Merkblatt zum Datengeheimnis

(Stand 07.08.14)

Im Rahmen Ihrer Tätigkeit bei der Universität kommen Sie in der Regel mit **personenbezogenen Daten** in Berührung – z.B. mit Noten, mit Krankmeldungen, mit Anträgen, mit E-Mails, etc. Wenn Sie im Bereich der DV-Systemtechnik / IT beschäftigt sind, bestehen vielfach Zugriffsmöglichkeiten auf Systeme und Datenbanken, mit denen personenbezogene Daten verarbeitet werden.

Das verfassungsrechtlich im Grundgesetz verankerte **Grundrecht** auf informationelle Selbstbestimmung verpflichtet die Universität als Körperschaft des öffentlichen Rechts, „den **Einzelnen** davor **zu schützen**, dass er durch die Verarbeitung seiner **personenbezogenen Daten durch öffentliche Stellen** in seinem Persönlichkeitsrecht beeinträchtigt wird“ (§ 1 Landesdatenschutzgesetz (LDSG)).

Diese gesetzlichen Vorgaben müssen Sie bei Ihrer Tätigkeit berücksichtigen. **Das Gesetz verpflichtet Sie daher ausdrücklich zur Wahrung des Datengeheimnisses (§ 6 LDSG):**

> „Den bei öffentlichen Stellen beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder sonst zu verwenden (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.“

Beispiele für personenbezogene Daten sind: Name, Geburtsdatum, Religion, Adresse, Telefon, Gehalt, Urlaubszeiten, Krankheiten, Mitgliedschaften.

Gegenstand datenschutzrechtlicher Regelungen ist der gesamte Verarbeitungsprozess personenbezogener Daten, also der gesamte „Lebenszyklus“. Dieser beginnt beim „Erheben“, geht über das „Speichern“ und „Verändern“ der personenbezogenen Daten, die Weitergabe der personenbezogenen Daten innerhalb der Universität („Nutzen“) und an Stellen außerhalb der Universität („Übermitteln“) bis hin zum Löschen.

Jede Datenverarbeitung ist verboten, es sei denn, sie ist durch eine Regelung erlaubt oder der Betroffene hat (grundsätzlich schriftlich) eingewilligt (§ 4 Abs. 1 LDSG).

Soweit Sie im Rahmen Ihrer Tätigkeit der DV-Systemtechnik / IT an der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirken (ggf. z.B. E-Mail), seien Sie sich bitte bewusst, dass Sie zur Wahrung des **Fernmeldegeheimnisses** verpflichtet sind.

Verstöße gegen das Datengeheimnis, das Fernmeldegeheimnis oder anderer Datenschutzvorschriften können zu **arbeitsrechtlichen Konsequenzen** bis hin zu **Schadensersatzforderungen** führen und können außerdem mit **Geld- oder Freiheitsstrafe** geahndet werden.

Was bedeutet dies konkret für mich?

