UNIVERSITÄT
BERN

Weisungen

Datenschutz im IT-Bereich der Universität Bern

Verteiler	Verwaltungsdirektion, IT-Verantwortliche, Informatikdienste
Klassifikation	Für internen Gebrauch
Dokumentenstatus	Freigegeben

Inhaltsverzeichnis

1. Grundsätzliches 3
1.1 Zweck 3
2. Datenschutz 3
3. Daten 3
3.1 Besonders schützenswerte Daten 3
4. Informationssicherheits- und Datenschutz-Konzept 4
5. Umgang mit Daten 4
6. Allgemeine technische Grundsätze der Informatik 4
6.1 Daten auf mobilen Datenträgern transportieren 5
6.2 Besonders schützenswerte Daten 5
6.3 Fernmeldegeheimnis 5
7. Kontakte 6
8. Links 6
9. Schlussbestimmungen 6
9.1 Widersprechende Bestimmungen 6
9.2 Inkrafttreten 6

1. Grundsätzliches

1.1 Zweck

Diese Weisungen sollen mithelfen, Daten im IT-Bereich in Bezug auf Verantwortlichkeit und Schutzwürdigkeit besser klassifizieren zu können, und liefern einige grundsätzliche Leitplanken, welche technischen Hilfsmittel sich für welche Schutzklasse eignen können.

Die Weisungen gliedern sich in einen rechtlichen und einen technischen Teil.

2. Datenschutz

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 Ergebnissen aus Umfragen
- als Erbringende von Dienstleistungen, etwa im Zusammenhang mit Krankengeschichten
- als Informatikbeauftragte im Zusammenhang mit Fragen des Datenzugangs und der Sicherung von Datenmaterial

Die Universität untersteht als öffentlich-rechtliche Anstalt des Kantons Bern der **kantonalen Datenschutzgesetzgebung**, namentlich dem kantonalen Datenschutzgesetz vom 19. Februar 1986 (KDSG; BSG 152.04). [1]

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."*

3. Daten

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

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

3.1 Besonders schützenswerte Daten

Besonders schützenswerte Daten unterstehen bezüglich ihrer Sicherung und Weitergabe besonderen Einschränkungen. Solche Daten sind gemäss Art. 3 KDSG 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

4. 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) erstellt werden.

Bei Fragen in diesem Zusammenhang kontaktieren Sie bitte die Informatikdienste. [2]

Wird eine Datenbank mit Personendaten angelegt, ist deren Eigentümerschaft verpflichtet, diese Datensammlung bei der Datenschutzaufsichtsstelle des Kantons Bern zu registrieren [3].

5. 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 KDSG). Für besonders schützenswerte Daten müssen die gesetzliche Grundlage besonders klar und der Bearbeitungsauftrag zwingend sein (Art. 6 KDSG), 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 KDSG).

Die Universität ist für die Bearbeitung ihrer Daten selber **verantwortlich** (Art. 8 KDSG); für Missbräuche wird sie – auch schadenersatzrechtlich – zur Verantwortung gezogen. Die Missachtung der Datenschutzgesetzgebung durch ihre Angehörigen kann für die Universität erhebliche Kosten verursachen.

Personen, über die Daten bestehen, haben nach Abschluss allfälliger Verfahren (z.B. Leistungskontrollen, Promotions- oder Habilitationsverfahren) grundsätzlich **Anspruch auf Einsicht** in ihr Dossier (Art. 21 KDSG; zu den Einschränkungen dieses Grundsatzes vgl. Art. 22 KDSG).

