University of Zurich[UZH]

Legal Department and Data Privacy

University of Zurich
Department of Data Protection
Hirschengraben 56
CH-8001 Zurich

privacy@rud.uzh.ch
www.rud.uzh.ch

Version January 2020

Fact Sheet – Data Protection Principles

1. Lawfulness and Proportionality (§ 8 IDG)

UZH is permitted to process personal data only as appropriate and necessary in the fulfilment of its legal duties. The purpose and duties of UZH are set down in general in § 2 of the University Act (UniG of 15 March 1998) as follows:

- Conducting research and providing teaching and research-related services in the interests of the general public;
- Providing an academic education and, in this connection, creating a framework for pursing scholarly careers and activities;
- Fostering continuing academic education and promoting junior researchers.

Consent should only be used as a legal basis for data processing within the UZH by way of exception (e.g. when it is unclear whether data processing is appropriate and necessary).

2. Data Minimisation and Data Economy (§ 11 IDG)

Data processing systems and programs must be designed to ensure that

- No personal data is gathered and processed that is not necessary for the fulfilment of duties (§ 11 para. 1 IDG), and
- Personal data is deleted, anonymized, or partially anonymized as soon as possible and to the extent possible (§ 11 para. 2 IDG), and
- If the data cannot be anonymized partially or completely, it must be pseudo-anonymized as soon as possible and to the extent possible.

3. Transparency (§ 12 IDG)

The collection of personal data in itself as well as the purpose of its processing must be apparent to the data subjects from the circumstances. If the purpose for which the data is processed is not evident from the circumstances, the individuals whose data were procured must be notified accordingly. Violations of this principle or the principle of lawfulness include, for instance, unauthorized covert data collection via the manipulation of programs or unauthorized telephone surveillance.

When collecting sensitive personal data, the owner of the data file must explicitly inform the data subject of the purpose for which the data is being processed.

The principle of transparency also entails that data subjects should be immediately notified if his or her personal data have been unlawfully disclosed, modified or destroyed and the data subject is thus in danger of having his or her rights or legitimate interests impaired (i.e. material or immaterial damage such as economic disadvantages or damage to reputation). It is sufficient if such an occurrence can be assumed with a certain degree of likelihood on the basis of actual points of reference (e.g. if laptops or other data storage devices are lost in places where they are accessible to third parties or if data is stolen or accessed illegally from IT systems and the data and/or data storage devices were not encrypted).

In such cases, the data subject must receive notification concerning:

- When and what data have been disclosed, modified, or destroyed, and
- When this was ascertained, and
- What immediate steps were taken, for example, to remedy the cause of a data leak, and
- What preventive or damage limitation measures (such as changing passwords) have been recommended to mitigate potential further adverse consequences.

The data subject may not be notified if, and for as long as, investigations by law enforcement authorities are jeopardized.

4. Principle of Purpose Limitation (§ 9 para. 1 IDG)

Personal data may be processed only for the purpose specified when they were collected, for purposes made evident by the circumstances, or as provided for by law. (e.g. master data on staff collected for the purposes of hiring may not be reused for commercial purposes).

Personal data must be deleted, destroyed, or anonymized if:

- The data is no longer required for the originally specified purpose, and
- The statutory retention periods applicable to the records have elapsed, and
- The data is not, or no longer, required for the purposes of legal or court proceedings, and
- The relevant (final) archive to which the data were offered once the retention period elapsed has not taken over and archived the data.

The data may be disclosed for other purposes only if a statutory provision provides for their use for another purpose or if the consent of the data subject has been obtained for the case in question.

5. Principle of Data and Information Security (§ 7 IDG)

Measures to protect data and information must be based on the following objectives:

- Information may not be disclosed unlawfully; in other words, it must remain confidential and be protected from accidental or unlawful access, alteration, or disclosure. This also means that access to personal data may be granted only on a need-to-know basis to persons required to access personal data on the basis of their position and duties.
- Information must be accurate and complete; this means that incorrect or incomplete personal data must be deleted, corrected, or updated.
- Information must be available on demand; in other words, it must be protected from loss and destruction.
- The processing of information must be attributable to a specific person.
- Alterations to information must be evident and traceable.

The measures taken must be commensurate with the type of information, the type and purpose of their use, and the currently available technology.

6. Outsourcing Data Processing (§ 6 IDG)

In the absence of legal provisions or contractual agreements to the contrary, the processing of information may be delegated to third parties.

Outsourced assignments must be issued in writing and incorporate the relevant terms and conditions (see the UZH Package Solution on our website).

Outsourced assignments must be monitored to ensure that the contractual requirements have been fulfilled and the necessary corrections made, if necessary.

7. Cross-Border Disclosure of Personal Data (§ 19 IDG)

Personal data may be disclosed to recipients who are not subject to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data if:

- The recipient state can assure an appropriate level of data protection (see the list of states from the federal commissioner in French or German), or
- A legal framework allows a disclosure to protect specific interests of the data subject or predominantly public interests, or
- The public body in question has adopted appropriate contractual security measures.

8. Principle of Ensuring the Rights of Data Subjects and Access to Information (§§ 20, 21, 22, 28 IDG)

Data subjects can require from UZH that (§§ 21, 22 IDG):

- inaccurate personal data be corrected or destroyed,
- unlawful processing of personal data be ceased,
- the consequences of unlawful processing be redressed,
- the unlawfulness of processing be ascertained, and
- the disclosure of personal data to private individuals be blocked if the public body in question is able, on the basis of a special statutory provision, to disclose personal data without preconditions.

Steps must be taken to ensure that UZH processes and responds to the following within 30 days:

- Requests for access to information in accordance with the principle of public access to information (§ 20 para. 1 IDG), and
- Requests from data subjects for access to their own personal data present at UZH (§ 20 para. 2 IDG).