universität wien

Data Protection Guideline of the University of Vienna

Version: November 2018

TABLE OF CONTENTS

Glossary

DLE – service unit

DPO – Data Protection Officer (https://dsba.univie.ac.at)

DPA – Data Protection Act

GDPR – General Data Protection Regulation

IT representative – organisational unit's contact person for IT-related enquiries

Faculty representative – contact person for IT-related enquiries at the faculty

intra.univie.ac.at – intranet of the University of Vienna

ZID – Vienna University Computer Center

1. Introduction – Objectives of the Data Protection Guideline

Various international and national legal foundations, such as the General Data Protection Regulation of the EU (henceforth abbreviated as **GDPR**), as well as different national legislations regulate the processing of personal data, the rights of data subjects and the obligations of the relevant controller, as well as the applicable data protection measures for the processing of personal data.

This Data Protection Guideline aims at providing university employees with information about data protection and the handling of personal data at the University of Vienna to prevent violations against data protection provisions.

For the sake of completeness, we would like to point out that this Data Protection Guideline does not apply to data that do not contain any personal reference.

Please find further **information about the processing of personal data** on the intranet of the University of Vienna (https://intra.univie.ac.at/shortened/dsgvo/)

All employees of the University of Vienna are obliged to comply with the measures described in this Data Protection Guideline and to act in accordance with the resulting requirements and guiding principles. Employees violating the provisions (and prohibitions) specified in this Data Protection Guideline may face legal consequences under penal or labour law.

2. Data protection at the University of Vienna

In accordance with article 1, para. 1 of the GDPR (see General Data Protection Regulation handbook on the intranet of the University of Vienna https://intra.univie.ac.at/fileadmin/download/EU_General_Data_Protection_Regulation_(GDPR).pdf), the GDPR aims at protecting the fundamental rights and freedoms of individuals, in particular the right to the protection of personal data. Data protection provisions apply to the processing, i.e. the collection, storing and use of personal data. Simply put: Data protection legislation aims at protecting the personality rights of every individual (e.g. of every student, website user or yourself). They do not only protect personal data, but also the individuals themselves through a more careful approach in handling the data related to them.

2.1. Object of the GDPR – Personal data and special categories of personal data

Personal data in accordance with article 4, number 1 of the GDPR are any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified directly or indirectly (e.g. by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person). This includes, in particular, data such as name, address, marital status, date of birth, citizenship, profession, religious denomination, as well as income and financial situation. Processing (including collection, storage, use) of personal data is only permissible if the GDPR, the Data Protection Act (henceforth abbreviated as **DPA**) as amended or any other legal provisions permit or demand it.

The GDPR provides special protection to special categories of personal data. Article 9, number 1 of the GDPR defines special categories of personal data as personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership", as well as genetic data, biometric data for the purpose of uniquely

identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. In addition, special stipulations apply to the processing of personal data relating to criminal convictions and offences, as defined in article 10 of the GDPR.

The special categories of personal data mentioned above may only be processed under even stricter conditions. In some circumstances, they are subject to data protection impact assessments carried out by the data protection officer in accordance with article 35, para. 1, 2, 3, letter (b) of the GDPR (see item 4.3).

2.2. Appointment of a data protection officer

In accordance with article 37, para. 1 letter (a) of the GDPR, the University of Vienna is obliged to appoint a data protection officer (henceforth abbreviated as **DPO**). Articles 38 and 39 of the GDPR define the position and tasks of the data protection officer.

The DPO of the University of Vienna is the contact person for all matters regarding data protection for the Rectorate and university staff. The DPO provides advice if there are any doubts regarding data protection. For further information, please go to https://dsba.univie.ac.at/ (in German).

2.3. Data protection obligation

Persons responsible for the processing of personal data are not allowed to process personal data in an inadmissible manner. Every employee of the University of Vienna is reminded of data protection by means of this Data Protection Guideline as well as additional relevant information provided by the DPO and on the intranet. S/he is obliged to act accordingly.

2.4. Technical and organisational implementation of data protection

In accordance with article 32 of the GDPR, the University of Vienna has to implement appropriate technical and organisational measures to ensure compliance with the provisions of the GDPR. The measures taken have to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems (including the ability to restore the availability of personal data in the event of a physical or technical incident) in the context of data processing.
The University of Vienna ensures compliance with these requirements by implementing appropriate methods and processes (for further information, see https://zid.univie.ac.at/it-security/, in German). If you have concerns regarding the security of data processing activities at the University of Vienna, please contact the DPO and/or the IT security of the Vienna University Computer Center (henceforth abbreviated as **ZID**).

