5) Die Übermittlung von Personaldaten an Dritte ist unzulässig, es sei denn, dass der betroffene Beschäftigte vorher zustimmt oder die TUD kraft Gesetzes zur Auskunft verpflichtet ist.
Über Auswertungen, die auf Daten aus dem System zurückgreifen und über den Rahmen des Dienstverkehrs zwischen Dienststelle und oberster Dienstbehörde hinausgehen, ist der Personalrat zu informieren.

§ 3
Rechte der Beschäftigten

(1) Jeder Beschäftigte erhält auf Antrag bei der personalverwaltenden Stelle Auskunft über alle zu seiner Person gespeicherten Daten, ihre Verwendung und den Zweck ihrer Verwendung.
Die Auskunft schließt die Aushändigung einer vollständigen Übersicht zu den über den Beschäftigten im Rahmen des Systems gespeicherten Daten in unverschlüsselter und lesbarer Form ein.

(2) Gespeicherte personenbezogene Daten über einen Beschäftigten sind auf dessen Verlangen zu berichtigen oder zu ergänzen, wenn der Beschäftigte ihre Unrichtigkeit bzw. Unvollständigkeit nachweist. Personenbezogene Daten, deren Richtigkeit vom Beschäftigten bestritten wird und von der TUD nicht nachgewiesen werden kann, sind zu löschen.

(3) Das Recht der Beschäftigten auf Einsichtnahme in ihre Personalakte nach Maßgabe der geltenden Rechtsvorschriften bleibt unberührt.

§ 4
Rechte des Personalrates

(1) Der Personalrat erhält eine Kopie des Verfahrensverzeichnisses in der jeweils geltenden Fassung und eine Übersicht über die gespeicherten personenbezogenen Daten (Niederschrift 1). Bei Änderung der Merkmale nach Niederschrift 1 wird der Personalrat beteiligt.

(2) Dem Personalrat wird auf Verlangen Einsicht in Ablauf und Funktionsweise des Systems gewährt.

§ 5
Datenschutz und Datensicherheit

(1) Bezüglich der Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit gilt das Sicherheitskonzept laut gesonderter Niederschrift 2, die Bestandteil dieser Dienstvereinbarung ist.

(2) Die TUD trifft nach dem jeweiligen Stand der Technik Maßnahmen, die geeignet sind zu gewährleisten, dass
- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
- personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
- personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),
- jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),
- festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

§ 6
Schlussbestimmungen

(1) Das SächsDSG und das Sächsische Personalvertretungsgesetz finden Anwendung. Die Kontrollbefugnisse des Datenschutzbeauftragten der TUD bleiben unberührt.

Bei der Anwendung des Systems sind über die datenschutzrechtlichen Vorschriften hinaus die einschlägigen Bestimmungen insbesondere des Arbeits- und Tarifrechts sowie des Dienstrechts zu beachten.

(2) Änderungen und Ergänzungen der Dienstvereinbarung müssen als solche gekennzeichnet sein und bedürfen zu ihrer Wirksamkeit der Schriftform.

(3) Die Dienstvereinbarung kann mit einer Frist von 3 Monaten gekündigt werden.

(4) Nach der Kündigung der Dienstvereinbarung gelten ihre Regelungen weiter bis sie durch eine andere Dienstvereinbarung oder Abmachung ersetzt worden ist. Entsprechende Verhandlungen sind unverzüglich aufzunehmen.

(5) Die Dienstvereinbarung tritt mit ihrer Unterzeichnung in Kraft. Gleichzeitig tritt die Dienstvereinbarung vom 11./ 23. Februar 1998 über die Einführung und Anwendung des Personaldatensystems HISSVA-UNIX außer Kraft.

