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 August 2018

Checklist – Data Protection at Work

The following checklist provides basic guidelines for dealing with personal data in your daily work at UZH.[1]

1. Data Protection Principles

☐ I understand that **the processing of personal data is subject to restrictions** under data protection law; particularly relevant for UZH are the restrictions set down in the **Act on Information and Data Protection** (IDG[2]) and the **Ordinance on Information and Data Protection** (IDV[3]) **of the Canton of Zurich**.

☐ I understand that **data protection** covers the **protection against misuse of an individual's data**, including the **right of every individual** to **decide independently what happens to data relating to his or her person**.

☐ I understand that **personal data** refers to data related to an **identified or identifiable natural person or legal entity**.

- A person is deemed to be **identified** if their identity is directly apparent from the data. In most cases this pertains to information containing concrete mention of a person's name, address, or date of birth; it is also applicable when a photo is provided with the information in, for example, a personnel file, passport, tax document, or an official certificate.

- A person is deemed to be **identifiable** if their identity can be inferred without undue effort by combining the information with other information. Such information includes: an ID number, student number, bank account number, insurance policy number, a phone number, or an e-mail or IP address. Regarding such information, registers are available that enable these data to be used for identification purposes.

☐ I understand that **data processing** covers practically **any instance where personal data are handled**, for example, the collection, storage, use, modification, disclosure, or destruction of personal data. Disclosure is deemed to be any instance in which access to personal data is granted, for example, permission to inspect, forward, or publish personal data.

☐ As a UZH employee, **I may only process personal data as required by my job or area of responsibility**.

☐ If required, I can use the **learning program developed by the Data Protection Officer of the Canton of Zurich**[4] to improve my **knowledge** of the principles of data protection.

---

[1] This checklist is based on material contained in the learning program developed by the Data Protection Officer of the Canton of Zurich (https://review.datenschutz.ch/datenschutz/), and issue 4 of "backUp," the IT security magazine published by the Schleswig-Holstein independent state data protection center (https://www.datenschutzzentrum.de/uploads/it/backup04.pdf).
[2] IDG: http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.4
[3] IDV: http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.41
[4] Learning program of the Data Protection Officer of the Canton of Zurich (in German): https://review.datenschutz.ch/datenschutz/

2. My Computer and My Workplace

☐ I **choose my password in accordance with the guidelines laid down by the Office for Information Technology**.[5] I furthermore keep my password secret and do not reveal it to third parties, including work colleagues, my superior, my IT support officer, and my IT administrator.

☐ I keep **data, documents** (e.g. correspondence and printouts), and **data carriers** (e.g. CDs, USB sticks, memory cards, and external hard disk drives) containing personal data **under lock and key** (e.g. in a filing cabinet or desk drawer) when I'm not working on them.

☐ Whenever I leave my workspace during working hours, **I lock the screen of my computer**. When I finish work for the day, **I log out and shut down my computer**.

☐ I have installed a **password-protected screen saver that switches on automatically** after a certain period of time.

☐ On leaving the office, **I lock the door**.

☐ I keep my **badge and the keys** to my office, filing cabinet, and desk drawer **in a safe place**. I ensure that the screen of my computer is set up so that no unauthorized person can read what is on the screen.

☐ I ensure that **I only have visitors in my office when I am present**, and I ensure that they **cannot gain unauthorized access to any personal data** (e.g. in documents or on my computer screen).

☐ I do **not print out any personal data on an unsupervised printer** and **do not leave printouts lying in the printer for longer than necessary**.

3. Handling Work and Private Data

☐ I understand that **all personal data I process when using UZH's work infrastructure or equipment are in principle deemed to be UZH data and thus qualify as official data**.

☐ I understand that **UZH data**:

- Are **in principle** subject to **official secrecy** and may under certain circumstances also be subject to **professional confidentiality** (e.g. regarding doctors, dentists, and psychologists) or **manufacturing or trade secrecy**;
- May only be **processed for official work purposes**;
- May only **be processed** and **stored** on **devices that are protected from unauthorized access**; this applies both in case of access by means of work devices and in case of access by means of private devices; this is also to be considered, as far as I do not access work e-mails via webmail of the UZH, via IBM Notes or via IBM verse[6].

[5] Password guidelines (in German): https://www.zi.uzh.ch/de/support/identitaet-zugang/manage-password.html
[6] Verse: https://www.zi.uzh.ch/de/support/e-mail-kollaboration/mobiles.html

- May not **be processed** or **stored** via an **infrastructure offered by external providers** (e.g. cloud providers) if the data protection provisions of UZH are not fully observed.[7]

☐ I **do not redirect or forward any work e-mails to my private e-mail account**; I only forward a **work e-mail to an external e-mail address if the recipient is authorized** to receive the message **via the external e-mail address**.

☐ To ensure **that e-mail is available and easily retrieved**:

- **I move business relevant work e-mails** from my own assigned e-mail account **to a MailIn account**, as far as such account is required and available for the function and as far as the e-mails must be accessible to the deputy;
- **I move business relevant work documents in electronic form to a folder assigned to me** (on a drive of UZH's own servers or on the server of an authorized UZH external data processing provider); as far as the documents must be accessible to the deputy;
- **I ensure that**, during an absence, **my deputy has access to the MailIn account and the assigned folder**.

☐ **Business-relevant** are such documents and information, which are **indispensable for the traceability of the course of the business**; the **decision** as to whether documents and information are indispensable in this sense **is borne by the respective employee of UZH**.