3. Data protection measures taken by the University of Vienna

To ensure compliance with the applicable data protection provisions, the University of Vienna has defined the following methods and processes. University employees have to observe and comply with these. Other policies and documents referred to in this Data Protection Guideline form an integral part of it and have to be complied with.

In addition, employees who process personal data or are responsible for the processing of personal data have to complete training courses on data protection (unless the relevant employee already has the necessary knowledge or has completed training courses on data protection before).

You can find current course dates as well as a video tutorial on the intranet of the University of Vienna at https://intra.univie.ac.at/shortened/dsgvo.

3.1. Handling of personal data

The following rules apply to the handling of personal data.

3.1.1. Fundamental regulation on the transfer of personal data

Personal data are protected. You have to be authorised to process personal data. Note that you may not transfer personal data to third parties without a legal basis. Therefore, please check if you are in doubt. This provision also applies to verbal and telephone communication. If you have confidential conversations, please make sure that no unauthorised person(s) can overhear.

3.1.2. Storing documents entrusted to you

Employees entrusted with documents containing personal information have to store them in a way that guarantees that no unauthorised party can access them. For further information, please go to the intranet of the University of Vienna at https://intra.univie.ac.at/shortened/dsgvo.

3.1.3. Waste-paper baskets

From a data protection point of view, waste-paper baskets are sensitive facilities. You are not allowed to throw in the waste-paper basket any personal information that is worth protecting. You have to use separate closed disposal containers or destroy the relevant documents in a suitable shredder.

3.1.4. Disposal of electronic data storage media and data

You may not throw away electronic data storage media containing personal data (e.g. CDs, DVDs, external hard disks, memory cards, flash drives, laptops and PCs) into the household waste. Competent persons or companies have to take care of the disposal of the data storage media and devices mentioned above. For further information, please contact the IT representative, the ZID or the Facility and Resources Management unit.

3.2. Clean desk

Unless you have your own office that you can lock when you are not at work, you have to ensure that any personal information that is worth protecting as well as special categories of personal data (article 9, para. 1 of the GDPR, see item 2.1) are protected appropriately.

The Rahmenbetriebsvereinbarung Daten (University of Vienna framework agreement on the use of personal data) as well as the associated supplementary agreement define the different categories of personal data. You can find these documents on the intranet of the University of Vienna under https://intra.univie.ac.at/fileadmin/upload/personalwesen/Betriebsvereinbarungen/Rahmenbetriebsvereinbarung_RBV-Daten.pdf (University of Vienna framework agreement, in German) and https://intra.univie.ac.at/fileadmin/upload/personalwesen/Betriebsvereinbarungen/Zusatzvereinbarung_zur_RBV-Daten.pdf (supplementary agreement, in German).

3.3. Screen, printer and copying machine

Set up screens and printers in a way (if structurally possible) that ensures that no unauthorised persons can view and access the devices. This also includes locking your workplace computer or laptop when you leave your desk. Do not leave printouts containing personal data unattended in the printer. Collect them as soon as printing is done. This also applies to copying machines. You may not leave poor copies or original documents unattended if they contain personal information that is worth protecting.

3.4. Workplace computers and mobile devices

3.4.1. Using hardware and software

You have to encrypt mobile devices such as notebooks, smartphones or tablets with which you process personal data and protect the log-in with a password/PIN in accordance with the current state of the art.

Guidelines for encrypting different operating systems
Windows https://support.microsoft.com/en-gb/help/4028713/windows-10-turn-on-device-encryption
Apple https://support.apple.com/en-gb/HT204837
Linux https://wiki.ubuntuusers.de/LUKS/ (information in German)

Guidelines for encrypting smartphones and tablets
https://www.ispa.at/wissenspool/broschueren/broschueren-detailseite/broschuere/detailansicht/bewerben-und-internet.html (information in German)

Make sure that unauthorised parties cannot read along or overhear personal data when you use mobile devices.

3.4.2. Storing and erasure of personal data

Storing personal data is only permissible if there is a legal basis for it (e.g. legal basis pursuant to the Universities Act).

The organisational units of the University of Vienna, such as service units (henceforth abbreviated as **DLE**), have to develop concepts and routines for the erasure of data. You can find a list of erasure periods on the intranet of the University of Vienna under the menu item Data protection compliance programme (https://intra.univie.ac.at/shortened/dsgvo). The DPO provides assistance to organisational units in developing concepts and routines for the erasure of data.

3.4.3. Using private devices (Bring Your Own Device – BYOD)

Using private devices for university purposes is generally permissible. However, you have to ensure compliance with the applicable data protection provisions. If you are in doubt, please consult with the IT representatives and/or the DPO.

If you fear that university-related personal data might have fallen into the hands of third parties, you have to immediately notify the University of Vienna (superior and DPO). This may be the case if you lost your device or if it was stolen or has disappeared.

