

Richtlinien zum Datenschutz im IT-Bereich

Die folgenden Richtlinien sollen mithelfen, Daten im IT-Bereich in Bezug auf Verantwortlichkeiten und Schutzwürdigkeit besser klassifizieren zu können und liefern einige grundsätzliche Leitplanken, welche technischen Hilfsmittel sich für welche Schutzklasse eignen können. Die Richtlinien gliedern sich in einen juristischen Teil sowie einen darauffolgenden technischen Teil.

1. Datenschutz – ein Thema für Universitätsangehörige?

Alle Universitätsangehörigen kommen gelegentlich mit „Daten“ in Berührung, z.B.

- als Studierende im Zusammenhang mit der Immatrikulation
- als Prüfungsverantwortliche im Zusammenhang mit der Bekanntgabe und Archivierung von Prüfungsergebnissen
- als Forschende im Zusammenhang mit empirisch gewonnenen, personenbezogenen Daten oder mit Umfrageergebnissen
- als Erbringer/-in von Dienstleistungen, etwa im Zusammenhang mit Krankengeschichten
- als Informatikbeauftragte im Zusammenhang mit Fragen des Datenzugangs und der Sicherung von Datenmaterial

Die Universität untersteht als öffentlichrechtliche Anstalt des Kantons Bern der **kantonalen Datenschutzgesetzgebung**, namentlich dem Datenschutzgesetz vom 19. Februar 1986 (DSG; BSG 152.04).

Der Datenschutz ist eine Konkretisierung der verfassungsmässigen Rechte des Persönlichkeitsschutzes sowie des Schutzes des Privat- und Geheimbereichs. So bestimmt die Bundesverfassung vom 18. April 1999 in Artikel 13 Absatz 2: „**Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.**“

2. „Daten“

„Daten“ im Sinne der Datenschutzgesetzgebung sind immer **Personendaten**, also „Angaben über eine bestimmte oder bestimmbare natürliche oder juristische Person“ (Art. 2 Abs. 1 DSG). Darunter fallen namentlich:

- Immatrikulationsunterlagen
- Prüfungsunterlagen
- personenbezogene Dossiers wie Korrespondenz, Gesuche, Vermerke, Berichte und Evaluationen
- personenbezogene Forschungsdaten wie ausgefüllte Fragebögen und Befragungsprotokolle

Besonders schützenswerte Daten unterstehen mit Bezug auf die Anforderung an ihre Sicherung und die Voraussetzungen der Weitergabe besonderen Restriktionen. Solche Daten sind gemäss Art. 3 DSG namentlich solche über:

- die religiöse, weltanschauliche oder politische Ansicht, Zugehörigkeit und Betätigung sowie die Rassenzugehörigkeit
- den persönlichen Geheimbereich, insbesondere den seelischen, geistigen oder körperlichen Zustand
- Massnahmen der sozialen Hilfe oder fürsorgerischen Betreuung
- polizeiliche Ermittlungen, Strafverfahren, Straftaten und die dafür verhängten Strafen oder Massnahmen

3. Informationssicherheits- und Datenschutz-Konzept

Ist bekannt oder wird vermutet, dass Daten im Sinne der Datenschutzgesetzgebung in einer Organisationseinheit bearbeitet werden, muss eine Analyse respektive ein Konzept zu Informationssicherheit und Datenschutz (ISDS-Analyse respektive ISDS-Konzept) gemäss den Vorgaben des Amts für Informatik und Organisation (KAIO) erstellt werden.

Bei Fragen in diesem Zusammenhang steht die Security-Gruppe der Informatikdienste gerne zur Verfügung. Die ISDS-Vorlagen des KAIO können hier heruntergeladen werden:

<http://www.id.unibe.ch/content/dokumente/anleitungen/security/>

4. Umgang mit Daten

Personendaten dürfen nur dann und nur so weit bearbeitet (also gesammelt, verändert, weitergegeben etc.) werden, wie eine genügende gesetzliche Grundlage, ein **gesetzlicher Auftrag** hierzu besteht (Art. 5 DSG). Für besonders schützenswerte Daten muss die gesetzliche Grundlage besonders klar und der Bearbeitungsauftrag zwingend sein (Art. 6 DSG), während für die Bearbeitung der übrigen Personendaten

auch eine implizite Grundlage – also etwa die Ableitung aus dem Anstaltszweck und den Aufgaben der Universität – ausreicht.

