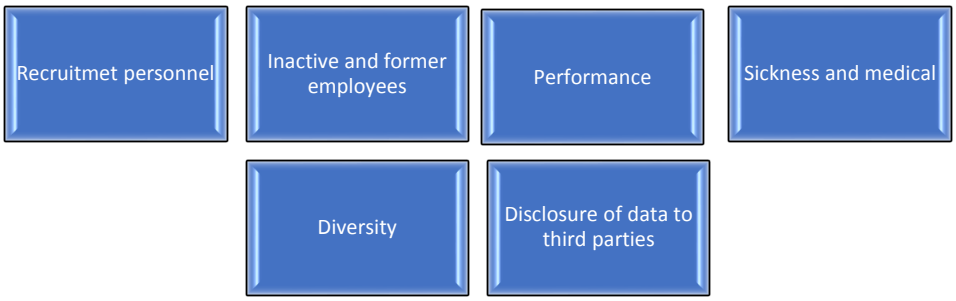
Thematic Privacy & Personal Data Protection Policy—Processing Personal Data

PERSONNEL

Readers' Guide

This Thematic Policy on Personnel is part of the Privacy & of Personal Data Protection Policy and describes the way in which Tilburg University implements the General Data Protection Regulation (GDPR) on the protection of Personal Data with regard to staff members (whether or not they are in salaried employment).

For the sake of readability, we have divided this Policy into the following sub-areas.



All information relating to European legislation (GDPR) and the Protection of Personal Data is included on the **Tilburg University website,**[1] including the Frequently Asked Questions. On this website you can also find practical details and examples.

Every School/Division within Tilburg University has appointed Data Representatives. They are the first point of contact for employees who have questions about the Protection of Personal Data.

This Policy includes references to other policy documents. These are marked as "**referrals**". The applicable guidelines are shown in blocks to make them easy to find:

Subject	Guideline.

Many definitions are included in this Policy (see **Appendix 1**). The terms that can be found in the definition list are capitalized.

When he is referred to in this Policy, it is understood to mean he/she or gender-neutral.

[1] https://www.tilburguniversity.edu/intranet/legal-affairs/privacy

Table of contents

1. General

An item of Personal Data is

any information that can identify a natural person or information that can be traced back to that person now or in the future.

This may be the name, administration number, or other data that uniquely identifies an individual. However, it may also be a combination of a number of data that in itself cannot be traced back to a person, but can be traced back in combination, or can be traced back to a person in the future by means of, for example, technical possibilities, the so-called Traceable Personal Data,. The combination of, e.g., place of residence, age, organizational unit can be traced back to a person. When it comes to data relating to an individual, it quickly becomes Traceable Personal Data.

With regard to personnel, this means applicants, salaried employees (in Dutch: *personeel in loondienst, PIL*), external employees (in Dutch: *personeel niet in loondienst, PNIL*) and former employees from whom we process Personal Data. Tilburg University attaches great importance to the careful processing of Personal Data in the context of its personnel, whereby we seek a good balance between privacy, security, and functionality as misuse of data can cause great damage to Tilburg University and its staff. In the context of processing personal data by HR, the term Data Subject is used in the GDPR, which mainly concerns applicants, salaried employees (PIL), external employees (PNIL), and former employees. In this Policy, we talk about this group as a whole as “Personnel.”

Processing is understood to mean the processing of Personal Data, whether or not automated, such as collecting, recording, organizing, structuring, storing, modifying, retrieving, consulting, using, disclosing (forwarding), distributing or making available, combining, shielding, or erasing data. It concerns paper files or archives, digital files, or Personal Data in an application/system (including mailboxes, laptops, or other data carriers). In other words, everything you do with Personal Data.

This Policy applies to all Processing of Personal Data that takes place in the context of Personnel Management under the responsibility of Tilburg University and applies to everyone working under the responsibility of Tilburg University.

Responsible	The **Process Owner of** the process in which the Personal Data are processed is **ultimately responsible** for the Protection of this Personal Data. The Process Owner must ensure that all employees carry out the Processing of Personal Data in accordance with this Policy.

2. General Guidelines

2.1. Processing Basis and Purpose for Processing

Any Processing of Personal Data must be lawful, i.e., there must be a legal Processing Basis and purpose for Processing. For Personnel, the possible Processing bases are included in **Appendix 2:**

Processing Basis	Processing of Personal Data is **only permitted** if one of the **Processing bases included in Appendix 2** is **complied** with. The basis of the Processing in question (depending on the process) must be stated in the Processing Register.

In addition, Processing must have a concrete purpose (purpose limitation). This concerns the following for personnel[2]:

Staff (PIL and PNIL)	1. The handling of personnel matters; 2. personnel and payroll administration; 3. managing the work of the Data Subject; 4. the implementation of employment conditions; 5. determining and arranging for the payment of salary entitlements, allowances, and other amounts and remunerations in kind to or for the benefit of the Data Subject; 6. calculating, recording, and paying taxes and contributions for the benefit of the Data Subject; 7. arranging for entitlements to unemployment benefits in connection with the termination of an employment contract; 8. the occupational health care of the Data Subject; 9. staff welfare services; 10. the election of the members of a participation body regulated by law; 11. internal control and corporate security; 12. drawing up a list of dates of anniversaries of Data Subjects and other festivities and events; 13. granting resignation; 14. the administration of the Employee Association and of the association of former employees; 15. liaising with the Data Subject's employer; 16. dealing with disputes and carrying out audits; 17. recovering claims, including placing such claims in the hands of Third Parties; 18. the Data Subject's training;

[2] Based on exemption degree Personal Data Protection Act.

	19. the transfer of the Data Subject to or his temporary employment with another part of the group, as referred to in Article 2:24b of the Dutch Civil Code, to which the responsible party is bound; 20. the implementation or application of legal regulations; 21. archive management; 22. carrying out scientific, statistical, or historical research.
Former employees	1. Keeping in touch with Data Subjects; 2. dealing with disputes and carrying out audits; 3. the implementation or application of legal regulations.
Applicants	1. Assessing the Data Subject's suitability for a position that is or may become vacant; 2. handling the expenses incurred by the applicant; 3. internal control and corporate security; 4. the implementation or application of legal provisions.

Purpose limitation	• Processing of Personal Data of personnel is permitted if the Processing is based on one of the purposes mentioned above. • If a Processing takes place based on a purpose that does not appear in this list, it must be aligned with the Data Protection Officer in advance, after which it will be added to the above list if justified.

Once purpose limitation and lawfulness have been established, additional requirements apply. These are included in the remainder of this Policy.

2.2. Personnel Rights

The staff member has a number of rights with regard to his Personal Data. For more information, please refer to the **Privacy & Personal Data Protection Policy.**

Right	Staff members have the right to
Right to be informed	be informed regarding which Personal Data are processed.
Right of access	have access at all times to the Personal Data collected in respect of their person. **Please note**: there may be exceptions to this rule based on the Dutch Medical Treatment Contracts Act.
Right to rectification	demand at all times to have incorrect Personal Data be rectified.
Right to restriction	restrict the Processing of Personal Data, for example, pending the outcome of an objection. Restriction means that Personal Data will be marked and may not be Processed or shared during this period.
Right of erasure	make an application to erase his Personal Data.

Right to object	Indicate that he does not want his data to be processed (anymore).

If a staff member wishes to invoke one of these rights, he must follow the procedure set out on the website. This does not apply to the right to rectification/correction for which the staff member has the possibility to modify these data himself in My Employee Portal. The staff member enters the changes he can make himself in My Employee Portal (such as contact details).

Personnel rights	Employees have the rights of Data Subjects as mentioned in the GDPR. For more details, please refer to the **Privacy & Personal Data Protection Policy—Chapter 10.**
Responsible	HR Director In order to exercise his rights, the staff member follows the procedure (with the exception of rectification requests, which he himself can carry out in My Employee Portal). The Data Protection Officer (DPO) shall coordinate the other requests.
Restriction of personnel rights	The rights of a staff member do not extend to working documents, internal memorandums, and notes of supervisor(s) and/or HR employees insofar as these contain the personal thoughts of a supervisor or HR employee and are exclusively intended for internal consultation and deliberation.

3. Recruitment Personnel

For recruiting & selection of new personnel, personal data of applicants are processed. This chapter deals with aspects of the selection procedure that need to be specified in the context of the GDPR.

3.1. Vacancy

The selection procedure starts with drafting a vacancy text. The following requirements apply to the text.

Vacancy text	• The vacancy text includes a statement that Tilburg University will handle the Personal Data provided by the applicant with care, including a link to the Privacy Statement. • If an assessment and/or psychological or medical examination may be part of the selection procedure, this will be stated in the vacancy text.

3.2. Headhunters, Recruiters, and Recruitment Agencies

Tilburg University makes limited use of external parties in its search for suitable candidates. For positions in the higher segment, an executive search often takes place via a specialized agency. Tilburg University has no permanent contract partners for this.
If an external party is called in for the recruitment, this external party is the independent Controller. The agreement with the third party contains agreements on the responsibilities of both parties and the security of Personal Data.

Involving external parties in the selection procedure	Tilburg University only engages recruiters, headhunters, and recruitment agencies that comply with the GDPR. These external parties are independent Controllers. The protection of Personal Data is guaranteed by means of a written agreement.

3.3. Selection Procedure

During the selection procedure, the applicant will provide Tilburg University with the Personal Data necessary for the following purposes:

- assessing the candidate's suitability;
  This includes the CV, the cover letter and, depending on assessment criteria, any additional documents such as certificates, references, publication lists, lists of grades, and/or chapters of a thesis.
- the communication with the applicant;
  This concerns the salutation, full name, e-mail address, telephone number, desired language of communication (Dutch/English) and, in the case of international recruitment, the place of residence of the Data Subject.

The applicant provides this information via the online recruitment application SAP SuccesFactors Recruiting.

