Directives

Data protection in the IT domain at the University of Bern

Distributor: Administrative Director's Office, IT Manager, IT Services Office
Class: For internal use
Document status: Approved
Table of contents

1. Basic information .................................................................................................................. 3
   1.1 Aim ................................................................................................................................. 3
2. Data protection and the academic community ..................................................................... 3
3. “Data” .................................................................................................................................. 3
   3.1 Sensitive data .................................................................................................................. 3
4. Information security and data protection plan ..................................................................... 3
5. Handling data ........................................................................................................................ 4
6. General technical principles for IT ...................................................................................... 4
   6.1 Data protection on the university network ...................................................................... 5
   6.2 Sensitive data ................................................................................................................ 5
   6.3 Telecommunications confidentiality ............................................................................... 5
7. Final provisions ..................................................................................................................... 5
   7.1 Conflicting provisions ................................................................................................... 5
   7.2 Entry into force .............................................................................................................. 5
8. References/links ..................................................................................................................... 6
1. Basic information

1.1 Aim

These directives are designed to enable the more effective classification of data in the IT domain according to level of responsibility and sensitivity. They provide basic guidelines as to which technical tools are best suited to which level of protection.

The directives are divided into legal and technical sections.

2. Data protection and the academic community

Everybody affiliated with the university occasionally comes into contact with "data", including:

- students, e.g. during their enrollment;
- examination officers, e.g. when announcing and archiving exam results;
- researchers, e.g. when dealing with survey findings or empirically obtained data relating to individuals;
- service providers, e.g. when consulting medical histories;
- IT officers, e.g. when handling data access requests and securing physical data.

As a public-law entity the university is subject to the cantonal data protection legislation of the Canton of Bern, specifically the Cantonal Data Protection Law of 19 February 1986 (KDSG; BSG 152.04): [1]

Data protection is the implementation of constitutional laws that safeguard personal rights, privacy and confidentiality. Article 13, paragraph 2 of the Federal Constitution of 18 April 1999 states: "Every person has the right to be protected against the misuse of their personal data."

3. Data

Within the meaning of data protection legislation, "data" signifies all personal data, i.e. "information about an identified or identifiable natural or legal person" (Art. 2, para. 1 KDSG). This includes:

- personal data;
- enrollment documents;
- exam papers;
- personal files such as correspondence, appeals, notes, reports and evaluations;
- personal research data such as completed questionnaires and interview transcripts.

3.1 Sensitive data

Sensitive data is subject to particular restrictions in terms of its security and distribution. Under Art. 3 KDSG, sensitive data is specifically that which concerns:

- a person's religious, ideological or political beliefs, affiliations or activities, and ethnicity;
- personal privacy, in particular a person's physical, mental or psychological condition;
- social care or welfare support arrangements;
- police investigations, criminal proceedings, offenses and any punishments or other measures subsequently imposed.

4. Information security and data protection plan

If it is known or suspected that data is processed in an organizational unit within the meaning of data protection legislation, an information security and data protection (ISDP) analysis or plan must be established according to the instructions of the Department of Informatics and Organization (KAIO).

If you have any questions in this regard, please contact the IT Services Office.
If a new database containing personal data is created, the owner of that database is obliged to register it with the supervisory authority for data protection. Databases can be registered via the Legal Services Office using the following e-mail address: info@rechtsdienst.unibe.ch

5. Handling data

Personal data may only be processed (i.e. collected, modified, distributed, etc.) where and to the extent that a legal mandate provides a sufficient legal basis to do so (Art. 5 KDSG). For sensitive data, the legal basis must be particularly clear and the need to process that data compelling (Art. 6 KDSG). For the processing of all other personal data, an implicit basis – e.g. one derived from the institutional purpose and functions of the university – is sufficient.

Where data is processed for research purposes, personal data must be redacted such that no conclusions can be drawn about the person in question (Art. 15 KDSG).

The university is itself accountable for the processing of its data (Art. 8 KDSG) and must take responsibility for misuse, including the payment of any damages. The university could face significant costs if those affiliated with it fail to comply with data protection legislation.

Individuals about whom data exists have the right to access their file on completion of any processes (e.g. assessments of academic achievement, doctoral or post-doctoral processes) (Art. 21 KDSG; for restrictions of this principle see Art. 22 KDSG).

However, during ongoing processes, the provisions of the Administrative Justice Law of 23 May 1989 (VRPG; BSG 155.21) apply.

6. General technical principles for IT

General technical principles are rules, which must consistently be applied, regardless of data protection level:

- no unsecured (unencrypted) transmission;
- no access to IT resources without appropriate protection (password, certificate, etc.);
- clear rules on the right to access IT resources, restrictions where necessary/feasible, periodic checks;
- shutdown, deactivation, uninstallation of any devices, services, etc. not being used (any longer);
- no storage on externally controlled media/services (clouds);
- no unnecessarily held on mobile data carriers, e.g. CDs, laptops, smartphones, etc.;
- maintenance of IT resources: patch management, updates, malware protection, etc.;
- secure and restricted physical access to IT resources;
- production and distribution of user directives (for subjects not already covered by existing university directives);
- development of a backup strategy (including for data confidentiality/integrity);
- compliance with the Richtlinien der Informatikdienste für die sichere Entsorgung von IT-Datenträgern sind einzuhalten (guidelines on the secure disposal of electronic data carriers) [2].
6.1 Data protection on the university network

- Where a user group uses another secure local network in parallel to the university network, the two connections must be kept physically separate. Users may directly connect to either the university network or a secure network segment, but not both at the same time.

6.2 Sensitive data

- Sensitive data used for research, services and administration, in particular sensitive personal data within the meaning of Art. 3 KDSG, must not find its way onto the university network.
- Exceptions from this rule are only possible where data communication hardware and software allows only a single encrypted and authenticated data exchange with the terminal device in question.
- Terminal devices holding unencrypted sensitive data must not be directly connected to the university network.
- Where sensitive data is held on a terminal device, user groups are obliged to take adequate measures to protect that data.
- Sensitive data is subject to additional technical protective measures in the IT domain. While those measures may suffice individually, they are generally combined. Specifically, they include:
  a) protection of the local network with a suitable filter (firewall, packet filter);
  b) protection of data confidentiality/integrity on data carriers through encryption;
  c) protection of data confidentiality/integrity during transmission through encryption.

6.3 Telecommunications confidentiality

- Information transmitted via the university network is protected under telecommunications confidentiality. In particular:
  d) information acquired incidentally or in the course of one’s work, including mere awareness of that information, is to remain confidential;
  e) it is forbidden to access the university network with the intention of acquiring or manipulating transmitted information, introducing false information or interfering with transmission;
  f) it is forbidden to access the university network with the intention of gaining unauthorized access to or deliberately interfering with terminal devices on the university network or connected networks, or attempting to do so.

7. Final provisions

7.1 Conflicting provisions

Any existing provisions, which conflict with these directives are hereby repealed.

7.2 Entry into force

The present directives enter into force upon approval.
8. References/links

The legal bases mentioned above can be found in the link directory of the university's Legal Services Office. If you have any questions about data protection, please contact the university's

Legal Services Office
Hochschulstrasse 6
3012 Bern
info@rechtsdienst.unibe.ch

Extensive technical information is available via the link directory of the IT Services Office. If you have any questions about IT security or ISDP, please contact the

IT Services Office
Hochschulstrasse 6
3012 Bern
security@id.unibe.ch


Bern, 2/14/2017

For the Executive Board of the University of Bern
The Rector:

Prof. Dr. Christian Leumann