☐ I transfer **all business relevant official, work-related information and documents to an** (electronic or physical) **folder** in accordance with the guidelines, as far as my office/organizational unit has issued such guidelines for the organized storage and management of records.[8]

☐ To **avoid mixing private and work data** and any resulting issues, for example, the **unwanted disclosure of details of my private life** if my IT support officer or IT administrator accesses my data, I **limit my use** of UZH's work infrastructure and equipment **for private purposes**.

☐ **If** I nevertheless **process private data on UZH work equipment, I clearly designate such data as private.** I achieve this by **moving**:

- **Private e-mails to a sub-folder** of my own assigned e-mail account, which I name "**PRIVATE**";
- **Private information and documents to a folder assigned to me for personal use**, which I name "**PRIVATE**."

[7] Outsourcing Data Processing: http://www.dsd.uzh.ch/de/outsourcing.html
[8] Fact sheet on managing files and folders (in German): http://www.archiv.uzh.ch/dam/jcr:ffffffff-e406-9649-0000-000046c958ba/2014_04_01_uaz_merkblatt_aktenfuehrung.pdf

4. Disclosing Personal Data

☐ If I receive **requests to access information** in accordance with § 20 para. 1 and para. 2 IDG **and requests for legal or administrative assistance**, I **contact** the **Delegate for Data Protection of UZH**, who will decide how to proceed.

☐ Before sending an e-mail, I **ensure the e-mail distribution list is correct**.

☐ I send **information containing sensitive personal data**[9] or subject to **professional confidentiality**[10] to both members of UZH and external recipients:

- In electronic form **only via encrypted e-mail**;
- In physical form **only in a sealed envelope** marked “confidential”;
- **Never by fax** (in exceptional cases, arrangements must be made by phone to ensure the recipient is present and ready to receive the fax with no delay).

5. Outside the Office

☐ If my position and duties require that I process **official data**, in particular personal data, **outside my office** (e.g. if I have a meeting outside the building, am traveling for work, or am working from home), I only take with me, or access from outside the office, **the data that I need to perform the concrete tasks in question,** and **I ensure that these data are protected from unauthorized access and disclosure**.

☐ **In public**, especially in airports, train stations, or on mass transit such as buses or trains:

- I **do not hold confidential conversations** (face-to-face or on the phone);
- I **only edit confidential data on my laptop if it is equipped with a privacy screen** (e.g. a screen protector from 3M) in order to prevent a person sitting next to me from reading the screen.

☐ Regarding my work **laptop**, work **mobile phone**, and **work documents**:

- I **never** leave them **unattended**;
- I do **not** leave them lying **in the car in plain view**;
- I keep them **under lock and key in hotels** (e.g. in the hotel safe) **or at home**.

[9] Sensitive personal data comprise information that is particularly vulnerable to a breach of privacy due to its significance, the manner of processing, or the possibility to link it with other information. This includes information on religious, ideological, political or union-related views and activities, information on health and the intimate sphere, racial or ethnic origin, use of social benefits, and/or administrative or criminal proceedings or sanctions. Sensitive personal data also include collections of information that enable a compilation of key personality traits of a private individual (personality profile).
[10] Professional confidentiality is a statutory duty of confidentiality that applies to certain professional groups at UZH and their ancillary staff. Such professional groups include doctors, dentists, and psychologists.

6. Trust Is Good; Control Is Better

☐ I understand that **as a UZH employee**, I am **in possession of confidential information** that could be of interest to other people. To gain access to this information, interested persons might resort to methods ranging from eavesdropping, reading an e-mail over my shoulder, or simply hearing about the content of a document on to electronic eavesdropping via the Internet using spyware, phishing, or other means.

☐ When dealing with **confidential matters I clarify the identity of unfamiliar people**:

- Who call me on the phone by, for example, agreeing to call them back;
- Who seek me out in person before I have given them access to UZH premises or documents by, for example, requesting their name and their office or organizational unit, and by asking them to show their work ID.

☐ I make an effort to **contact the** (purported) **sender of a message personally** by, for example, phoning them if I:

- **Receive e-mail with surprising or unusual content** (before I respond);
- **Receive e-mail with data attachments I was not expecting** (before I open the attachment).

☐ **If** I am **unsure** about an incident, I:

- Talk to my superior to clarify **the confidentiality of a piece of information**;
- Talk to my superior to clarify **the authorization of an external person or co-worker at UZH**; and
- Talk to my IT support officer to clarify **computer-related issues**.

☐ I **never connect electronic data carriers I find or am given by unknown persons**, in particular USB sticks or memory cards, **to my work computer**.

7. Deletion or Destruction of Personal Data

☐ I **regularly check to see what data I no longer require** to perform my professional duties.

☐ I ensure that I **delete or destroy personal data** if:

- They are **no longer required for the originally specified purpose**; and
- The **statutory retention periods** applicable to the records **have elapsed**; and
- The **data are not** (or no longer) **required as evidence** in the scope of legal or court proceedings; and
- The **UZH Archive**, to which I offered the data once the retention period has elapsed, **have not taken over and archived the data**.

☐ I undertake to **delete or destroy personal data** in such a way that **unauthorized use thereof is no longer possible**. I therefore:

- Do **not dispose misprints or documents containing personal data in the wastebasket**. Misprints and documents of this sort must be shredded immediately or disposed of in a closed container used to collect documents for proper destruction;
- Do **not dispose data carriers (e.g. CDs, USB sticks, memory cards, or hard disks)** that are to be discarded or destroyed **in the wastebasket**; I hand them over to the IT section responsible for unit to ensure secure official disposal. The Office for Information Technology ensures that the information stored on the data carriers can no longer be read or that the data carriers are destroyed.