Für die Datenbearbeitung zu **Forschungszwecken** gilt, dass Personendaten so zu anonymisieren sind, dass Rückschlüsse auf die betroffenen Personen unmöglich sind (Art. 15 DSGVO).

Die Universität ist für die Bearbeitung ihrer Daten selber **verantwortlich** (Art. 8 DSGVO); für Missbräuche muss sie – auch schadenersatzrechtlich – gerade stehen. Die Missachtung der Datenschutzgesetzgebung durch ihre Angehörigen kann die Universität somit teuer zu stehen kommen!

Personen, über die Daten bestehen, haben nach Abschluss allfälliger Verfahren (z.B. Prüfungen, Promotions- oder Habilitationsverfahren) grundsätzlich **Anspruch auf Einsicht** in ihr Dossier (Art. 21 DSGVO; zu den Einschränkungen dieses Grundsatzes vgl. Art. 22 DSGVO). Darauf ist bereits bei der Aktenherstellung zu achten; ehrverletzende oder herabsetzende Bemerkungen haben in amtlichen Akten unbedingt zu unterbleiben!

Während hängiger Verfahren gelten dagegen die Bestimmungen des Gesetzes vom 23. Mai 1989 über die Verwaltungsrechtspflege (VRPG; BSG 155.21).

5. Allgemeine IT-technische Grundsätze

Allgemeine technische Grundsätze sind Regeln, welche unabhängig vom Schutzgrad der Daten immer angewendet werden sollten:

- Kein Zugang zu Informatikmitteln ohne Passwort- oder Token-Schutz
- Zugriffs-Rechte auf Informatikmittel sauber regeln und periodisch überarbeiten
- Bauliche Bereiche von Informatikmitteln sichern
- Benutzer-Weisungen erstellen und kommunizieren (soweit nicht durch bestehende Weisungen der Universität abgedeckt)
- Backup-Strategie erarbeiten (auch unter dem Gesichtspunkt der Vertraulichkeit/Integrität der Daten)
- Entsorgungs-Strategie von Informatikmitteln regeln

6. Besonders schützenswerte Daten und deren IT-technischen Umgang

Besonders schützenswerte Daten sind zusätzlichen technischen Schutzmassnahmen im IT-Bereich zu unterwerfen, die einen unbefugten Zugriff verhindern. Solche Schutzmassnahmen können einzeln genügen, werden aber meist kombiniert angewendet, und beinhalten insbesondere:

- Absichern des lokalen Netzwerks durch geeignete Filter (Firewall, Paket-Filter)

- Gewährleistung der Vertraulichkeit/Integrität auf Datenträgern durch Verschlüsselung der Daten
- Gewährleistung der Vertraulichkeit/Integrität bei Datenübermittlung durch Verschlüsselung

7. Weiterleitende Links und Ansprechstellen

Die angeführten Rechtsgrundlagen finden sich unter der Link-Sammlung des Rechtsdiensts der Universität. Für Fragen im Zusammenhang mit dem Datenschutz wende man sich an den Rechtsdienst der Universität, Hochschulstrasse 4, 3012 Bern, info@rechtsdienst.unibe.ch.

Ausführliche technische Informationen sind unter der Link-Sammlung der Informatikdienste erhältlich. Für Fragen im Zusammenhang mit IT-Security oder ISDS wende man sich an die Security-Gruppe der Informatikdienste, Gesellschaftsstrasse 6, 3012 Bern, security@unibe.ch.

Datenschutzgesetz (KDSG): http://www.sta.be.ch/belex/d/1/152_04.html

Informatikdienste der Universität Bern
Bern, 4. Februar 2009