FAQs and Instructions on Data Protection at TU Wien

Version: 23/4/2019

The list is constantly being added to (also as far as templates and forms for information, required consent, etc.) and updated as well. New questions are highlighted in yellow.

>FAQs and Instructions<

Contents

The principles of data protection

In principle, in each individual case the following question should be clarified on whether the General Data Protection Regulation (GDPR[1]/DSG[2]) is applicable:

Is there fully or partially automated or non-automated processing of personal data that is stored in a file system?

"Personal data" are items of information about data subjects whose identity has been determined or can be determined. In this case it is irrelevant whether private, professional, commercial information, attributes, skills or physiological feature are concerned. Personal data are therefore things like, for instance, family name, date of birth, address, gender, income, financial assets, lifestyle, IQ, sales turnover, number of employees, profits, information on creditworthiness as well as also pictures, voice, finger prints or genetic data. Thus, all data that make it possible to identify a person.

☐ No: GDPR/DSG is not applicable; no further review is necessary.

☐ Yes: GDPR/DSG is applicable; a review of whether it is allowed is necessary.

The processing of personal data is basically prohibited. It is only allowed in those cases which are specifically cited in the law. According to art 6 (1) GDPR, this is allowed and thus legal if:

1. there is consent (art 6, par 1a), or
2. for the purpose of contract fulfilment or for fulfilment of pre-contractual measures (art 6, par 1b), or
3. there is a legal obligation (art 6, par 1c) or
4. the data are being processed for the purpose of protecting vital interests (art. 6, par 1d) or
5. it is a question of protecting public interests or exercising public authority (art. 6, par 1e) or
6. it occurs to defend the legitimate interests of the controller (art. 6, par 1f).

= PERMISSION CRITERIA

Regardless of the fact that data processing is only allowed if either consent (point 1) or a statutory permission criterion (points 2 through 6) applies, the data protection principles of GDPR must be complied with:

1. Legality: A legal basis for the processing must exist, in other words one of the permission criteria must be met;
2. Good faith: The processing must be fair and decent (imprecise legal concept);

---

[1] General Data Protection Regulation

[2] Datenschutzgesetz (Data Protection Act)

3. Transparency: The data processing must be intelligible for the data subject (cf. information obligations, data protection information);
4. Earmarking principle: The data processing may only occur for previously established, unambiguous and legitimate purposes;
5. Data austerity: The data processing must be restricted to the necessary earmarked minimum;
6. Objective correctness: The data must be objectively correct and up to date;
7. Restricted storage: The data must be erased as soon as possible, as soon as earmarked necessity of storage lapses;
8. Integrity and confidentiality: Inadmissibility of unauthorised or illegal processing and protection against loss and damage.

If any of the permission criteria is met and if the controller responsible for processing can show that the data protection principles were complied with, then the data may in principle be processed for each indicated purpose.

Check the personal data you are processing, update and erase it if the purpose of processing has lapsed: Attention: Observe erasure deadlines.[3]

[3] A list is being prepared

>FAQs and Instructions<

I. Generalities

1. May I continue to send external and internal persons who have ordered my newsletter or whom I have in my contact network my mailings?

Yes, only in the case of new external persons must there be consent in advance - it may be sent to internal persons (legal coverage by means of an employment contract or a justified interest of the employer).
Should there already be consents from external persons, then it must be ensured that the latter correspond to the requirements of GDPR. In this regard, the following must be ensured:
- unambiguous consent (consequently: silence or lack of action is not consent)
- notification must be given about which data are being processed and for what purpose (this must occur before consent)
- consent must occur by means of an unambiguous confirming act, therefore preferably in writing (a box to click on would also be allowed).

The consent may be withdrawn at any time. Information about the existence of this option of revocation of consent, and how this can be done, must be included in every mailing and newsletter.

TU.it offers different mailing lists where addresses outside TU Wien may also be integrated and existing lists be loaded into. There are many different configuration options for unsubscribing the mailing list; the option of unsubscribing by yourself is provided for. Information on this can be found here: https://www.it.tuwien.ac.at/uptodate/list/

You can get consent forms from your data protection coordinator (as soon as there is an internal area on the TU Wien website, all documents will also be available there).
https://www.tuwien.at/fileadmin/Assets/dienstleister/Datenschutz_und_Dokumentenmanagement/Datenschutz/Datenschutz-Organisation_der_TU_Wien.pdf

Besides consent, the processing of personal data may also be required to fulfil a task provided for by the 2002 University Act (UG). The tasks of the university are listed in § 3 UG. If the mailing of the newsletter falls under one of the points mentioned there, then mailing is possible even without explicit consent.