A selection committee (in Dutch: *benoemingsadviescommissie: BAC*) is set up for each vacancy.

Access to application data	Application data is only accessible to the: • BAC members; Externals may be part of the BAC; • HRSC vacancy Expert Team (for administrative processing)
Disclosure of application data	The disclosure of the application data to the BAC members is done via the digital application. For reasons of security, the information is not provided by e-mail (not encrypted either) or (internal) mail.
Storage period	The candidate's Personal Data will be Anonymized 28 days after completion of the selection procedure in accordance with the Recruitment Code of the Dutch Association for Personnel Management and Organization Development (*Nederlandse Vereniging voor Personeelsmanagement & Organisatieontwikkeling*; hereinafter: NVP). With the applicant's consent, application data may be stored for a maximum of one extra year (at the applicant's or university's request). This period of one year can be extended with additional consent, giving the applicant the opportunity to update his data.

3.3.1. Recruitment outside the online recruitment application

For specific groups of employees (student assistants, invigilators, sports instructors, examiners, proofreaders, academic staff recruited via the jobmarket or network, and people from the target group register), recruitment takes place outside the online application.

Recruitment outside recruitment application	Recruitment takes place under the responsibility of the individual organizational unit or Department in accordance with the NVP recruitment code and in line with the provisions of this guideline. HR supports the organizational unit or Department in this.

3.4. Health Situation and Application

An applicant's health data fall under the category of Special Personal Data. In principle, the Processing of these data is prohibited.

Health data relevant to a position	Candidates are not required to give any information about their health that is not directly relevant to the performance of the duties for which they are applying at the time of the interview. However, applicants are required to report any health complaints that they know, or are supposed to understand, will make them unsuitable for the job. Tilburg University may, therefore, only ask the applicant about the applicant's health situation if and to the extent that this is necessary to assess his capability for work (and the activities involved) in the specific position

3.5. Screening Methods for Applicants

Screening methods are used by Tilburg University to gather background information from an applicant in order to assess his suitability for the job and/or his integrity. Tilburg University only uses screening if there is a legitimate reason (legitimate interest) and the screening is necessary.

3.5.1. Request for references

Requests for references	are only permitted with the specific consent of the applicant and if this is necessary for the performance of the job. • The applicant approaches the reference himself or Tilburg University approaches the reference (after consent). • Reference provides Tilburg University with the applicant's data ○ in writing: included in the online recruitment application. • References will be provided as feedback to the applicant.
Access to references	References are only available for applicants, BAC members, and the HRSC vacancies expert team. References will be anonymized in accordance with the NVP Recruitment Code 28 days after the completion of the selection procedure.

Information on the role of Tilburg University as reference is included in **Section 9.3** of this Policy.

3.5.2. Assessment/personality tests

Within Tilburg University, limited use is made of assessments and/or personality tests in the selection phase. These resources will only be used if they are necessary to assess the applicant's suitability for the vacant post. This mainly concerns senior management positions in the higher segment. If an assessment/personality test is used as a selection tool, an external party will be called in to do this.

Collaboration with external parties	Collaboration is only permitted with parties that comply with the GDPR. The external party can be seen as a Processor. A Processing Agreement will be concluded.
Disclosure of Personal Data	Only necessary Personal Data will be disclosed. Tilburg University will only disclose contact details of the applicant that are required by the external party to carry out the assessment or personality test and, if applicable, their CV and cover letter.
Results of the assessment or test	The results of the assessment or test will only be provided to Tilburg University if and when the external party has obtained the applicant's consent. The results are only available to the HR advisor and manager involved in the vacant position,
Storage period	The results will be erased after a maximum of 28 days following the completion of the selection procedure. The results of the assessment or test of the selected candidate may be included in the personnel file, with the exception of medical and health data. The results will only be included in the personnel file if there is a basis for doing so (in the context of the execution of the employment contract,

	including the assessment of the employee's performance, or a legitimate interest of the employer).

3.5.3. Certificate of Conduct

A Certificate of Conduct (In Dutch: *Verklaring omtrent gedrag*; hereinafter VOG) is a certificate which shows that a staff member's conduct in the past does not constitute an obstacle to the performance of a specific job. In the event of a legal obligation to submit a VOG, Tilburg University will request it. There are currently no positions at Tilburg University that are subject to a legal obligation to submit a VOG.

Certificate of Conduct	Currently, Tilburg University does not request a VOG. If, in the future, there are positions at Tilburg University for which a VOG is required by law, or if Tilburg University develops additional policy regarding a VOG, this will be requested and stored in the personnel file.
Storage period	Not applicable at present (in case of possible future situations, in connection with legal obligation or additional Tilburg University policy: 2 years after ending employment)

3.5.4. Social media and applicants

The NVP states that applicants should be aware of the impact of offering Personal Data on/via the Internet. Applicants are responsible for this themselves. In addition, Tilburg University is aware that the information available on social media regarding applicants is not necessarily reliable.

Consulting an applicant's profile on social media is regarded as processing Personal Data.

Consulting social media	Tilburg University will only consult social media channels if this is necessary to assess the suitability of the candidate, taking into account proportionality and subsidiarity. In that context, consulting a LinkedIn profile is justified.
Informing the applicant	If consulting social media, Tilburg University will be transparent about the information obtained and discuss it with the applicant.[3]

3.6. Application and Affirmative Action Policy

Based on the legislation on equal treatment, Tilburg University can apply an affirmative action policy in the selection procedure for women, people of non-Dutch origin, and people with a disability or chronic illness. At Tilburg University, an affirmative action policy is pursued within the framework of the Philip Eijlander Diversity Program and the implementation of the Participation Act.

Transparency of target group policy	If an affirmative action policy is pursued or if setting an age limit is necessary for the position, this shall be explicitly stated in the vacancy text including the reason for this.

[3] For this, Tilburg University is in line with the NVP Recruitment Code and the European privacy regulators' opinion on "Data processing at work."

Processing Personal Data of target groups	Tilburg University has the right to process any Personal Data necessary to verify that the applicant falls within the specific target group. For the implementation of the Participation Act, Tilburg University processes the BSN in order to check with the Employee Insurance Agency (UWV) whether the applicant belongs to the target group. The BSN is deleted immediately after checking.

3.7. Determination of the Terms and Conditions of Employment

If the applicant is selected for the vacant position, he may be asked to submit an old salary slip in order to establish a real salary. The applicant is not obliged to provide the salary slip.

Salary Strip	The applicant may be asked to provide a salary slip, but is not required to do so.
Storage period	The salary slip is only consulted for determining the amount of the salary and is not kept by Tilburg University.

4. Entry into Employment

The selection phase is followed by the staff member's entry into employment. This chapter describes which Personal Data is processed in the context of the entry into employment.

4.1. Personnel Intake

A staff member's entry into employment starts with the completion of a staff intake form. The staff member must complete the form. Tilburg University has a legal obligation for the processing of the requested Personal Data, or processing is necessary for the execution of the (employment) agreement.

Tilburg University has a legal identification requirement for every new staff member. Tilburg University must check the identity document for authenticity and validity and keep a copy. In this context, a new member of staff will be asked to provide a full copy of his identity document to Tilburg University.

In order to comply with the legal obligation to check that the bank account is (partly) in the name of the staff member, the staff member will also be requested to provide a copy of his bankcard or other evidence of his bank account.

Processing Basis	Legal obligation (Dutch Wages and Salaries Tax Act) Execution of the employment contract
Content of the processing	Legal obligation: Name, address, residence, BSN, date and place of birth, nationality, request for income tax and national insurance contributions to be applied or not. Execution of the employment contract: contact details, marital status, desired language of communication and way of addressing, bank account number, part-days on which the staff member will work, date of possible PhD defense (requirement for certain positions), data required for the execution of the employment conditions (years-of-service bonus: data on previous employment contracts with educational and government institutions). On the form, the staff member has the choice of including information about his partner (as emergency contact) and whether he wants to become a member of the Employee Association.
Erasure of form	The form will be erased as soon as the data have been entered into the personnel and salary system.
Copy of passport	There is a legal obligation to keep a copy of the identity document of every employee (Compulsory Identification Act). This must be valid at the time of the intake. If the identity document expires during the employment, it does not need to be replaced. Based on the law, Tilburg University stores this until five years after the end date of the contract.

Copy bankcard	In order to carry out the statutory duty of supervision (Dutch Labour Market Fraud (Bogus Schemes) Act), the salaried employee will be asked to provide a copy of his bankcard (or other documentary evidence). Tilburg University keeps this for the duration of his employment.

4.2. International Staff Member

Additional Personal Data will have to be processed when an international staff member starts employment. For example, under the law, Tilburg University is responsible for applying for a possible residence and work permit with the Immigration and Naturalisation Service (in Dutch: *Immigratie- en Naturalisatiedienst*: IND). Tilburg University applies for the permits for the staff member and for his accompanying (possibly minor) family or relatives. Tilburg University uses the VisaCare system for the provision of the necessary Personal Data to the IND. A Processing Agreement has been concluded for the use of the VisaCare system.

During the period of employment, Tilburg University is obliged to inform the IND about changes in the staff member's Personal Data that may affect his right of residence (e.g., when the employee no longer meets the salary requirement, change of position, termination of employment, or when the employee returns to his country of origin).

Processing basis	Legal obligation (Aliens Act + Foreign Nationals (Employment) Act)
Content of the processing	In order to apply for a residence and/or work permit for the staff member (and his family, if any), VisaCare will provide the IND with the Personal Data that are necessary for this purpose on the grounds of the law. Tilburg University has a legal obligation to inform the IND about changes that may affect the right of residence.
VisaCare	The data exchange with the IND takes place via VisaCare. VisaCare is a Processor. A Processing Agreement has been concluded for the use of VisaCare.
Storage period	The documents used for the application of the residence and/or work permit are erased after obtaining the permit. The license(s) themselves are stored in the personnel file. There is a storage period of five years starting after the end date of the contract.

