Was ist weiterhin zu beachten

- Zur automatisierten Verarbeitung personenbezogener Daten dürfen Verfahren nur nach vorheriger schriftlicher Abwägung zwischen den Gefahren für die Rechte Betroffener, die wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien entstehen können, sowie der Beherrschbarkeit der neuen Technologie eingesetzt werden (Vorabkontrolle: § 7 Absatz 3 NDSG).

- Sofern nicht-freigegebene, unlizenzierter und selbst erstellte Software sowie Programme von Public Domain und Shareware eingesetzt wird, trägt die alleinige Verantwortung für Datenschutz und Datensicherheit der Anwender dieser nicht-lizenzierten Programme.

- An der bereitgestellten Hardware dürfen keine Veränderungen vorgenommen werden.

- Verfahren, Programme, Software, Anwendungen und Daten dürfen nicht verfälscht und unbefugt an Dritte weitergegeben werden.

- Der PC und die darauf gespeicherten Verfahren (Programme, Software, Anwendungen) und Daten dürfen nur zur Erfüllung der vorgegebenen dienstlichen Aufgaben verwendet werden.

- Die vorgegebenen Sicherheitsmaßnahmen zum Zugangs- und Zugriffsschutz sind sorgfältig einzuhalten.

- Personenbezogene Daten auf einem tragbaren Laptop, Notebook, PC sind verschlüsselt zu speichern.

- Alle sonstigen vorgegebenen technischen und organisatorischen Maßnahmen sind anzuwenden (vgl. § 7 NDSG).

Die Nichtbeachtung der vorgenannten Hinweise und die Nichteinhaltung der vorgegebenen Sicherungsmaßnahmen können arbeits- und im Rahmen der Strafgesetze auch strafrechtlich verfolgt und geahndet werden.

Kontakt

Technische Universität Braunschweig
Der Präsident
Pockelsstraße 14
38106 Braunschweig

http://www.tu-braunschweig.de

Technische Universität Braunschweig
Der Datenschutzbeauftragte
Prof. Dr. Michael Wettern

Telefon 0531 391 5886
Fax 0531 391 8208

http://www.tu-braunschweig.de/datenschutz
E-Mail: datenschutz@tu-braunschweig.de

Stand: 18.01.2005

CAROLO-WILHELMINA

Datenschutz und Datensicherheit

TECHNISCHE UNIVERSITÄT
CAROLO-WILHELMINA
ZU BRAUNSCHWEIG

Merkblatt zum Datenschutz – Datensicherheit

Sehr geehrte Mitarbeiterinnen,
sehr geehrter Mitarbeiter,

es ist sicher nicht in Ihrem Sinne, wenn personenbezogene Daten über Sie und über Ihre persönlichen Verhältnisse Unbefugten zur Kenntnis gelangen würden. Davor schützen Sie das Bundesdatenschutzgesetz (BDSG), das Niedersächsische Datenschutzgesetz (NDSG) und weitere bereichsspezifische Datenschutzbestimmungen (z. B. das Sozialgesetzbuch).

Die Technische Universität Braunschweig schützt sämtliche personenbezogenen Daten

Durch das Niedersächsische Datenschutzgesetz wurde die rechtliche Verpflichtung geschaffen, die zur Einhaltung des Datenschutzes notwendigen technischen, personellen und organisatorischen Maßnahmen zu treffen. Dies beinhaltet u.a. die Erstellung eines Sicherheitskonzeptes und ebenso das Festlegen eines Planes für Notfälle.

An der TU Braunschweig sind diese Erfordernisse zur IT-Technologie in drei entsprechende Ordnungen eingeflossen. Sie finden diese auf den Internetseiten der TU Braunschweig (http://www.tu-braunschweig.de/datenschutz). Die Ordnungen beschreiben Vorgehensweisen, um die IT-Sicherheit an der Universität zu gewährleisten. Sie regeln die Nutzung der Informationstechnologie, machen Vorgaben für die Internetpräsentation, listen Rechte und Pflichten bei der Nutzung der Informationstechnologie auf und nennen die sich aus Verstößen gegen diese Vorgaben ergeben Haftungen.

Datenschutz im Rahmen Ihrer dienstlichen Tätigkeiten

- Sie sind im Rahmen Ihrer beruflichen Tätigkeit dazu verpflichtet, die personenbezogenen Daten anderer vertraulich und weisungsgerecht zu behandeln.
- Sie sind dafür verantwortlich, dass die Ihnen anvertrauten erforderlichen personenbezogenen Daten zweckgebunden (§ 10 NDSG) nur im Rahmen Ihrer Aufgabenstellung verarbeitet, d.h. erhoben, gespeichert, verändert, übermittelt, gesperrt oder gelöscht werden.
- Nicht mehr erforderliche personenbezogene Daten sind unter Beachtung von Aufbewahrungsfristen datenschutzgerecht zu löschen bzw. zu vernichten, damit eine missbräuchliche Weiterverwendung ausgeschlossen wird.
- Der Missbrauch und jede Weitergabe dieser Daten ist unzulässig oder ggf. sogar strafbar und kann Schadensersatzansprüche auslösen.
- Für jedes Verfahren, bei dem personenbezogene Daten automatisiert verarbeitet werden, ist dieses der Abt. 52 auf einem dafür vorgesehenen Formblatt mitzuteilen.
- Bei einer Auskunftserteilung bzw. Übermittlung von personenbezogenen Daten an Dritte ist die Identität der bzw. des Ersuchenden zu prüfen und zu dokumentieren. Ebenfalls ist die Rechtsgrundlage für die Auskunftserteilung / Datenübermittlung zu prüfen. Im Zweifelsfall wenden Sie sich deswegen an die Abt. 31.
- Grundsätzlich gilt: Der Verursacher der Verarbeitung personenbezogener Daten ist für deren sachgerechte Handhabung, was auch die Entsorgung einschließt, verantwortlich.

Ihre persönlichen Schutzmaßnahmen können z.B. sein

- Schützen Sie die Ihnen anvertrauten Daten und Datenträger, wenn Sie nicht unmittelbar daran arbeiten, indem Sie diese unter Verschluss halten.
- Stellen Sie sicher, dass Besucher und Gäste bei ihrer Vorsprache nur die ihre Angelegenheit betreffenden personenbezogenen Daten zur Kenntnis nehmen können. Dies gilt sowohl für Daten in Akten als auch für deren Verarbeitung mit einem Computer.
- Schließen Sie Ihr Büro ab, wenn Sie es verlassen.
- Beim Verlassen des Arbeitsplatzes sind alle PC-Anwendungen zu schließen und der Bildschirmschoner zu aktivieren. Bei längerer Abwesenheit und Dienstende sind die Fenster und Türen zu schließen.
- Schalten Sie Ihren PC abends aus.
- Schützen Sie die Daten auf ihrem Rechner stets durch aktuelle Sicherheitseinstellungen für Ihr System.
- Schützen Sie Ihr Passwort:
  Das Passwort sollte mindestens 6 - 8 Zeichen einschließlich Sonderzeichen aufweisen, jedoch keine Abhängigkeiten enthalten. Niemand darf Passwörter weitergeben, auch nicht im Vertretungsfall. Vertretungen werden über eigenständige Arten der Zugangsberechtigungen geregelt.