2. How long may I store my data?

Basically, personal data may only be processed (stored) as long as their purpose is still current. If that no longer obtains, then the data must be erased.
Please note that TU Wien is subject, in regard to erasure and retention deadlines, to many different statutory regulations and obligations. In case of uncertainty or any question of whether you may erase something or not, please consult the Department for Data Protection and Document Management and the TU Wien archives.

3. What do I have to watch out for in email correspondence? Are there any changes here?

Send emails if possible bcc (except where the recipients should know about each other) in order not to forward an unnecessary number of email addresses. Send them both internally as well as externally only to such recipients that require the personal data.

Emails and attachments with personal data should be avoided. In this matter, one should successively switch to links that can only be seen by the data subjects (password!). The corresponding passwords may not be sent by email.

In TU-OwnCloud you can enable folders for each employee. In TU-proCloud inclusion of external project partners is also possible.

4. What is data confidentiality?

Members of TU Wien are obliged to maintain data confidentiality.

Data confidentiality according to § 6 DSG (DPA)

(1) The controller, the processor and their employees, this includes workers (employees) and persons in a worker-like (employee-like) capacity, must maintain the confidentiality of personal data from data processing entrusted to them or made accessible to them solely on the basis of their professional employment, without prejudice to other statutory confidentiality obligations unless there is some other legally admissible reason for transmittal of the personal data entrusted or otherwise made accessible (data confidentiality).

At TU Wien the obligation to maintain data confidentiality occurs electronically.

5. How must customer data or data of external persons be treated (CRM)?

If data are processed for the purpose of contract fulfilment, then processing is legitimate. After successful execution of the contract, the data are to be erased while complying with statutory erasure deadlines. In cases of uncertainty about erasure deadlines, please contact the Department for Data Protection and Document Management or the TU Wien archives.

6. What do I have to do if I am processing personal data for the first time (i.e. storing, forwarding, using)?

I have to check whether I am entitled to process the personal data:

a. Is there any legal basis? (employment contract, other contractual relationship: e.g. supplier, caterer, sponsor, partner, legal obligation), or
b. Does TU Wien have any „legal obligation“ for this particular processing (e.g. is the processing associated with the fulfilment of a university task according to § 3 UG)? or
c. Is the processing for fulfilment of a task in the public interest?
d. Is there a justified interest in the processing which takes precedence over the data subject’s data protection interests?
e. Do I have consent from the data subject to process the data?

If I am entitled to process the data, I have to I comply with the information obligation and point out data subject rights („data protection declaration“).

7. May personal information be given over the phone?

If the identity of the interlocutor is not established, a call-back or a written enquiry should be agreed. In case of doubt, the identity of the caller must always be clarified.

8. I operate a social media account for my institute or my department. Am I allowed to do that?

The European Court of Justice has decided that the operator of a Facebook fan site is co-responsible for processing of personal data.[4] What does that mean for the site operator? What personal data are processed here?

From the ruling:[5]

„Administrators of fan pages […] can obtain anonymised statistical data on visitors to the fan pages via a function called “Facebook Insight”, which Facebook makes available to them free of charge under non-negotiable conditions of use. The data is collected by means of evidence files, so-called cookies, each containing a unique user code, which are active for two years and are stored by Facebook on the hard disk of the computer or another device of visitors to the fan page. The user code, which can matched with the connection data of users registered on Facebook, is collected and processed when the fan pages are opened […] In the opinion of the Court, the circumstance that an operator of a fan page uses a platform set up by Facebook to avail himself of the concomitant services does not release the latter from observing his obligations in the matter of protection of personal data.“

This does not mean that the operation of Facebook sites is illegal but that the operators of Facebook sites (and consequently also for other social media sites) are jointly responsible with Facebook for seeing to it that data protection is complied with as well as for data protection breaches by Facebook. The liability extends to the extent that Facebook’s cooperation in data processing can be assumed. That is, it is only a matter of processing of the data that was picked up via the Facebook site or a social plugin.[6]
Does that now mean that you must erase your pages? Not necessarily. But you should ask the question if it is really necessary to operate a Facebook site or other social media sites. The recommendation is to check the following:

- How great is the return?