Dresden, den 07.09.2009

Für die TU Dresden

gez. Wormser

Der Kanzler

Dresden, den 17.09.2009

Für den Personalrat

gez. Hochmuth

Der Vorsitzende

Anlagen: Niederschrift 1
Niederschrift 2

Niederschrift 1

über

die gespeicherten personenbezogenen Daten gemäß § 4 (1) der Dienstvereinbarung zwischen der TU Dresden und dem Personalrat der TU Dresden über die Nutzung eines Personaldateninformationssystems

Die folgenden personenbezogenen Daten der Beschäftigten werden im Personaldatensystem zur Vertragsabwicklung und zur Erfüllung des Finanz- und Personalstatistikgesetztes, des Vollzuges des Schwerbehindertenrechts nach SGB IX sowie der Kapazitätsverordnung erfasst:

Name
Vornamen
Geschlecht
Geburtsdatum
Geburtsname
Geburtsort
Akademische Grade, einschließlich Habil- und Berufungsdaten
Adresse(n)
Staatsangehörigkeit(en)
Familienstand

zur Vertragsabwicklung erforderliche Daten:
Beginn evtl. Ende des Vertrages
Probezeit
Arbeitszeit
Tätigkeit
Eingruppierung einschließlich evtl. Zulagen und Personalkosten
Finanzierung des Vertrages
Bankverbindung
Kostenstelle
Beurlaubungen (Grund und Zeitraum)
Krankheitszeiträume

zur Bestimmung der Lehrleistung und -auslastung:
Lehrdeputate einschließlich evtl. Minderungen

für den Vollzug des Schwerbehindertenrechts (SGB IX):
Schwerbehindertenstatus
Gültigkeitszeitraum
Ausweisausstellende Dienststelle

NIEDERSCHRIFT 2

über

Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit gemäß § 5 der Dienstvereinbarung zwischen der TU Dresden und dem Personalrat der TU Dresden über die Nutzung eines Personaldateninformationssystems

§ 1
Anwendungssystem

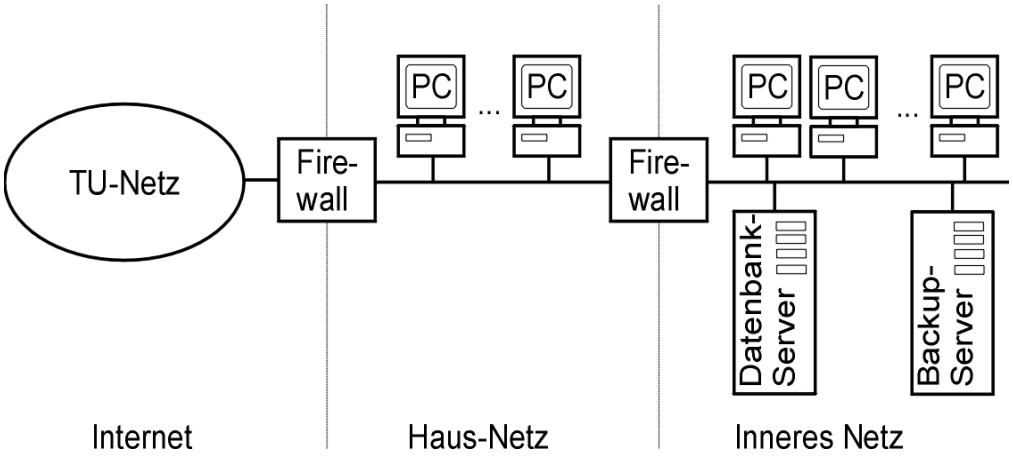
Das Anwendungssystem ist ein Mehrplatzsystem, das aus einem Datenbankserver und PC-Clients besteht.

§ 2
Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit

Zur Gewährleistung des Datenschutzes und der Datensicherheit werden an der TU Dresden gemäß § 5 (2) der Dienstvereinbarung nachstehende DV-technische bzw. organisatorische Kontrollmaßnahmen realisiert:

1. Vertraulichkeit

Die Nutzung des Personalsystems erfolgt in einem inneren lokalen Netz, das über eine Kaskade von zwei Firewall-Routern an das TU-Netzwerk angeschlossen ist. Die äußere Firewall wehrt einen Großteil der Zugriffe aus dem Internet auf das Haus-Netz ab. Die innere Firewall blockiert sämtliche Zugriffe aus dem Haus-Netz (einschließlich des Internets) auf das innere Netz, also auch auf den Datenbankserver und die Client-PCs; siehe dazu untenstehendes Bild. Die dafür zuständigen Firewall-Regeln sind bei den Netzwerk-Administratoren dokumentiert.



Die Daten lagern auf dem Datenbank-Server. Sie werden auf den Client-PC angezeigt, aber nicht gespeichert.

