Datenschutz

Im Rahmen des Grundrechts auf informationelle Selbstbestimmung hat jede Person das Recht über die Preisgabe und Verwendung ihrer personengebundenen Daten zu bestimmen. Personengebundene Daten sind Angaben über bestimmte (z. B. Name) oder bestimmbare (z. B. Kontonummer) natürliche Personen. Im Zuge der rasch fortschreitenden technischen Entwicklung im Bereich elektronischer Datenverarbeitung, die es erlaubt, sehr große Datenbestände schnell und kostengünstig zu speichern, zu verarbeiten und abzurufen, hat das Thema Datenschutz eine neue Bedeutung gewonnen.

Der Begriff Datenschutz umfasst alle technischen, organisatorischen und rechtlichen Maßnahmen, die dazu dienen, das Grundrecht der informationellen Selbstbestimmung als Freiheitsrecht des Bürgers zu sichern. Dabei sind folgende Grundsätze zu beachten:

- Datensparsamkeit (nur zwingend erforderliche Daten dürfen verarbeitet werden),
- Vertraulichkeit (keine Weitergabe der Daten an Unbefugte; kein Zugriff auf die Daten durch Unbefugte),
- Datenintegrität (keine Manipulation und kein Löschen der Daten, auch nicht durch technische Störungen),
- Verfügbarkeit (Daten müssen abrufbereit sein, insbesondere auch für die betreffende Person selbst).

Viele Hochschulen verfügen über Datenschutzbeauftragte, die Sie über die für Sie geltenden Regelungen informieren können. Auch wenn das Thema Datenschutz nicht zu Ihrem expliziten Aufgabenbereich gehört, wie dies z. B. bei Systemadministratoren der Fall ist, sind Sie in Ihrem Verantwortungsbereich für die Einhaltung der geltenden Regelungen verantwortlich. An dieser Stelle möchten wir Ihnen einen Überblick über grundlegende technische Möglichkeiten zum Datenschutz geben, die Sie mit vertretbarem Aufwand in Ihren Arbeitsalltag integrieren können.

Anonymisierung / Pseudonymisierung
Ein Weg, datenschutzrechtliche Probleme zu vermeiden, ist die Anonymisierung der Daten. Bei der Anonymisierung werden die Daten so verändert, dass es nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, aus den Daten auf eine bestimmte Person zu schließen. Dazu müssen nicht nur Namen gelöscht werden, sondern auch alle anderen Informationen, die die Identifizierung einer Person ermöglichen (z. B. „der 1986 an die Universität Musterstadt berufene Professor der Psychologie“).
Die Pseudonymisierung ist eine Vorstufe zur Anonymisierung. Dabei wird anstelle der Identifizierungsmerkmale ein Zuordnungsmerkmal (Pseudonym) verwendet. Die Pseudonymisierung ist einerseits praktisch, da sie eine Zusammenführung der zu einem Pseudonym gehörenden Daten erlaubt. Andererseits besteht die Gefahr, dass durch die Enttarnung des Pseudonyms sämtliche Daten einer bestimmten Person zugeordnet werden können.

Datenschutzfreundliche Software
Transparente Software, deren Quellcode öffentlich zugänglich ist und die somit unabhängigen Prüfungen bezüglich ihrer Sicherheit unterzogen werden kann, gilt als datenschutzfreundlich (siehe z. B. Datenschutzbeauftragte des Bundes und der Länder). In diesem Zusammenhang sind insbesondere so genannte Open Source -Produkte zu nennen, deren Sicherheitslücken in der Regel besser eingeschätzt und schneller geschlossen werden können als die

kommerzieller Programme.

Weiterführende Informationen

- Bundesamt für Sicherheit in der Informationstechnik
- Zendas – Zentrale Datenschutzstelle für Badenwürttembergische Universitäten
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Letzte Änderung: 11.06.2015

Zitation

e-teaching.org (2015). Datenschutz. Zuletzt geändert am 11.06.2015. Leibniz-Institut für Wissensmedien: https://www.e-teaching.org/technik/datenhaltung/datenschutz/index_html. Zugriff am 16.02.2019