---

[4] Cf.:https://derstandard.at/2000080989027/EuGH-Facebook-Fanpages-mitverantwortlich-fuer-Datenschutzverstoesse (last retrieved on 20/06/2018)

[5] Press release on the ruling: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180081de.pdf (lass retrieved on 18/06/2018)

[6] You can find detailed information here: https://allfacebook.de/policy/eugh-urteil (last retrieved on 18/06/2018)

- How large is the number of actual interactions (commentaries and news on contributions)?
- How many „likes“ does a contribution get on average?
- What is the site used for?
- What added value does the site provide for my institute, my project or my area of research?
- Are there other options for reaching similarly widespread coverage?
- How much time does maintenance of the fan page require?

If you come to the conclusion that operating the fan page generates actual added value, then it is in any case necessary to inform the users what data are being saved. You can find an example of the necessary information here: https://www.facebook.com/notes/kanzlei-keeseaufs/datenschutzhinweise-für-die-fanpage/1076429195844483/

II. Events

1. How do I handle my lists of participants (at events, conferences, etc.), contact lists, customer data, email distribution lists, newsletter subscriber lists?

With events of TU Wien relating to students, alumni or in general an area of research of TU Wien, we assume that this is covered by § 3 of the 2002 University Act (UG) (Tasks of a university). This provides a legal basis for the processing of data for the purpose of conducting the event.

If the data processing relates to sections which are not part of the statutorily regulated tasks of a university, then it must be checked whether there is another legal basis for processing, such as for instance a contractual basis or a consent. If there is no such basis, then consent must be obtained. In that case, the procedure is as follows:

Go through existing lists to see if they are up-to-date and correct and are still being used. If yes, then check if there is any valid consent. If not, erase them electronically (local erasure, empty recycling basket) or destroy the hardcopy (shredding). If the contact is still needed and there is no consent available, then this must be obtained.

You can obtain consent forms from your data protection coordinator (as soon as there is an internal area on the website, all documents will also be available there):
https://www.tuwien.at/fileadmin/Assets/dienstleister/Datenschutz_und_Dokumentenmanagement/Datenschutz/Datenschutz-Organisation_der_TU_Wien.pdf

2. How do I deal with new contacts from events, conferences, trade fairs, etc. that I would like to keep or save?

Here again, II.1 (page 9) applies. Data subjects must be informed about the data processing (data protection declaration), where required consent declarations must be signed.[7]

For sending emails to several persons TU.it offers a mailing list service (cf. https://list.tuwien.ac.at/sympa/). Existing lists can be incorporated. There are several different configuration options for unsubscribing from the mailing list. The option of unsubscribing by yourself is provided for.

You can get a consent form for photos, for newsletter mailings as well as for data protection information for conferences from your particular data protection coordinator (as soon as there is an internal area on the website, all documents are also available there):
https://www.tuwien.at/fileadmin/Assets/dienstleister/Datenschutz_und_Dokumentenmanagement/Datenschutz/Datenschutz-Organisation_der_TU_Wien.pdf

3. How do I handle business cards that I receive?

Handing out a business card can be understood as implicit consent for data processing of personal data. No consent to be signed by the data subject is required; I may keep the hard copy (business card) and store the contact.

4. I would like to hold an event and keep the list of participants. May I do this?

Here again II.1. (page 9) applies. On the registration form, information must be provided on this. Where applicable, consent must be obtained that the participants are in agreement with onward transmittal and storage of the contact data.

You can obtain a consent form for photos, for newsletter mailing as well as data protection information for conferences from your particular data protection coordinator (as soon as there is an internal area on the website, all documents are also available there) :
https://www.tuwien.at/fileadmin/Assets/dienstleister/Datenschutz_und_Dokumentenmanagement/Datenschutz/Datenschutz-Organisation_der_TU_Wien.pdf

5. I would like to have pictures taken at my event. May I do that?

For that, consent by the participants is required. If there is no such consent, photos are not allowed. At academic celebrations photos are basically allowed, however, if needed, a photo-free area should be provided. Moreover, information should be given by means of Department of Buildings and Engineering (TU GUT) signposting that photographs are being taken at the event.

---

[7] The consent must make it clear what is being consented to (which data, for whom, for what purpose, as well as the revocation option).

You can obtain a consent form for photos, for newsletter mailing as well as data protection information for conferences from your particular data protection coordinator (as soon as there is an internal area on the website, all documents are made available there):
https://www.tuwien.at/fileadmin/Assets/dienstleister/Datenschutz_und_Dokumentenmanagement/Datenschutz/Datenschutz-Organisation_der_TU_Wien.pdf

6. May I film students or lecturers?

As stated before, only with the consent of the data subjects.

III. Studies, teaching and research

1. May I as a lecturer keep attendance and participant lists?

Yes, this is legally covered by the 2002 University Act (justified interest of TU Wien).