Tilburg University offers international personnel support to ensure that the relocation from abroad runs smoothly. A number of Schools within Tilburg University make use of P&Dcare's relocation services in this context. Tilburg University provides P&Dcare with individual employees' Personal Data necessary for the performance of these services.

Processing basis	Execution of (employment) contract
Content of the processing	Name and contact details of the staff member, in so far as these are necessary to ensure that the relocation from abroad runs smoothly

P&Dcare	P&Dcare carries out the support on behalf of Tilburg University. P&Dcare is a Processor. A Processing Agreement has been concluded with P&Dcare.
Storage period	Tilburg University stores the documents relating to the relocation from abroad in connection with the fiscal legislation for the reimbursement of the relocation costs up to seven years after the end date of the (employment) contract.

The 30% tax facility makes it possible to provide 30% of the salary tax-free to an international staff member. The application of the scheme requires a decision by the Tax and Customs Administration. SOFIE (in Dutch only) intervenes as a third party between Tilburg University and the Tax and Customs Administration.

Tilburg University submits the Personal Data necessary to determine whether there is a right to the 30% tax facility to SOFIE. SOFIE checks whether the conditions are met and submits the required Personal Data to the Tax and Customs Administration. The Tax and Customs Administration issues the decision to SOFIE, and SOFIE sends this back to the university. SOFIE does not pass on the Personal Data received to other parties.

On request, SOFIE also assesses the determination of the country of residence and the tax and social security position of an individual employee. The name, date of birth, nationality, and country from which the employee was recruited by the university will be provided to SOFIE.

Processing basis	Execution of the (employment) contract Legitimate interest
Content of the processing	Tilburg University provides SOFIE with the documents necessary to determine whether a member of staff meets the conditions for the 30% tax facility and/or the tax and social security position.
SOFIE	SOFIE is a partnership of Dutch universities and not a separate legal entity (and, therefore, has no legal personality). In the participant agreement that the universities have concluded with SOFIE, there is a passage about the protection of Personal Data and compliance with the GDPR.

If a staff member is covered by social insurance abroad, Tilburg University is legally obliged to pay social security contributions in that country. Tilburg University provides Personal Data regarding the staff member concerned to the competent authority in the country where the person in question is insured. This only concerns Personal Data that are necessary for the payment of the contributions. The competent authorities are independently responsible for the processing of the Personal Data.

Processing basis	Legal obligation
Content of the processing	Tilburg University provides the necessary Personal Data to the social security authority of the country where the member of staff is covered by social insurance.
Processing Agreement?	Since the provision is based on a legal obligation, no Processing Agreement is concluded.

4.3. Internal disclosure of Personal Data for Making Facilities and Provisions Available

For the allocation of Tilburg University facilities and provisions, the required Personal Data of employees are disclosed internally to the responsible unit. This involves the disclosure of Personal Data necessary to arrange access to the intranet, a Tilburg University e-mail address, wireless access, the employee printers, Tilburg University SharePoint, the Tilburg University Card, and the library's lending system. Access to these facilities and provisions is necessary for the proper performance of the (employment) contract by the staff member.

4.3.1. Language Center

Under the terms of the employment contract, employees who join Tilburg University for a minimum period of 12 months are obliged to take part in the English Language Assessment of Tilburg University's Language Center. In connection with this requirement, HR sends the names of new employees and associated professional e-mail addresses to the Language Center on a monthly basis. The Language Center uses this personal information to send an invitation for the Assessment. There is a legitimate interest in this internal provision. The level test stems from the university-wide language policy adopted by the Executive Board, University Labor Representation Board, and University Council.

Processing basis for disclosure	Justifiable interest
Content of the processing	Name, professional e-mail address, and to which Language Assessment the staff member should be invited.
Feedback from Language Center to HR	The Language Center provides the results of the Assessment to the employee, the supervisor, and HR.

4.3.2. UTQ coordinators

Tilburg University's scientific personnel may be obliged to obtain a UTQ certificate (the University Teaching Qualification, a certificate of didactic competence for lecturers in university education) based on the employment contract. In this context, the names, including the professional e-mail addresses, of new staff members who are subject to this obligation and have not yet obtained this certificate are sent to Tilburg University's UTQ coordinators. The UTQ coordinators use these personal details to send invitations for the UTQ training courses. There is a legitimate interest for this internal disclosure. Dutch universities, in the context of the VSNU, have drawn up this UTQ certificate as a quality mark for qualified lecturers in academic education. The UTQ coordinators need the Personal Data to invite them to the sessions leading to the UTQ certificate.

Processing basis for disclosure	Justifiable interest
Content of the processing	Name and professional e-mail address

Feedback from UTQ to HR	After obtaining the certificate, the UTQ coordinator provides this to the staff member and HR. HR records the date of obtaining the certificate and stores it in the personnel file.

4.4. External Disclosures in Connection with Entry into Employment

4.4.1. ABP

Employees who work for Tilburg University build up a pension with the General Pension Fund for Public Employees (in Dutch: *Stichting Pensioenfonds: ABP)*. The ABP is the statutory pension fund for government and educational institutions. Tilburg University is obliged to report new employees to the ABP. In addition, Tilburg University is required, on a monthly basis, to provide the ABP with Personal Data that are necessary for the ABP to administer its pension plans. Since there is a legal basis for providing Personal Data, no Processing Agreement has been concluded with the ABP.

4.4.2. Employee Association

The Tilburg University Employee Association is a separate foundation and organizes activities for staff and former staff of Tilburg University. If the staff member indicates on the intake form that he wishes to become a member of the Employee Association, his name and contact details are given to the Employee Association. With this information, the Employee Association is able to invite members to activities.

Processing basis for disclosure	Justifiable interest
Content of the processing	Name, date of birth, and contact details
Deregistration	A member of the Employee Association can deregister at any time. The Employee Association will be informed accordingly.
Retirement	If a member leaves employment, membership of the Employee Association will end. The Employee Association is informed if a member leaves the university's employment. See in this respect **Section 9.1.1** of this Policy.

4.5. Ancillary Activities

Based on the CLA (Article 1.14) and the Sectoral Scheme Covering Ancillary Activities, salaried employees (and PNIL full professors) are obliged to request consent to perform ancillary activities via My Employee Portal. Tilburg University registers all ancillary activities. The registered English-language ancillary activities for academic staff are also publicly published on the Scientific Profile page. The above is part of Tilburg University's agreement with the person in question.

Processing basis for disclosure	Execution of the (employment) contract Justifiable interest

Content of the processing	In accordance with the Sectoral Scheme Covering Ancillary Activities, the following information must be provided when the member of staff reports ancillary activities: a. nature of the ancillary activities to be performed; b. the body for which ancillary activities are carried out; c. the start and end date of the ancillary activities and the time involved (during/outside working hours + number of hours); d. whether (private) income is received; e. permission to publish. As far as academic staff is concerned, the ancillary activities for which Tilburg University has given permission are published on its publicly accessible Scientific Profile page. These are the data referred to under a. and b. above.
Access	Ancillary activities that are not open to the public are accessible to • staff members, • supervisor, • HRSC employee and HR advisor, • internal Audit & Compliance, • internal financial control,
Storage period	Until two years after the end of the agreement

5. Performance, Appraisal, and Development

*This chapter deals with Personal Data processed by Tilburg University in the context of the performance, appraisal, and development of a staff member. It should be noted in advance that Tilburg University qualifies data relating to the performance of a staff member as Sensitive Personal Data (**Section 4.4.4 Privacy & Personal Data Protection Policy).** Extra care must be taken when processing these data. In addition, performance data should only be visible to staff members for whom it is necessary in the course of performing their duties.*

5.1. Performance and Assessment - R&D cycle

In the annual Result & Development (R&D) interview between the supervisor and the staff member, the results and development achieved by the staff member are evaluated and assessed. In addition, result and development agreements are made for the future period. The data is recorded on the R&D form.

Processing basis	Execution of the (employment) contract
Contents	On the R&D form, the results achieved and developments expected for the future are recorded. Agreements on subjects in the checklist of the R&D report are also included in the form. Only relevant information is recorded on this form. The R&D form may contain Sensitive and Special Personal Data (e.g. about the staff member's health).
Access	The R&D forms are included in the personnel file and are only accessible to the • staff member, • supervisor, • HRSC employee and HR advisors.
Storage period	R&D forms are kept for up to 4 years after adoption of the report. They will then be erased from the personnel file. The date of the interviews will remain on file even after the expiry of the four-year period.

The storage period of four years after adoption of the R&D report also applies to Personal Data collected in the context of the R&D cycle (feedback that the supervisor or staff member himself has requested from colleagues as input for the R&D discussion).

If the staff member submits a request for a review of his appraisal and then appeals, the procedural documents form part of the R&D file. In this case, the storage period of four years will commence at the moment of the last transaction in the review and/or appeal process.

5.2. Job Profile Classification

Tilburg University staff members are assigned to a specific position according to the system of University Job Classification System (UFO). If the staff member wonders whether the level of the

position or the job profile is (still) appropriate for the tasks assigned to him, the supervisor may, on behalf of the Director, request advice from the HR department regarding the position.

If the advice given regarding the position of the staff member does not produce the desired result, he shall have the option of applying for a review. This may be followed by an objection. During the objection procedure, a national committee will handle the case. The national committee receives the staff member's Personal Data that it needs to render advice on the UFO classification. This concerns, in any case, the HR specialist's advice regarding the positon, the intended classification decision, the request for reconsideration, and Tilburg University's reasons for the objections and opinion.

Processing basis	Execution of the (employment) contract. It is necessary for the execution of the contract to know in what position the work carried out by the staff member is classified.
Contents	As a result of this job profile evaluation, the following will be included in the personnel file: • HR specialist's advice regarding the position; • proposed classification decision; • request for a review; • possible objection and advice from the national committee and the decision on the objection.
Access	Accessible to: • staff member, • supervisor, • HRSC employee and HR advisor, • HR Specialist regarding job classification, • national committee.
Storage period	A maximum of two years after termination of employment.
External hiring	Pursuant to the administrative rules for UFO classification decisions, Tilburg University must involve a national committee in the event of a notice of objection. The national committee will take the GDPR into account when handling the objection and, after the decision on the objection, will not store the Personal Data for longer than necessary.

5.3. Education and Training

For the implementation of the agreement, it is necessary for Tilburg University to know what education (plus work experience) the staff member has at the time of joining the institution and what he completes during his employment with Tilburg University. Tilburg University also has a legitimate interest in processing this data, as it provides insight into the staff member's potential and is important for staff planning. In this context, the following Personal Data will be processed.

#	Type	Explanation	What Personal Data are processed?	Where?
1	Pre-recruitment education and training	This concerns the education and training that the staff member has already acquired at the time of commencement of employment with Tilburg University.	CV	PF
2	UTQ/Senior Qualification (SKO) for Scientific staff, English Language Assessment, other compulsory courses. For an explanation, see **Section 4.3.1** and **Section 4.3.2** of this Policy.	Obligation to participate/obtain a certificate for defined categories of staff under the terms of the employment contract	- Diplomas and/or certificates - Registration of participation	PF PF
3	Course or training followed internally (coordinated by HREC)	Training courses organized by HREC in the context of leadership skills, educational skills, etc.	Application form with contact details and information necessary to determine whether the training is suitable for the staff member (e.g., School).	HREC
4	External education/training: (partly) compensated by Tilburg University	Training that, in the opinion of the employer, is necessary or relevant to the staff member's present or future position (categories I + II of the Training Facilities Regulations).	- information about training - agreements on training - repayment obligation (if applicable)	PF PF PF
5	Development days	Under the CLA, staff members are entitled to two development days a year. These days can be used for activities that contribute to the personal development and/or sustainable employability of the staff member.	Method of expenditure	PF

In this table, PF stands for personnel file, HREC for HR Expertise Center.

Processing basis	Execution of the (labor) contract
Access	The documents contained in the personnel file are only accessible to the • staff member, • supervisor, • HRSC employee and HR advisor The application form for internal education and training courses is only available to the HREC policy officer.
Storage period	Type 1, 2, and 5 documents are kept for 2 years after dismissal. Type 3 documents are kept for 1 year after completion of the course. Type 4 documents: 3 years after completion of the training course and/or expiry of the agreed repayment period.
Hiring a Third Party for internal training	If an external party is used to provide the type 3 training or course, only the Personal Data needed to provide the training is disclosed to the Third Party. A Processing Agreement is concluded with the external party.
Evaluation internal training	The evaluation of an internal training course is carried out with a digital tool. Because it contains Personal Data, a Processing Agreement must be concluded for this purpose.

5.4. Career Counseling, Training Advice & Coaching

Career counseling includes the guidance, coaching, and advice of employees on career issues. Depending on the nature of the request for support, the advice will be given by an HR advisor, or external assistance will be engaged.

Training advice is the advice on the development of the future or current position. Depending on the question, the advice is given by the HR advisor or by the HR Expertise Center specialist.

Processing basis	Execution of the (labor) contract
Contents	Advice and possible reports of consultations. It is possible that (Sensitive and/or Special) Personal Data is processed in this procedure. This could include data on the performance of the staff member and health data (in terms of possibilities/restrictions).
Access	The training documents are included in the career file managed by the HR advisor or HR Expertise Center specialist. The documents are only accessible to the • staff member, • supervisor (only advice, no interview reports), • HR advisor or HREC specialist (depending on the course of action).
Storage period	A maximum of 2 years after termination of employment
External hiring	If a third party is engaged for (support regarding) the career, training advice and/or coaching, a Processing Agreement will be concluded

	with the external party. Only those Personal Data of the necessary for the execution of the assignment will be sent to the external party.

5.5. Development Processes, Redeployment, and Outflow

If the performance of the staff member is not satisfactory, Tilburg University shall endeavor to improve the performance of the staff member. As discussed above, this can be done by means of, among other things, education, courses, and/or training. Other possibilities are starting a development process to improve the performance, mediation, or a re-employment study. As this concerns the performance of staff, it is sensitive data.

Processing basis	Execution of the (employment) contract Statutory re-employment obligation
Contents	The following may be included in the Personnel File: • agreements and results of the development process; • agreements about and outcomes of the mediation; • letter with confirmation of the status of the re-employment candidate
Access	The documents are only accessible to the • staff member, • supervisor, • HRSC employee + HR advisor, • HR Expertise Center specialist
Storage period	Up to two years after expiry date of the contract
Hiring a mediator or other external counselor	If a third party is engaged, depending on the circumstances of the case, a Processing Agreement will be concluded or the responsibilities within the framework of the GDPR will be considered in the main agreement. The external party will only be provided with the Personal Data necessary for the execution of the assignment. This may include Special Personal Data.

Ending the employment is the ultimate remedy in case of performance problems or other unsolvable situations. During the dismissal process, it is possible that Personal Data (including salary data) of the employee is provided to a lawyer or legal advisor. This information is necessary for the execution (and finalization) of the contract. In certain cases, an application for dismissal will be submitted to the UWV. In this case, the UWV will only be provided with the Personal Data necessary for the assessment of the dismissal file.

6. Sickness, Absenteeism, and Medical Records

Information about a person's health is Special Personal Data. Processing these data is in principle prohibited, save for the exceptions mentioned in the law. In general, Tilburg University is permitted under the GDPR (Implementation Act) to process health data insofar as the processing is necessary for the reintegration or supervision of employees in connection with illness and incapacity for work. In addition, Tilburg University is entitled to process health data if this is necessary for the proper implementation of statutory regulations (such as the Dutch Eligibility for Permanent Incapacity Benefit Restrictions Act, in Dutch: Wet Verbetering Poortwachter), pension schemes, and the Collective Labour Agreement, to the extent that these provide for agreements that depend on the state of health of the Data Subject. This chapter elaborates in more detail regarding which Personal Data Tilburg University processes in the context of illness and reintegration. The Policy Rules on the Sick Employee of the Dutch Data Protection Authority (Dutch DPA) from 2016 (Dutch only), which are still in force according to the DPA, were used as a starting point.

6.1. Reporting Sick

The first phase of a staff member's incapacity for work starts with reporting sick. The staff member reports sick in My Employee Portal.

Processing basis	Execution of the employment contract Legal obligation (Eligibility for Permanent Incapacity Benefit (Restrictions) Act + 7:658a Dutch Civil Code) GDPR Implementation Act Article 30, paragraph 1
Contents reporting sick	In accordance with the DPA's Policy Rules, only the following information is requested/recorded in the event of reporting sick: • first sick day, • expected duration of the illness, • nursing address and telephone number if not the home address, • current business/work that needs to be delegated • whether there is any work that can still be done by the staff member, • adjustments needed to get (back) to work, • whether there is a catch-all situation, • whether the illness is related to an (occupational) accident Data that the staff member himself provides to Tilburg University about his illness are in principle not processed.
Access	The data concerning a sickness report are only accessible to the • staff member, • supervisor, • HRSC employee + HR advisor.
Storage period	Until two years after the end of the contract. If the sickness situation falls within the scope of the own-risk bearer status under the Dutch

	Sickness Benefits Act or Work and Income (Capacity for Work) Act (in Dutch: WIA), longer storage periods apply (see **Sections 6.3** and **6.4**).

In the event of reporting sick, Tilburg University may also ask the staff member whether he is covered by the catch-all provision of the Sickness Benefits Act. The basis for this is Article 29 of the Sickness Benefits Act, i.e., the no-risk policy. This applies only if the staff member has completed two months' service at the time of the illness. If the staff member is covered by the no-risk policy, the UWV will assume responsibility for the continued payment of wages during illness. See **Section 6.6** and **7.1**.

6.2. Reintegration in the Event of (Impending) Long-term Absenteeism during the Period of Continued Payment of Wages

During the first two years of a staff member's incapacity for work, Tilburg University has a legal obligation to continue to pay wages and to reintegrate. The basis for these two obligations is Section 7:629 of the Dutch Civil Code, the Eligibility for Permanent Incapacity Benefit (Restrictions) Act and Sickness and Disability Scheme for the Dutch Universities (In Dutch: *Ziekte- en Arbeidsongeschiktheidsregeling Nederlandse Universiteiten*: ZANU). In this chapter, the data processing that takes place in the context of these obligations is discussed.

6.2.1. Data exchange with the occupational health and safety service

Tilburg University has a legal obligation to get support from experts for the reintegration obligation and the sick leave counseling of its staff. In order to comply with this legal obligation, Tilburg University has entered into a contract with the Arbo Unie. The Arbo Unie takes care of the engagement of occupational health physicians at Tilburg University.

Processing basis	Legal obligation (implementation of the Working Conditions Act) Execution of employment contract GDPR Implementation Act Article 30
Content of the Tilburg University's provision to the occupational health and safety service	Tilburg University only provides the personal details of a sick member of staff to the Arbo Unie that are necessary for the implementation of the absenteeism counseling by occupational health physicians. These include: • name and contact details: to be able to make appointments with the employee; • employment data: to be able to determine the employee's limitations for performing the job; • Supervisor's contact details: the supervisor is the case manager; • information about the absence notification: first day of illness, absence history, and percentage of illness; • notifications of recovery.
Agreement with Arbo Unie	The Arbo Unie itself determines the purpose and means of the data processing. As a result, the Arbo Unie is the independent Controller under the GDPR. This means that no Processing Agreement has been concluded but that the main agreement contains agreements on security and responsibilities.

	The Privacy Regulations of the Abo Unie are an integral part of the main agreement. The Arbo Unie processes the Personal Data of Tilburg University staff members with whom they have a clinical relationship solely for the performance of its task as an occupational health and safety service provider.

The previous part discusses the disclosure of Personal Data from Tilburg University to the Arbo Unie. The disclosure of Personal Data from Arbo Unie to Tilburg University takes place in the context of the actual supervision of absenteeism by the occupational health physicians (see the next section). In addition, Tilburg University receives an annual report from the Arbo Unie. No Personal Data are included in this report. The report consists of quantitative absenteeism figures, causes of absenteeism, and the occupational health physicians' observations about Tilburg University (e.g., trends that the Arbo Unie sees in absenteeism). The above data cannot be traced back to individual members of staff and are thus Anonymized.

6.2.2. The absence management

If an employee is absent from work for a long period of time (or is likely to be absent from work), an appointment for supervision will be made with the occupational health physician of the Arbo Unie. The occupational health physician prepares a problem analysis and advice for the plan of action and provides it to Tilburg University. Based on the advice of the occupational health physician, Tilburg University draws up the plan of action together with the staff member.

During the period of incapacity for work, the staff member periodically visits the occupational health physician. The HRSC receives the conclusions of the occupational health physician about the possibilities of the staff member to resume work and the guidance agreements that have been made about this. A copy of the report is provided to the supervisor, HR advisor, and employee in question.

Processing basis	Legal obligation (implementation of Articles 7:629 + 7:658a of the Dutch Civil Code, Eligibility for Permanent Incapacity Benefit (Restrictions) Act, and Regulations governing the Procedure during the 1st and 2nd Year of Illness) Execution of the employment contract GDPR Implementation Act Article 30
Content of disclosure by the occupational health physician to Tilburg University	The occupational health physician is permitted to provide Tilburg University with the following Personal Data about the employee's health: • work for which the employee is no longer or still capable (functional limitations, residual possibilities, implications for the type of work that the employee can still do); • expected duration of the absence; • extent to which the employee is unfit for work; • any advice on adaptations, work facilities, or interventions the employer must provide for reintegration. These data are included in the problem analysis, the plan of action, and reports of the consultation hours with the occupational health physician.

	No other possible data regarding the employee's health are necessary for the employer for the continued payment of wages obligation and/or for the reintegration/absenteeism management. This information is subject to medical confidentiality and is not provided to Tilburg University by an occupational health physician. This includes information requested by the occupational health physician from (attending) doctors about therapies, diagnoses, etc. The occupational health physicians of the Arbo Unie only place personal medical data in their own system.
Reintegration file	The employer is obliged to keep track of sick leave and reintegration in the reintegration file. The reintegration file may contain the following information: • problem analysis + adjustments, • advice and reports from occupational health physicians, • action plan + adjustments, • advice and reports from occupational health physicians and other parties involved, such as case managers and reintegration companies, • actions taken for reintegration, • all other correspondence, e.g., with an occupational health physician. The reintegration file only contains health data that are necessary for the reintegration (such as the restrictions set by the occupational health physician).
Access	The reintegration file is accessible to the • employee, • supervisor, • HRSC + HR advisors
Storage period	Maximum storage period for the reintegration file is two years after leaving employment. This period is longer • if the staff member receives a WIA benefit after the period of continued payment of salary (see **Section 6.3**); The file will be kept for the duration of the WGA process (Return to Work (Partially Disabled Persons) Regulations) (maximum of ten years). • if the staff member falls under the own-risk bearer status of the Sickness Benefits Act (see **Section 6.4**), a storage period of five years applies. This period starts in the year following the closure of the reintegration file.

Information from attending (general)	The Staff member must always give consent for requesting medical data from his attending physician and/or specialist by means of a

physician or specialist to occupational health physician	written authorization. Tilburg University does not receive this medical information.

6.2.3. Socio-medical Team (SMT)

The aim of the SMT (Socio-medical Team) is to coordinate the absence management and reintegration of individual employees who are unable to work.

Discussion in SMT	• In the SMT, the occupational health physician, the Director of the School or Division for which the staff member works, the HR advisor and, if necessary, the supervisor, discuss the progress of the reintegration. • In accordance with the DPA's Policy Rules, the SMT only shares the degree of incapacity for work, the expected duration, functional limitations, and any labor-related adjustments. Medical data are explicitly not discussed.

6.2.4. Second opinion of occupational health physician

A staff member can request a second opinion from another occupational health physician (who does not work at the Arbo Unie) if he has doubts about the correctness of the advice given by the regular occupational health physician.

Disclosure of information to other occupational health physicians for a second opinion	The occupational health physician only provides all relevant and available information (as included in the Working Conditions Decree (in Dutch; *Arbobesluit*)) to the occupational health physician who carries out the second opinion with the explicit consent of the staff member.
Advice from other occupational health physicians to regular occupational health physicians	The advice of the occupational health physician who carries out the second opinion will only be sent to the regular occupational health physician after the explicit consent of the staff member.

6.3. Application and Guidance WIA (Work and Income (Capacity for Work) Act)

After two years of incapacity for work, a staff member may (possibly) qualify for a WIA benefit. The UWV assesses whether a staff member is eligible for a WIA benefit. Tilburg University prepares the WIA application together with the staff member. When the staff member has been unfit for work for 89 weeks, Tilburg University draws up a reintegration report with the staff member based on the reintegration file and sends it to the staff member (Article 25, paragraph 3 of the WIA).
The occupational health physician draws up the medical part and sends it directly to the staff member (not to Tilburg University). The staff member can use these documents to submit an application to the UWV for a WIA benefit. The staff member sends the reintegration report together with the reintegration file and the medical part to the UWV for the WIA application.

Processing basis	Legal obligation (Regulations governing the Procedure during the 1st and 2nd Year of Illness + WIA + ZANU) Execution of the employment contract GDPR Implementation Act, Article 30
Reintegration report	The reintegration report contains the documents referred to in Article 6, paragraph 1, of the Regulations governing the Procedure during the 1st and 2nd Year of Illness. It concerns the following staff member's Personal Data: • required administrative data of the staff member; • information concerning the position of the staff member; • information concerning the competences of the staff member; • first day of illness; • the occupational health physician's opinion and advice; • the action plan and adjustments agreed between the employer and the employee; • evaluation at the end of the first year of illness as well as the most recent evaluation of the progress and implementation of the agreements made in the action plan; • an up-to-date assessment of the quality of the working relationship by the employer and the occupational health physician; • a current assessment by the occupational health physician of the course of the unfitness for work, the functional limitations, and the possibilities of the staff member to perform work; • the staff member's opinion of the information and opinions recorded above.
Medical data	The occupational health physician draws up the medical part of the reintegration report and sends it to the employee. Tilburg University will not receive a copy.

After the employee has submitted the WIA application, the UWV carries out the WIA assessment. As part of the WIA assessment, the staff member will be assessed by the insurance company's medical advisor and the occupational health expert of the UWV. The UWV will then decide whether or not to award a WIA benefit. The WIA consists of a Fully Disabled Persons Income Scheme (in Dutch: IVA) benefit and a WGA benefit.

- The IVA benefit is for staff members who have little or no possibility of working with a small chance of recovery: the UWV provides for this group and pays the benefit and takes care of the reintegration. Tilburg University is not an own-risk bearer for the IVA.
- The WGA benefit is for employees who are for at least 35% incapacitated for work and who can work (now or probably in the future). Tilburg University is the own-risk bearer for the WGA and, therefore, has the legal obligation to pay this benefit and to promote the reintegration of the (former) staff member (Article 42, paragraph 1 of the WGA).

UWV decision	The UWV sends the WIA decision to the staff member and to Tilburg University. Tilburg University is an interested party as an own-risk bearer. The decision states whether the employee is eligible for a WIA

	and, if so, how much it is. Tilburg University will also receive information on how the UWV arrived at this opinion. No medical information on the staff member is provided.

Tilburg University currently supports (former) staff members with a WGA benefit itself. Agreements are made at an individual level about reintegration counseling. Within the framework of the reintegration, only the (health) data of the individual employee necessary for that purpose will be processed. The WGA file is kept in accordance with the DPA's Policy Rules for the duration of the WGA process (maximum of ten years).

6.4. Own-risk Bearer Sickness Benefits Act

Tilburg University has an own-risk bearer status for the Sickness Benefits Act. This means that Tilburg University is also responsible for, among other things, the reintegration of former staff members whose temporary contract has ended during the two-year pay obligation. For this category, the reintegration process will continue as if the staff member were still employed. This means that the Personal Data collected during the reintegration after the end of the employment contract are the same as in the case of a regularly ill staff member.
There are only minor differences. For example, there is a separate occupational health physician for staff members who fall under the own-risk bearer status of the Sickness Benefits Act. The previously attending occupational health physician will pass on the reintegration file (including the medical data) to the new occupational health physician. The previously attending occupational health physician will inform the (former) staff member of this prior to the transfer.

Processing basis	Legal obligation (Article 3 Decree governing the Tasks, Administrative Regulations and Costs of Self-Insurance under the Sickness Benefits Act (in Dutch: *Regeling werkzaamheden, administratieve voorschriften en kosten eigenrisicodragen* (ZW)). GDPR Implementation Act, Article 30
Contents	Tilburg University will only process the former staff member's Personal Data covered by the Sickness Benefits Act (own-risk bearer status), as referred to in Article 3, paragraph 1, under b, of the Decree governing the Tasks, Administrative Regulations and Costs of Self-Insurance under the Sickness Benefits Act (ZW). These include, but are not limited to, the following • BSN and name; • period of unfitness and an overview of previous periods of unfitness; • amount of the gross ZW daily allowance and the reasons for this; • start, duration, and end of entitlement to ZW benefit and the reasons for this. The actual reintegration guidance is provided by HR advisors, supported by an occupational health physician.

Storage period	The statutory storage period for Tilburg University is five years. The five-year period begins in the year following the year in which the last transaction in the file was carried out. The occupational health physician, who holds the medical file, has a storage period of ten years.

6.5. Reintegration Company

During the obligation to continue to pay wages (the first two years of incapacity for work), reintegration assistance is provided by Tilburg University (supervisor, with support from HR) and the occupational health physician. Only in exceptional cases will a reintegration company be used to support the reintegration during the continued payment of wages obligation period.

In the short term, however, Tilburg University does intend to hire a permanent reintegration company to supervise all WGA employees and staff members who fall under the Sickness Benefits Act (*ERD voor de Ziektewet*).

Processing basis	Implementation of the contract (employment contract + collective agreement) Legal obligation (Section 7:658a of the Dutch Civil Code) GDPR Implementation Act, Article 30 Justifiable interest
Disclosure data to reintegration company	If Tilburg University engages a reintegration company, there is a legal obligation (Section 7:658a of the Dutch Civil Code) to provide the company with the Personal Data necessary to carry out the tasks assigned by the employer. This concerns contact details (such as BSN) and health information available to Tilburg University (e.g., functional limitations) if these are necessary for the proper guidance of the (former) staff member.
Hiring an external reintegration company	In the case of selection, the requirement is that this party acts in accordance with the GDPR. The way in which the responsibilities are defined on both sides depends on the assignment in an individual case. In most cases, both parties will be independent Controllers and the agreements will be included in the main agreement.
Information to staff member	The (former) member of staff is informed in advance regarding which Personal Data will be provided to the reintegration office.

6.6. Data Exchange with the UWV in the Context of Illness

Tilburg University and the occupational health physicians are legally obliged to provide the UWV with the incapacitated staff member's Personal Data required for the performance of the tasks of the UWV.

Processing basis	Legal basis (Article 54 of the Work and Income (Implementation Organization Structure) Act (in Dutch: *Wet SUWI*)

Disclosure of Personal Data to the UWV	Tilburg University only discloses Personal Data to the UWV if there is a legal basis for doing so, e.g., • in case of 42 weeks of illness; • sickness due to pregnancy (entitlement to WAZO benefit (Work and Care Act)); • employee is covered by a no-risk policy (entitlement to Sickness Benefits Act benefit is paid by the UWV).
Processing Agreement	Tilburg University provides only those Personal Data necessary for the UWV. Which Personal Data are necessary depends on the basis and circumstances of the case.
Disclosure of Personal Data from UWV to Tilburg University	The UWV is allowed to provide information to an employer when this is necessary for the performance of his duties (Article 73(3) of the SUWI).
Processing Agreement	Since disclosure is based on a legal obligation, there is **no** need to enter into a Processing Agreement.

If the reintegration reaches a deadlock, Tilburg University can ask the UWV to assess the situation by means of an expert opinion. Tilburg University provides the UWV with the necessary Personal Data to be able to make an assessment (e.g., problem analysis). Within the framework of the expert opinion, the UWV also requests Personal Data from the occupational health physician (about the medical aspect) and the staff member himself. Tilburg University will not have access to this medical information.

Tilburg University can also ask the UWV for a reassessment of the incapacity for work of a (former) employee who receives a WIA benefit. This reassessment will be requested if the health of the (former) staff member has changed during the WIA period. The application will include the name, BSN, and telephone number of the staff member, as well as an explanation of why the reassessment is being requested. The medical data is provided by the occupational health physician to the UWV; Tilburg University will not have access to this medical information.

6.7. Objection and Appeals Procedure: Physician and Legal representative

Tilburg University may call in the assistance of a physician and legal representative in the event of objection and appeal procedures at the UWV or other conflicts during the period of incapacity for work. Unlike Tilburg University, the physician and legal representative is entitled to see the medical file of the staff member. This allows the physician and legal representative to assess the (medical) grounds taken into account in the UWV's decision.

Processing basis	Justifiable interest GDPR Implementation Act, Article 30
Content disclosure	Tilburg University only discloses the details of the individual sick staff member necessary for the execution of the deployment as a physician and legal representative.

Cooperation with physician and legal representative	The physician and legal representative is the independent Controller. When selecting the physician and legal representative, it is a requirement that the physician and legal representative complies with the GDPR, and that agreements on the processing of Personal Data are included in the main contract.
Disclosure of Personal Data by physician and legal representative to Tilburg University	The physician and legal representative has a duty of confidentiality towards the employer with regard to staff members' medical data. Consequently, the physician and legal representative does not disclose the staff member's medical details to Tilburg University.

6.8. Illness Due to an Accident and the Possibility of Recourse

If a staff member becomes incapacitated for work as a result of an accident or mistreatment for which a third party is (possibly) liable, Tilburg University can and will try to recover the continued wage payment and reintegration costs from this third party. Tilburg University is supported by the Claims Settlement Office (in Dutch: *Bureau schadeafwikkeling* (BSA)) in the implementation of this right of recourse.

Processing basis	Justifiable interest
Disclosure of Personal Data	Tilburg University only processes and discloses the data necessary for the enforcement of the right of recourse pursuant to Article 6:107a of the Civil Code. These include the cause of the illness and salary details.
Execution of right of recourse by the BSA	The Personal Data that BSA receives from Tilburg University may only be used for the enforcement of the right of recourse. A Processing Agreement is concluded with the BSA.

6.9. Prevention

6.9.1. Open consultation hour of the occupational health physician (working conditions consultation hour)

The occupational health physician at Tilburg University has an open consultation hour, during which the staff member can discuss health issues in relation to his work on his own initiative.

Open consultation hour occupational health physician	• Tilburg University is never informed of who visited the consultation hour and/or the reason for the visit. • Tilburg University only receives quantitative (non-traceable) data (e.g., number of staff members who used the consultation hours).

6.9.2. Health check

Tilburg University offers its employees a health check without any obligation, which is carried out by an external party. If a staff member wants to participate, he fills in a form on the intranet and receives a personal login code by e-mail for completing online questionnaires about his own employability and health. After filling out the form, the participant will receive a report with a personal result.

The external party needs the requested Personal Data to contact the staff member (name, e-mail address), to make a correct health analysis (position, date of birth, and gender) and for an annual anonymized report to Tilburg University. The external party receives these Personal Data from the staff member himself. Tilburg University does not disclose Personal Data for this.

The staff member can make an appointment for the health check at the Tilburg University Sports Center. This check is carried out by a trained employee of the Sports Center. The outcome of the health check is recorded by the Sports Center employee in the external party's system. The participant in the health check can see the outcome of the check in the system of this party.

Content disclosure	Tilburg University does not disclose Personal Data to the Third Party. If the staff member wishes to participate, he sends the necessary Personal Data to the external party himself.
Access to data	Only the staff member and the external party have access to the results of the Health Check. The Sports Center employee has access to the outcome of the health check for the coaching.
Share information with Tilburg University.	The results of the health check are in no way made available to Tilburg University. An exception to this is the employee of the Sports Center, for whom the outcome of the health check can be seen as part of the coaching. Once a year, a feedback report is provided at university level by the external party, in which Tilburg University is informed of the number of participants of both parts of the health check (plus Department and organizational unit if this does not ensure the traceability of the participants). Only the participant receives the report and can view the results of the health check.
Collaboration with Third Party for Health Check	When selecting the party, it is a requirement that the Third Party complies with the GDPR. A Processing Agreement is signed.

7. Diversity

7.1. Job Quota

Tilburg University has a legal obligation to create jobs for people with disabilities (job quota). The persons for whom these jobs are intended are listed in the UWV's target group register.

If a suitable candidate is found to fill a job at Tilburg University, an employment relationship is entered into (directly employed by the university, employed by KCS, or seconded from a third party).

Processing basis	Legal basis Special Personal Data (taxable status of candidates, etc.) are processed by Tilburg University under Article 30, paragraph1 (a) and (b) of the GDPR Implementation Act. The data are necessary to assess whether there is a good match between the candidate and the vacancy.
Disclosure by Tilburg Municipality to Tilburg University	Tilburg University receives Personal Data from possibly suitable candidates from Tilburg Municipality: • Curriculum Vitae • Background information on work capacity, functional possibilities/ limitations, and any necessary adaptations/facilities in the workplace. If an employment relationship is entered into, this background information will be kept by the Participation Act policy officer. The background information is stored in order to be able to keep track of the candidate's possibilities and limitations, so that the work (also in the future) can be geared to this. It is also registered whether the candidate is covered by the no-risk policy.
Data exchange with the UWV	• Check inclusion in target group register In order to be able to comply with the job quota, Tilburg University needs to know whether a candidate actually belongs to the target group according to the UWV register. Therefore, Tilburg University is allowed to check with the UWV (by means of the disclosure of the BSN) whether the candidate is indeed included in the target group register (Article 38d, paragraph 7 of the Sheltered Employment Act; in Dutch: WSW). • Illness In the event of incapacity for work, a staff member with an occupational disability is eligible for a sickness benefit under the Sickness Benefits Act paid by the UWV (because of a no-risk policy). Tilburg University provides the UWV with the Personal Data required by law to receive sickness benefit (Article 29b of the Sickness Benefits Act).
Disclosures regarding subsidies	Tilburg University can apply for a subsidy that compensates for the reduced productivity of an employee with a work disability. For the application, it is necessary for Tilburg University to disclose Personal

	Data about the staff member with a work disability to the subsidy provider (the Municipality, the UWV, or the Tax and Customs Administration). This means that there is a legitimate interest in disclosing the disabled person's Personal Data required for the subsidy application to the subsidy provider.
Access to background information	Only the Participation Act policy officer has access to the background information.
Storage period	• CVs and background information on candidates who are not placed for a job opening are deleted after the selection procedure has been completed. • If a candidate is not placed but does have a profile suitable for future job openings, the candidate is explicitly asked for consent to keep his CV and background information for a period of one year. At the end of the one-year period, the candidate will be asked for consent again. The Participation Act policy officer manages the (deadlines of) files of potential candidates and is the only one who has access to the content of the files. • If a candidate is placed, the background data will be immediately erased at the end of the placement period.

In addition to the above, Tilburg University does not disclose any Personal Data to third parties. The VSNU and Social Fund for the Knowledge Sector (SoFoKles) only receive quantitative information on the number of placements of people with disabilities and the FTEs.

7.2. Cultural and Ethnic Minorities

The majority of Tilburg University's staff are Dutch and of native parentage. Tilburg University does not currently have a general policy to hire more staff with a migration background. There are, however, a number of initiatives aimed at increasing cultural diversity.

7.2.1. Positions for refugees

Tilburg University offers refugees the opportunity to make a start on the Dutch labor market by offering internships. In this context, the diversity policy officer receives Personal Data of possibly suitable refugees for an internship at Tilburg University from Tilburg Municipality.

Processing basis	Justifiable interest (Pre-contractual) execution of the (internship) agreement
Disclosure by Tilburg Municipality	The diversity policy officer receives Personal Data from possibly suitable refugees with the aim of offering the refugee an (internship) agreement: • Curriculum Vitae • Name, address, and domicile. The policy officer provides this information internally by encrypted e-mail to Directors and/or HR advisors who may have a position for the refugee.

Access to information	The diversity policy officer and Directors and/or HR advisors who may have a vacant position.
Storage period	Personal Data will be erased if matching is unsuccessful. If an internship agreement is agreed upon, the provisions of Chapter 10 of this Policy apply.

7.2.2. Scholars at Risk

Scholars at Risk is an organization that gives endangered scientists the opportunity to continue their work in a safe environment. As a socially responsible organization, Tilburg University offers this safe environment. In this context, Tilburg University receives Personal Data from Scholars at Risk from scientists who have been or are being prosecuted in their home countries. Tilburg University processes these Personal Data (CV, name, and address data) for the purpose of offering an agreement to the persecuted scientist. The diversity policy officer receives the Personal Data from Scholars at Risk and only discloses them internally to the supervisor(s) and/or HR advisor(s) who may have a position for the persecuted scientist. If the matching is unsuccessful, the Personal Data will be erased.

Processing basis	Justifiable interest (pre-contractual) execution of the contract
Disclosure by Scholars at Risk	Diversity policy officer receives Personal Data from the organization Scholars at Risk • Curriculum Vitae • Name, address, and domicile. The policy officer provides this information internally by encrypted e-mail to Directors and/or HR advisors who may have a position for the scientist in question.
Access to information	Diversity policy officer and Directors and/or HR advisors who may have a vacant position.
Storage period	Personal Data will be erased immediately if matching is unsuccessful. If an agreement is concluded with the scientist, the further processing of the Personal Data will be subject to the provisions of this Policy.

7.3. Gender

The Strategy states that the aim is to achieve gender equality. In order to promote this gender equality, the university takes various initiatives. In the implementation of these initiatives, the Personal Data of Tilburg University employees are processed.

7.3.1. Philip Eijlander Diversity Program (PEDP)

The PEDP increases the number of women in higher academic positions by creating additional assistant, associate, and full professor positions. The aim of these additional positions is to approach the targets for female full professors and female associate professors. The PEDP should be seen as an affirmative action policy. See Section 3.6. of this Policy for more information on the affirmative action policy.

Under the PEDP, a mentoring program is offered to the selected women. This mentoring program is led by an external trainer. In this context, the necessary Personal Data of the women are sent to the external trainer. It only concerns contact details.

Processing basis	(pre-contractual) executions of the contract
Content disclosure	The external trainer receives Personal Data from participants in the mentoring program necessary for this purpose (name, position, School, professional e-mail address). The external trainer is required to comply with the GDPR. The arrangements are laid down in the cooperation agreement.

7.3.2. Events in the context of Gender

Tilburg University organizes the Gender Unlimited Festival every year. If a staff member registers for participation in the program via the Tilburg University website, the gender policy officer will receive the Personal Data entered by the staff member. These Personal Data are limited and necessary for the organization of and invitation to the event.

There is also a Tilburg University Network for Women. If a member of staff applies to participate in this network, the gender policy officer will receive the necessary Personal Data. These Personal Data are limited and necessary for inviting staff members to the network meetings. If a staff member no longer wishes to be part of the network, he informs the gender policy officer and the Personal Data is erased.

Processing basis	Consent
Content disclosure	Gender Unlimited festival: name, professional e-mail, staff/student /other Tilburg University Network for Women: name and professional e-mail (mandatory), School, Department, and position (optional).

7.3.3. Monitoring

The gender policy officer monitors the progress of the initiatives in the area of gender and the agreements made with the Executive Board and/or Labor Representation Board. In this context, the gender policy officer has access to gender distribution in job applications, the male-female ratio in the Selection Committees and male-female ratio in positions (per School). The use of regulations aimed at gender (research support for maternity leave, parental leave, etc.) will also be monitored.

The Executive Board and the Labor Representation Board have agreed that a study into salary inequality will be carried out. In this context, the gender policy officer has insight into the Personal Data, which are necessary for the execution of and reporting on this study. In the report on the study, the Personal Data will not be traceable to individuals and will be made anonymous.

Processing basis	Justifiable interest
Content of the processing	Name, position, salary scale and step, scope of work, type of contract, date of commencement of employment, and date out of service
Access	Gender policy officer

8. Other Processing During the Employment Relationship

8.1. Leave

Tilburg University requires additional Personal Data for granting and carrying out certain special forms of leave. The staff member is asked to provide this information with the application of leave. The Processing Basis for these data is the execution of the employment contract (or terms and conditions of employment).

Processing basis	Execution of the (employment) contract
Content of the processing	Maternity leave: • Pregnancy leave: declaration by a doctor or obstetrician with a probable date of delivery, date of commencement of pregnancy leave and whether there are multiple births • Maternity leave: date of birth of child Adoption or foster leave: • Period of adoption or foster leave • Name and starting date of care for an adopted or foster child • Declaration by the staff member that he will be taking care of the child on a permanent basis Parental leave: • Period of parental leave • Name and date of birth of child • Declaration by the staff member that he will be responsibility for the care/upbringing of the child in the long term.
Access	• Staff member • Supervisor • HRSC employee and HR advisor
Data exchange with UWV	During maternity leave and adoption or foster leave, staff members are entitled to a WAZO benefit from the UWV. In order to exercise this right, Tilburg University provides the UWV with the staff member's Personal Data required for this purpose. The decision will be included in the personnel file.
Storage period	Until two years after the end of the agreement. The declaration of pregnancy is erased one year after the end date of the maternity allowance.

8.2. Internal Disclosures during the Employment Relationship

This section focuses on the internal disclosures that take place during the employment relationship but have not been mentioned previously in this Policy.

8.2.1. Disclosure of Personal Data for internal monitoring purposes

Tilburg University personnel in charge of internal monitoring (such as employees of the Internal Audit and Internal Financial Control units) necessarily have access to Personal Data of Tilburg University personnel for the performance of their duties. This includes, among other things, salary details. They may use Personal Data only to the extent that this is necessary for the performance of their monitoring duties.

Processing basis	Justifiable interest
Internal monitoring	Personnel in charge of internal monitoring whom, as a result, have access to the Personal Data of Tilburg University personnel will only use this data to the extent necessary for the performance of the monitoring task.

8.2.2. Disclosure of Personal Data to secretaries' offices

It is common for Directors, Deans, and supervisors to ask their secretaries' offices to request personnel data from the HRSC for their Department or organizational unit. In the event of such a request from a secretaries' office, the HRSC will only forward the information to the secretaries' office in the case of general employee data (such as names of staff members, unit/Department, professional e-mail addresses, professional telephone number, UFO position, etc.). If a secretaries' office requests Special Personal Data (information on sickness, performance, or salary), the HRSC will not provide this information to the secretaries' office, but to the person making the request (hierarchical superior, Director, Dean).

Processing basis	Execution of the (employment) contract Justifiable interest
Content disclosure	Requests from secretaries' offices to the HRSC to provide general employee information (such as name, unit/department, professional e-mail addresses, professional telephone number, UFO position, etc.) are sent directly to the secretaries' office. Requests from secretaries' offices for special data (such as salary, absenteeism, and performance data) are not provided to the secretaries' office by the HRSC. This information is only provided to the actual person requesting the information (supervisor, Director or Dean).

8.3. External Disclosures during the Employment Relationship

This section discusses the external provision of Personal Data during the employment of staff members that have not been discussed previously in this policy.

8.3.1. Information about the employment relationship of a staff member

It is possible for a third party to request information from Tilburg University about a staff member.

Request for information on staff member by third parties	Information from a member of staff to a Third Party (such as reference check by a potential new employer) shall only be disclosed with the written consent of the member of staff concerned.

8.3.2. Disclosure to the external auditor

Tilburg University has a legal obligation to provide Personal Data of employees to the external auditor (upon request) in connection with, among other things, the audit of the annual accounts. No more Personal Data than necessary will be provided. As there is a legal obligation to provide Personal Data, no Processing Agreement is required. The external auditor is the independent Processor.

8.3.3. Disclosure to bailiffs and debt counselors

In the event of an attachment of earnings by the bailiff, Tilburg University is obliged by law to provide Personal Data to the bailiff in question. These include the amount of the staff member's salary and the term for which the salary is to be paid. Tilburg University requests the bailiff to provide a copy of the guilty verdict and keeps it for the duration of the attachment of earnings.

Processing basis	Legal duty
Disclosure of Tilburg University to bailiff	Only Personal Data of staff members for whom a legal obligation to disclosure applies (e.g., amount of salary and term of salary payment).
Disclosure of bailiffs to Tilburg University	Tilburg University receives a copy of the guilty verdict and keeps it in the personnel file.
Access to data	HRSC only
Storage period	During the attachment of earnings. Afterwards, data relating to the attachment are deleted and destroyed.

Debt assistance provided by or on behalf of the Municipality takes place based on the Dutch Municipal Debt Counselling Act (*Wet gemeentelijke schuldhulpverlening*). Pursuant to this Act, the Municipality may request any information that is relevant to the execution of the debt assistance; this includes requesting Personal Data from Tilburg University if Tilburg University is the employer of the person for whom the debt assistance applies. In this context, Tilburg University provides information about the amount of the salary and whether there have been (previous) attachments of earnings. Only Tilburg University's HRSC is entitled to view information on debt assistance processes.

Basis	Legal obligation (Municipal Debt Counselling Act)
Disclosure of Tilburg University to the Municipality	Only Personal Data that are subject to a legal obligation to provide (including the amount of the salary and whether or not there are—previous—attachments).
Access to data	HRSC only
Storage period	During the debt assistance process. Thereafter, data on the debt assistance process are erased and destroyed.

8.3.4. Provision to the Minister of Education, Culture and Science

Under the law, Tilburg University is obliged to report data under the Senior Executives in the Public and Semi-Public Sector (Standards for Remuneration) Act (*WNT gegevens*) on senior officials to the Minister of Education, Culture and Science. The information to be disclosed is laid down in the law and consists of Personal Data (such as the name of the senior official, position, and remuneration).

Basis	Legal obligation (Standards for Remuneration Act + *Regeling bezoldiging topfunctionarissen OCW-sectoren (*Remuneration Senior Executives Regulations))
Disclosure of Tilburg University to the Municipality	Only Personal Data that are subject to a legal obligation to provide (e.g. name of senior official, position and remuneration)

8.3.5. Provision of aggregated Personal Data

For the sake of completeness, this section concludes with the appointment of parties to whom quantitative data are provided that cannot be traced back to individual members of staff. These data are provided to the VSNU (for quantitative WOPI reporting), Statistics Netherlands (CBS), and Tilburg Municipality[4] (for employment statistics).

8.4. Access to Mailbox or Staff Files

In some situations, it may be necessary for the employer to have access to the mailbox or staff files. Think, for example, in the event of the death of an employee or other situations that make it difficult to transfer work. It is important that this is done carefully and that the (privacy) interests of the staff member are well safeguarded, but that the business interests of the university are also safeguarded. According to the GDPR, employers have the right—subject to certain conditions—to check, for example, professional e-mail. We have the following procedures for this.

It is important for staff to be aware that in some situations Tilburg University may be able to access their professional mailboxes (the uvt.nl e-mail) or files (which are, e.g., stored on the M-drive, MySite on SharePoint, Google Drive, SURF drive). Awareness-raising campaigns are therefore regularly used to bring this to the attention of staff. Staff members are advised to take the following precautions in order to ensure the privacy of the staff member as much as possible in such situations.

- Use of professional e-mail address for private mail: mark this as 'personal' or save it in a folder personal or private. Do not forget “sent items.”
- Private files: Preferably do not put them on your business computer or disk, but if you do: put them in a folder personal or private.
- Files that need to be accessed by colleagues: do not put them on your personal disk but on the unit’s disk so that they are accessible at all times.

[4] An exception applies to the exchange of information with persons from the target group register. More information about this can be found in the chapter *Diversity*.

8.4.1. Request from management in connection with absence of staff member

Absence of staff member	Accessibility of staff member	Example	Procedure
Short-term	**Accessible**	leave illness	In the event of an **urgency**, and it is not possible to wait for the return of the staff member) • The supervisor contacts the member of staff and ask him to provide the necessary information (by e-mail) and, if necessary, to set up an out-of-office with an alternative contact address. **Please note**: The requested information may not be provided by a member of staff by providing his login details.
Short-term	**Not accessible**	Leave illness	In case of an **urgency** (and it is not possible to wait for the return of the staff member): • Supervisor submits a specified request to Legal Affairs. That request includes a motivation why urgent access to the data is needed and specification of the data (what is needed). • Legal Affairs assesses the request and assesses the privacy of the member of staff. Legal Affairs will only give a positive recommendation to the President of the Executive Board if there are serious reasons for doing so. • The Executive Board decides whether access is necessary. • The supervisor informs the employee of the decision. • Based on this consent, the IT Security Officer (hereinafter: ITSO) provides the requested information and, if necessary, sets up an out-of-office indicating an alternative contact address.
Long-term	**Accessible**	illness out of service	• The supervisor contacts the member of staff and asks him to provide the necessary information (by e-mail) and, if necessary, to set up an out-of-office with an alternative contact address. • If a member of staff indicates that he is unable to do so, the member of staff must give his (written) consent to the supervisor

			in order to obtain access to the relevant (specifically mentioned documents) or mailbox or personal disk. • Based on this consent, ITSO provides the requested information and, if necessary, sets up an out-of-office with an alternative contact address. **Please note**: The requested information may not be provided by a member of staff by providing his login details.
Long-term	**Not accessible**	illness, out of service, death	• The supervisor makes a specified request to Legal Affairs. That request includes a motivation why urgent access to the data is needed and specification of the data (what is needed). • Legal Affairs reviews the requests and considers employee privacy. Legal Affairs will only give a positive recommendation to the President of the Executive Board in the event of serious circumstances. • The Executive Board decides whether access is necessary. • Unless the employee has passed away, the supervisor will inform the employee of the decision. • Based on this consent, ITSO provides the requested information and, if necessary, sets up an out-of-office with an alternative contact address. NB: in the event of death, a number of additional measures must be taken. See the Protocol for dealing with the death of a (former) member of staff.
Long-term/ short-term		Conflict in the workplace	• The supervisor makes a specified request to Legal Affairs. That request includes a motivation why urgent access to data is needed and a specification of the data (what is needed). • Legal Affairs reviews the requests and considers the employee's privacy. Legal Affairs will only give a positive recommendation to the President of the Executive Board in the event of serious circumstances.

			• The Executive Board decides whether access is necessary. • The supervisor informs the employee of the decision. • Based on this consent, ITSO provides the requested information and, if necessary, sets up an out-of-office with an alternative contact address.

If mailboxes or personal disks have to be made available (after the consent of the staff member or the decision of the Executive Board), ITSO will follow the following procedure.

- A copy of the mailbox is made, of which will be deleted:
  - all e-mails in the folder personal or private,
  - all emails that are flagged as personal/private,
  - sent items: all e-mails older than 30 days,
  - deleted items/junk e-mails: all e-mails.
- A copy of Personal disk/computer is made, of which will be deleted:
  - folders marked personal or private.

After deletion of this data, the copies are transferred to the supervisor.

The procedure described above applies to existing data. If it is necessary to obtain access to future correspondence and if an out-of-office address including an alternative contact address is not sufficient, the following procedure applies.

Absence of staff member	Accessibility of staff member	Example	Procedure
Long-term/ short-term	**Accessible/ inaccessible**	illness, out of service, death, conflict in the workplace	• The supervisor makes a specified request to Legal Affairs. That request includes a motivation why urgent access to future data is needed and a specification of the data (what is needed). • Legal Affairs reviews the requests and considers the employee's privacy. Legal Affairs also determines whether a supervisor or an independent person should be granted access. Legal Affairs will only give a positive recommendation to the President of the Executive Board in the event of serious circumstances. • The EB decides whether access is necessary and for how long. • Unless the employee has passed away, the supervisor will inform the employee of the decision.

			• ITSO implements the technical measures based on this consent.

8.4.2. Request by the next of kin in the event of a staff member's death

In the event of the death of a staff member, it is important that this be dealt with carefully. See the Protocol for dealing with the death of a (former) member of staff. It may happen that next of kin request the personal files of the staff member. Think for example of photos etc. that are stored on the computer of the staff member in question. These requests will be received through supervisor(s).

Request for Personal Data of next of kin	If the next of kin request Personal Data from the staff member, this must be done carefully. Supervisors should try to find out which personal documents the next of kin want to receive. • The supervisor submits a request to Legal Affairs, who assesses this request and provides advice to the Executive Board. Generally, a request for inspection will not be honored, unless there are very special circumstances (e.g., suicide or missing person). Files that are **not** transferred are professional e-mail and documents relating to Tilburg University, internal e-mails, files sent to and from Third Parties, the complete mailbox, the Tilburg University password, or a complete copy of the hard disk. • The Executive Board takes a decision and can provide guidelines for this. • Based on the EB's decision, ITSO secures the mailbox and hard disk of the computer. • On behalf of the Executive Board, the confidential advisor will examine the mailbox and/or data files in collaboration with the ITSO. • The confidential advisor will take care of further processing in consultation with the next of kin. For more details see the protocol for dealing with the death of a (former) member of staff.

8.4.3. Integrity research

Access to the mailbox or staff files may be necessary in the context of an integrity audit. It is, of course, important that this be done carefully, whereby a balance is made between the privacy interests of the staff member and the interests of the university in the context of the research. The research is carried out carefully and confidentially.

Integrity research	If access to Personal Data is necessary in the context of a suspicion of a breach of integrity, the following procedure applies. • The supervisor reports the suspicion of a breach of integrity to the GRC officer. The GRC officer determines whether access to mailboxes or personal drives is necessary for the purpose of research and whether access to e-mail or files marked as personal is necessary. If this is desirable within the framework of the

	additional burden of proof, the GRC Officer will submit a (motivated) request to Legal Affairs. • Legal Affairs assesses the request and the privacy of the staff member. Legal Affairs will only give a positive recommendation to the President of the Executive Board if there are serious reasons for doing so. • The Executive Board decides whether access is necessary. The integrity audit is carried out under the responsibility of the GRC officer or Internal Audit, never by a supervisor. ITSO provides the GRC officer with a copy of the data.

9. Out of service (inactive and former employees)

This chapter deals with the processing of Personal Data after the expiry of the contract between Tilburg University and the staff member. This could include the situation in which the temporary employment contract was terminated, the staff member retired, or was dismissed. Ending of the relationship with PNIL also falls under this category.

9.1. