UNIVERSITÄT BERN

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

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 some 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

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 February 19, 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 April 18, 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” always 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 Highly sensitive data

Highly sensitive data is subject to particular restrictions in terms of its security and distribution. Under Art. 3 KDSG, highly sensitive data is 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 concept must be established.

If you have any questions in this regard, please contact the IT Services Office [2].

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 of the canton of Bern [3].

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 highly 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, on the other hand, 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 May 23, 1989 (VRPG; BSG 155.21) apply.

6. General technical principles for IT

The general technical principles set out below 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);
- compliance with the “Richtlinien der Informatikdienste für die sichere Entsorgung von IT-Datenträgern” (IT Services Office guidelines on the secure disposal of electronic data carriers) [4].
- 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);

6.1 Transporting data on mobile data carriers

Having personal data on mobile data carriers shall be reduced to a minimum and be understood to be an exception. In case of transportation, data must be protected from unauthorized read, copy, modify and/or delete. (cf. Art. 5 Abs. 1 Bst. c Datenschutzverordnung, DSV; BSG 152.040.1)

6.2 Highly sensitive data

- Particularly sensitive personal data may not be stored unencrypted in a public cloud or local data storage device; the data location is irrelevant.
  Storage is only permitted with an HYOK (Hold Your Own Key) solution in which the data is encrypted on the local client before being transferred to the data storage device. The key must not be accessible to the data storage provider;
- Particularly sensitive personal data may not be sent unencrypted by e-mail. This data must be encrypted before being sent with an HYOK (Hold Your Own Key) solution, and the key must only be known to the sending and/or receiving party;
- When particularly sensitive personal data is received by e-mail, the data must be removed from the in-box by the users and stored in encrypted form on a suitable data storage device;
- Particularly sensitive personal data must not under any circumstances be communicated in the subject line of a mail or in the e-mail message itself. This applies similarly for all communication services used;

6.3 Telecommunications confidentiality

Information transmitted via the university network is protected under telecommunications confidentiality. In particular:

- information acquired incidentally or in the course of one’s work, including mere awareness of that information, is to remain confidential;
- it is forbidden to access the university network with the intention of acquiring or manipulating transmitted information, introducing false information or interfering with transmission.
- 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. Contacts

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 or on technical solutions for encrypting particularly sensitive personal data, please contact the

IT Services Office
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. Final provisions

9.1 Conflicting provisions

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

9.2 Entry into force

The present directives enter into force upon approval.

Bern, 02/05/2023

For the Executive Board of the University of Bern

The Rector:

Prof. Dr. Christian Leumann