1. Die personenbezogenen Daten dürfen Sie **nur** für den **jeweiligen zur Aufgabenerfüllung gehörenden Zweck** verarbeiten. Insbesondere dürfen sie nicht Unbefugten zugänglich gemacht werden.
2. Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn es **zum jeweiligen Zweck erforderlich** ist. Insbesondere dürfen Mitarbeiter der IT nur dann Einsicht in Datenbestände nehmen, wenn dies zur Aufgabenerfüllung (z.B. Fehleranalyse) zwingend notwendig ist.
3. Es dürfen **nur diejenigen Daten** verarbeitet werden, die zur Aufgabenerfüllung zwingend **erforderlich** sind. Sie kommen damit dem gesetzlich normierten Grundsatz der Datenvermeidung und –minimierung nach. Im Bereich der IT ist dabei auch an das restriktive Schreiben von Protokolldateien zu denken.
4. Personenbezogene Daten sind **grundsätzlich beim Betroffenen** mit seiner Kenntnis zu erheben, bei Dritten nur in Ausnahmefällen.
5. Erfüllen Sie die Ihnen zugewiesenen Aufgaben mit der notwendigen **Sorgfalt** und beachten Sie bestehende Datenschutzvorschriften. Fragen Sie im Zweifelsfall (siehe unten) nach. Festgestellte Mängel sind unverzüglich zu beheben oder zu melden.
6. Alle Schriftstücke, elektronischen Dokumente und Datenträger, auch Abschriften, Durchschläge und Kopien, mit personenbezogenen Daten, haben Sie **sorgfältig aufzubewahren**, vor jeder Einsichtnahme Unbefugter zu schützen und auf Verlangen jederzeit – spätestens aber bei Beendigung des Arbeitsverhältnisses – Ihrem Vorgesetzten zu übergeben bzw. zu **löschen**. Sofern Sie sich faktisch nicht in der Lage sehen, der vorstehenden Verpflichtung nachzukommen, ist der Vorgesetzte entsprechend zu unterrichten.
7. Bei der Nutzung der Infrastruktur für digitale Informationsverarbeitung und Kommunikationstechnik sind Sie verpflichtet dafür zu sorgen, dass **Dritte keine Kenntnis** von Ihren Authentifizierungsinformationen (z. B. Passwort, PIN, Private Key) erlangen. Es ist Ihnen verboten, fremde Authentifizierungsinformationen zu ermitteln oder offen zu legen, unberechtigten Zugriff auf Informationen anderer Nutzer oder Nutzerinnen zu nehmen und Ihnen im Rahmen ihrer Tätigkeit bekannt gewordene Informationen anderer Nutzer oder Nutzerinnen weiterzugeben, selbst zu nutzen oder zu verändern**.**
8. **Geben Sie auf Anfragen keine Daten heraus, ohne die Rechtmäßigkeit zuvor kritisch geprüft zu haben** (Beispiele: Krankenkasse, Rentenversicherung, Ausländerbehörde, Privatunternehmen, Alumni-Einrichtungen, Studentenwerk, Ermittlungsbehörden, Meldebehörde, Rechtsanwalt, hochschulinterne Kommunikation). Bei Anfragen in telefonischer

Form oder per unverschlüsselter E-Mail ist die Identität des Anfragenden nicht ausreichend sichergestellt, verweisen Sie daher grundsätzlich auf die Schriftform (auch Fax). Anfragen, die auf die Herausgabe von personenbezogenen Daten gerichtet sind, müssen auf die Rechtsvorschrift hinweisen, die das Auskunftsersuchen rechtfertigt. Generell müssen Anfragen schlüssig bzw. plausibel sein. Nutzen Sie für Ihre Prüfung der Rechtmäßigkeit der Herausgabe die Informationen der ZENDAS:
https://www.zendas.de/service/verwaltung/index.html
Sofern Sie zum Ergebnis kommen, dass die Weitergabe zulässig ist, geben Sie die personenbezogenen Daten **in digitaler Form nie unverschlüsselt** heraus, sondern wenden eine Verschlüsselungstechnik an.

9. **Treffen Sie technische und organisatorische Maßnahmen zum Schutz der Daten.** Dazu gehört insbesondere, dass Sie Ihr Büro auch bei kurzen Abwesenheiten grundsätzlich abschließen, bei Publikumsverkehr herumliegende Unterlagen während des Arbeitstages so aufbewahren, dass sie nicht einsehbar sind und Akten in ausreichend gesicherten und verschlossenen Behältnissen/Schränken aufbewahren. Nutzen Sie zeitgemäße Verschlüsselungstechniken. Dies gilt umso mehr für Mitarbeiter der IT, die die Systeme so konfigurieren müssen, dass sie dem Schutz der personenbezogenen Daten gerecht werden. Sichern Sie – um nur einige wenige Maßnahmen zu nennen - die Räume mit Servern gegen unbefugte Zutritte ab, und sorgen Sie außerdem für eine ausreichende Passwort-Policy und dem Schutz der Daten vor Verlust oder Zerstörung durch Backup und USV.

Wie ist der Wortlaut der wesentlichen Regelungen?

Wichtige Vorschriften wie insbesondere das LDSG, das Telekommunikationsgesetz (Fernmeldegeheimnis in § 88 TKG) und das Strafgesetzbuch (Verletzung des Post- und Fernmeldegeheimnisses in § 206 StGB) finden Sie unter
http://www.zendas.de/recht/texte/index.html.

Wer kann mir bei Fragen weiter helfen?

Wenn Sie Fragen zur Verarbeitung personenbezogener Daten haben, finden Informationen auf den Webseiten der Zentrale Datenschutzstelle der baden-württembergischen Universitäten (ZENDAS):
https://www.zendas.de

Sofern Ihre Fragen dadurch nicht beantwortet werden, können Sie sich gerne an die Ansprechpartner an Ihrer Universität wenden. Diese finden Sie unter:
https://www.zendas.de/kontakt.html