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

6. Allgemeine technische Grundsätze der Informatik

Die nachfolgend genannten allgemeinen technischen Grundsätze sind Regeln, welche unabhängig vom Schutzgrad der Daten immer angewendet werden müssen:

- Keine ungesicherte (unverschlüsselte) Übermittlung
- Kein Zugang zu Informatikmitteln ohne geeigneten Schutz (Passwort, Zertifikat, o.ä.)
- Zugriffs-Rechte auf Informatikmittel klar festlegen, einschränken soweit sinnvoll und möglich, periodisch überprüfen
- Nicht (mehr) verwendete Geräte, Services, etc. ausser Betrieb nehmen, deaktivieren, deinstallieren
- Die "Richtlinien der Informatikdienste für die sichere Entsorgung von IT-Datenträgern" sind einzuhalten [4]
- Wartung der Informatikmittel: Patch Management, Updates, Malware Protection, etc.
- Physischer Zugang zu Informatikmitteln sichern und einschränken
- 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)

6.1 Daten auf mobilen Datenträgern transportieren

Das Mitführen von Personendaten auf mobilen Datenträgern ist auf ein Minimum zu reduzieren und als Ausnahme zu verstehen. Beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (vgl. Art. 5 Abs. 1 Bst. c Datenschutzverordnung, DSV; BSG 152.040.1).

6.2 Besonders schützenswerte Daten

- Besonders schützenswerte Personendaten dürfen nicht unverschlüsselt in einer öffentlichen Cloud oder lokalen Datenspeichern abgelegt werden.; Der Datenstandort ist dabei irrelevant.
  Die Ablage ist einzig mit einer HYOK (Hold Your Own Key) Lösung zugelassen, bei welcher die Daten auf dem lokalen Client vor dem Transfer auf den Datenspeicher verschlüsselt werden. Der Schlüssel darf dem Anbieter des Datenspeichers nicht zugänglich sein
- Besonders schützenswerte Personendaten dürfen nicht unverschlüsselt per E-Mail versendet werden. Sie sind vor dem Versand mit einer HYOK (Hold Your Own Key) Lösung zu verschlüsseln, wobei der Schlüssel nur der sendenden bzw. empfangenden Partei bekannt sein darf
- Beim Eingang von besonders schützenswerten Personendaten per E-Mail, sind diese durch die Nutzenden aus der Mailbox zu entfernen und verschlüsselt auf einem geeigneten Datenspeicher abzulegen
- Die Kommunikation von besonders schützenswerten Personendaten im Betreff oder der E-Mail-Nachricht selbst, ist zu unterlassen. Dies gilt analog für alle genutzten Kommunikationsdienste

6.3 Fernmeldegeheimnis

Die über das UniNetz übertragene Information steht unter dem Schutz des Fernmeldegeheimnisses. Insbesondere gilt:

- Zufällig oder in Ausübung einer dienstlichen Tätigkeit erlangte Information oder auch nur die Tatsache deren Wahrnehmung ist geheim zu halten
- Es ist untersagt, sich Zugang zum UniNetz in der Absicht zu verschaffen, übertragene Informationen zu erlangen oder zu manipulieren, falsche Informationen einzubringen oder die Übertragung zu stören
- Es ist untersagt, sich Zugang zum UniNetz in der Absicht zu verschaffen, unberechtigten Zugang zu Endgeräten am UniNetz oder an damit verbunden Netzwerken, auch versuchsweise, zu erlangen oder vorsätzlich zu stören

7. Kontakte

Die angeführten Rechtsgrundlagen befinden sich unter der Link-Sammlung des Rechtsdiensts der Universität Bern. Für Fragen im Zusammenhang mit dem Datenschutz wende man sich an den

Rechtsdienst der Universität
Hochschulstrasse 6
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 sowie zu technischen Lösungen zur Verschlüsselung von besonders schützenswerten Personendaten wende man sich an die

Informatikdienste der Universität
Hochschulstrasse 6
3012 Bern

security@id.unibe.ch

8. Links

[1] https://www.belex.sites.be.ch/frontend/versions/1028

[2] http://id.unibe.ch

[3] https://www.jgk.be.ch/jgk/de/index/direktion/organisation/dsa/formulare_bewilligungen.html

[4] http://id.unibe.ch/rechtssammlung

9. Schlussbestimmungen

9.1 Widersprechende Bestimmungen

Bestehende, diesen Weisungen widersprechende Bestimmungen werden hiermit aufgehoben.

9.2 Inkrafttreten

Die vorliegenden Weisungen treten mit ihrer Genehmigung in Kraft.

Bern, 02.05.2023

Im Namen der Universitätsleitung
Der Rektor:

Prof. Dr. Christian Leumann