3.4.4. Flash drives, CDs, DVDs, external hard drives, memory cards and other mobile electronic data storage media

According to the data protection provisions, storing personal data on private flash drives, CDs, DVDs, external hard drives, memory cards and other mobile electronic storage media is permissible. If you are in doubt, please consult with the IT representatives and the DPO. You have to encrypt external mobile storage media that you use to process personal data in accordance with the current state of the art. You can find guidelines under: https://zid.univie.ac.at/en/it-services-of-the-zid/it-security-in-german/cryptography/encrypted-containers-in-german/ (in German)

3.4.5. Using file and cloud services

If you do not only use cloud services offered by the University, but also file and cloud services offered by external providers, you have to make sure that the relevant service provider complies with the technical and organisational measures pursuant to the GDPR. If you are in doubt, please contact the DPO.

Special regulations apply if personal data are transferred to countries outside the EU/EEA (i.e. third countries) and if the data can be accessed from these countries in any other form. If you are in doubt, please contact the DPO.

3.5. Using server infrastructure

You have to ensure compliance with the data protection provisions when using systems that are not centrally managed. If you are in doubt, please consult with the IT representatives and the DPO.

3.6. Maintaining websites

The University of Vienna provides the central content management system (CMS) TYPO3. We recommend using this system to maintain your websites. You have to appoint an administrator for all websites that are not operated via the central CMS. S/he has to ensure (in particular in view of the known and unknown risks on the Internet) that the relevant CMS meets up-to-date security standards and is carefully maintained and checked at regular intervals.

3.7. Remote access to the University of Vienna's infrastructure

Remote access (access from outside the University of Vienna) to the IT infrastructure of the University has to be encrypted in any case. When setting up remote access for third parties, the employee has to make sure that it is encrypted.

3.8. Entries in the record of processing activities of the University of Vienna

Any processing activities in accordance with article 30, para. 1 or para. 2 of the GDPR have to be entered in the University of Vienna's record of processing activities (available at https://verarbeitungsverzeichnis.univie.ac.at). If the record already contains a superordinate entry for the same processing activity (with the same purpose), you should not make a new entry. If it is a new type of processing activity, you have to find out whether a data protection impact assessment is necessary. If you are in doubt, please contact the DPO.

3.9. E-mail system and Internet

According to the University of Vienna's Code of Conduct (available on the intranet of the University under https://intra.univie.ac.at/themen-a-z/initiale/c/thema/code-of-conduct-1), you may also use the e-mail system of the University for private purposes. Employees are allowed to use their workplace Internet access and their personal e-mail address for private purposes to a limited extent, as long as it does not compromise the quality and quantity of their official task fulfilment, as well as the availability of the Internet access for official purposes. This agreement may be revoked at any time.

When using a web browser, you have to make sure that your communication is encrypted (lock symbol). This applies in particular when filling in personal data that are worth to be protected in web forms.

3.10. Passwords

You have to comply with the password policy of the ZID, which is available in German at https://zid.univie.ac.at/passwort/#c11720.

3.11. Using social media

When using social media, you have to comply with the applicable confidentiality obligations and the Social Media Guidelines of the University of Vienna, available on the intranet of the University of Vienna under https://intra.univie.ac.at/fileadmin/user_upload/public/pdf/Folder_social_media_EN.pdf.

4. Special data protection methods

4.1. Right of access by the data subject and right to obtain information/right to erasure

According to article 15 of the GDPR, data subjects (e.g. students, interested parties and website users) have the right to obtain information from the University of Vienna as to

- the type of personal data that the University of Vienna stores,
- the recipients or categories of recipients to whom the personal data are transferred,
- the purpose of storage,
- the envisaged period for which the personal data will be stored, and
- the source of the personal data, if applicable.

Please immediately and directly forward any requests for information directed at the University of Vienna or the responsible unit in accordance with article 15 of the GDPR to the DPO (further information under https://dsba.univie.ac.at/). S/he is responsible for answering any such requests. The employee who received the request has to inform the head of his/her organisational unit. The same applies to requests for the erasure of personal data pursuant to article 17 of the GDPR.

4.2. Notification and communication of a personal data breach pursuant to articles 33 and 34 of the GDPR

Every employee is obliged to immediately notify the DPO in any case of conflicts or risk situations regarding data protection and if you fear that personal data might have been lost, stolen or accessed by unauthorised third parties.

4.3. Entry in the record of processing activities for new processing activities; data protection impact assessment by the data protection officer

Every employee is obliged to inform the data protection officer of any new processing activities or any changes to existing processing activities performed on personal data. The DPO decides whether it is necessary to carry out a data protection impact assessment. S/he will inform the relevant employee and discuss any further actions with him/her.