2. How are interim grades dealt with? May I post grades or interim grades on the wall of the institute?

Since the matriculation number as well as the first name and last name constitute personal data, publication of any grades whatsoever is not allowed at the institute. This must be done via TUWEL.

If you would like to announce only the final marks in a course to the students, then use directly the TISS function „Notify students about grading.“ In order to announce individual test results or partial results to students on a person-by-person basis, it is best to use TUWEL.

Link to the video tutorial »Displaying grading in TUWEL«:

https://tuwel.tuwien.ac.at/mod/url/view.php?id=502363

3. May participant lists for excursions be passed on to eternal parties?

If for an excursion the participants must be made known to the external party (for instance for security reasons), then this forwarding is allowed. However, only the absolutely necessary data may be passed on. Usually, that will be the name of the participant. Consent is not required in this case, but in the course of registering for the excursion, the students must be informed about this.

4. May I transfer personal data to the email address at hansiwürstel@gmx.at?

If the identity of the sender is not clarified, no personal data may be sent to the address. Since it cannot reasonably be expected, particularly in teaching, to check each identity, we recommend that it be clarified at the beginning of every course that all email communication in the course should be carried out via the students' generic TU Wien email addresses. For this reason, it is to be stressed to the students that forwarding from the TU Wien email address to another email address should be deactivated. Should the students feel that this is unreasonable, then in any case a first-name.last.name@g... address must be used.

5. I would like to make my lectures available on YouTube. May I do this? Or, may I continue to avail myself of the services of Google?

YouTube is part of the Google corporate concern. YouTube is headquartered in the US and operates computer centres all over the world. In order to achieve the highest possible level of security – or so Google argues – the data are stored in different places. Since neither Taiwan nor Singapore are listed by the EU Commission as safe third countries and it cannot be excluded that data are processed there, an agreement must be signed with Google for data transfer on the basis of standard contractual clauses. Otherwise, no personal data should be processed via Google. Even if you pseudonymise personal data you enter into GoogleSheets, to take an example, personal data are still transferred to Google with your IP address and processed there.

In regard to streaming of lectures, we recommend the use of LectureTube. That application, provided by the Teaching Support Centre, makes it possible to record courses at minimum expenditure, in order to make them available to students as a multimedia resource in TUWEL. More information on this can be found here: https://teachingsupport.tuwien.ac.at/lecturetube/

As an alternative to Google Cloud, TU Wien's OwnCloud, belonging to TU Wien, can be used.

To create online-surveys, we recommend limesurvey (https://www.limesurvey.org/de/).

IV. Personnel

1. What happens to my work mobile, PC or laptop? Do I have to take precautions here?

Keep your equipment locked and secured with a password or a code. Do not pass on any passwords, change your password regularly and use safe passwords. More precise information on this may be found at: https://www.zid.tuwien.ac.at/tu_passwort/

Hard disks of mobile devices like laptops and tablets on which personal data are stored must be encrypted. Since a large number of different devices are in use at TU Wien – and they to some extent have not been issued by TU.it and therefore cannot be serviced by it either – we ask that you, if you cannot undertake encryption yourself, contact the IT administrator in your institute or department.

All of the newly issued mobile devices from TU.it will as of 1 June 2018 only be supplied with encrypted hard disks. If you still have a device issued by TU.it, where no hard disk encryption has been activated, you can contact the helpdesk about this.

Current smartphone operating systems generally run on encrypted file systems. Please check whether this applies to your smartphone and, if necessary, have it encrypted. To do this, go into the menu heading "Security" under "Configurations" where the opportunity should be given of encrypting your device (it generally takes an hour).

The access of apps (WhatsApp, Skype, Messenger etc.) to personal data, which you have stored on your device, must be prevented (by configuration setting or erasure of the app in question).

When using TU-OwnCloud, it must be ensured that it is not synchronised on your work mobile.

In case the work mobile goes missing, there is a possibility of resetting the device to its factory settings via WebMail and in that way prevent access to your emails. Instructions on how to do this can be found here: https://www.zid.tuwien.ac.at/uptudate/anleitungen/lostphone_datadelete/

2. May employee cards with a photo be used?

Yes, in this case the interest of TU Wien in the identifiability of the data subject takes precedence over the confidentiality interest of the employees.

3. May employee photos from TISS appear on the TU Wien homepage?

Yes, since each employee can upload the photo themselves to TISS and therefore can decide themselves whether a photo appears there or not. TU Wien employees should be aware that the TU Wien address book is publicly accessible.

4. May I forward salary and sick leave data of an employee to a sponsor?

Yes, if this is covered by the employment contract (an addendum to the employment contract is required). If there is no passage in the employment contract, then you must obtain the consent of the researchers to forward their salary and sickness absence data.

5. How are absences in the team calendar to be treated?

For example: The employees enter their absences in a team calendar to which all employees have access. In case of illness this is noted in the team calendar. In that case, a standard neutral expression chosen for all reasons for absences (for instance: „absent"). This is because exchanging special personal data (= "sick") is not required for purposes of employment.

6. How can protection against unauthorised inspection of data be guaranteed?

Personnel data, regardless of whether in electronic or hardcopy form, must be protected against being made known to unauthorised persons (e.g. no open documents on the desk). Hardcopy records must be kept in a locked cabinet and the office must be locked upon leaving. If you need lockable cabinets then please contact TU GUT.

Sending data:
If personal data are sent by employees then the data must be transported in such a way that they cannot be inspected (e.g. documents in sealed envelopes, encrypted and password-protected data media). Within TU Wien sending by email is allowed.

Documents with personal data sent to recipients outside of TU Wien must be sent secured, for instance encrypted or password-protected. Unencrypted USB sticks must be completely avoided for processing, storing or transmitting personal data.

In the TU-OwnCloud, directories for each employee may be set up. In the TU-proCloud the integration of external project partners is also possible.

7. How can I be sure that the camera and access system and biometric readers installed at TU Wien meet the requirements of GDPR?

In cases of doubt, please contact TU GUT (Security).

8. My server or website is not operated by TU.it. Who is responsible for the security of the data?

The Rectorate is only responsible for those sections which are actually under its control. Anyhow, this is correct for the services that are offered by TU Wien. Please check whether the operation of services by your own section continues to be economical and appropriate or whether a switch to the consolidated services of TU.it would be a practical alternative. Please also note in addition that services operated by yourselves, which process personal data, must be listed in the processing list of TU Wien. Please pass all information on this to your respective data protection coordinator who will then make an entry.

V. Annex

Shortlist[8]

„Important Measures for Data Protection and Security“(Part 1)

All of the following measures relate to hardcopy documents or electronic files or rather data media (e.g. CDs, USB sticks) with personal data on them[9] (hereafter referred to as “relevant documents” or “relevant data” or “relevant data media“).

1. „Clean desk“: Relevant documents and data media may not „lie around“ openly in the office, laboratory, etc., but must be kept inaccessible for third parties (e.g. locked cabinet). Measure: Relevant documents and data media must always be kept locked up!

2. Safe disposal: If relevant documents have to be disposed of, this may not be done like „normal“ waste paper: Disposal only with a shredder or a „blue bag“ (available from TU GUT. Up until being handed over to GUT, the „blue bag“ must also be kept locked up)! Measure: Shred relevant documents or discard them safely by “blue bag!”

3. Password for IT devices: IT devices on which there is relevant data (PC, notebook, smartphone, etc.) must be made safe with as good a password as possible against access by third parties.[10] The password may not be accessible for third parties (that means no sticker on the monitor screen or on the desk blotter!). Measure: Provide IT devices with a safe password which must not be accessible to third parties!

4. Safe management of passwords: In order to support a maximally uncomplicated management of passwords, there are safe and easily operated password managers (e.g. as apps for the smartphone but even as software for the PC or the notebook).[11] Alternatively, password records can also be stored safely (locked up). Measure: Password records must either be kept locked up or passwords must be managed with a safe password manager (software or app)!

5. Disposal of data media (including out of IT devices): Data media (CDs, USB sticks) or hard disks out of IT devices (PC, notebook, server, etc.) at the end of their useful life and on which relevant data are kept, must be discarded safely. For that purpose, the service „TU Disk Shredder“ in TU IT Services (ex ZID) must be used.[12] Measure: Disposal of data media (including out of IT devices at the end of their useful life) only by way of the TU Wien IT service „TU Disk Shredder!“

---

[8] 22/03/2018, Markus Haslinger.

[9] Examples of personal data: Last names, matriculation numbers or email addresses of students, lists of participants, test results, evaluation sheets, etc.

[10] For more information, for instance, cf.: https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html (22.3.2018).

[11] Cf. for instance https://futurezone.at/apps/die-besten-passwort-manager-im-ueberblick/249.643.370 (22/03/2018).

[12] Cf. https://www.zid.tuwien.ac.at/tudiskshredder/ (22.3.2018).