Zum Zugriff vom Client-PC auf die Datenbank ist ein individuelles Login (Name/Passwort) des Nutzers erforderlich. Nach mehrmaliger Eingabe eines falschen Passwortes wird das Login gesperrt.

Die Anzeige der Daten mit Hilfe des Anwendungssystems erfolgt generell über vorgegebene Menüs, die für jeden Nutzer individuell konfigurierbar sind. Dadurch sind für jeden Nutzer nur bestimmte Daten einsehbar. Die Konfiguration der Menüs und die Verwaltung der Zugriffe der Nutzer obliegt dem Dezernat Personal; technische Unterstützung leistet das Sachgebiet Datenverarbeitung.

Die Anmeldung auf dem Datenbankserver ist nur speziell dafür autorisierten Administratoren mittels individuellem Login (Name/Passwort) möglich.

Der Server befindet sich in einem alarmgesicherten Serverraum, zu dem ausschließlich die befugten Administratoren Zutritt haben. Die Datensicherungsmedien befinden sich in einem Tresor eines ebenfalls alarmgesicherten Raumes.

Die Informationen auf auszusondernden bzw. fehlerhaften Datenträgern werden mit einem Datenträgerlöschgerät zuverlässig entfernt.

Zusätzlich ist auf allen PC ein Virenschutz-Programm installiert. Durch ständige Updates (ggf. mehrmals täglich) der Virensignaturen kann schnellstmöglich auf veränderte Schadsoftware reagiert werden.

2. Integrität

Bei der Installation des Anwendungssystems wurden die Richtlinien des Herstellers beachtet, so dass das System optimal mit der Datenbank zusammenarbeiten kann. Durch die regelmäßige Installation von Updates und Patches werden Fehler in der Software behoben.

Die Integrität der Daten ist ferner dadurch gewährleistet, dass eine transaktionsgesicherte Datenbank verwendet wird, so dass nur teilweise veränderte Daten im Falle eines Fehlers wieder in ihren Zustand vor Beginn der unvollständigen Veränderung zurückgesetzt werden.

Eine mutwillige Veränderung der Daten wird durch die im Punkt 1 genannten Maßnahmen verhindert.

3. Verfügbarkeit

Eine hohe Verfügbarkeit des Gesamtsystems wird vor allem durch Maßnahmen zur Erhöhung der Redundanz an neuralgischen Punkten (Hardwarekomponenten des Servers, Netzwerkkomponenten) erreicht.

Zusätzlich wird automatisch täglich eine Sicherung der gesamten Datenbank auf einem Backup-Server angefertigt. Der Backup-Server befindet sich ebenfalls in dem besonders geschützten inneren Netz, aber örtlich getrennt vom Datenbank-Server in einem alarmgesicherten Raum.

Im schlimmsten anzunehmenden Fall (Ausfall einer zentralen Komponente) kann innerhalb von einer Frist von ca. 3h die Arbeit mit dem Anwendungssystem wieder aufgenommen werden.

4. Authentizität

Die Nutzerauthentifizierung erfolgt mit den Mitteln des Betriebssystems, wodurch bereits eine sehr hohe Sicherheit gegen Fälschung der Daten gegeben ist. Zudem erfolgt die Kommunikation innerhalb eines sicheren Netzes, das durch ein im Punkt 1 genanntes mehrstufiges Konzept von unsicheren Netzen abgeschirmt ist.

Innerhalb der Datenbank wird die Authentizität durch die Verwendung eindeutiger Identifikatoren gewährleistet.

5. Revisionsfähigkeit

Alle Änderungen an den Daten werden mit Angabe von Zeit und ausführendem Sachbearbeiter vom Anwendungssystem maschinell protokolliert.

6. Transparenz

Das DV-Verfahren ist in der Programmbeschreibung des Herstellers ausreichend dokumentiert. Dazu gehört auch eine ausführliche Beschreibung der Bedeutung aller Tabellen und Merkmale der Datenbank.

Über entsprechendes Rundschreiben wurden alle Mitarbeiter der TU darüber informiert, dass sie auf Wunsch Auskunft über alle zu ihrer Person erfassten Daten in lesbarer Form erhalten.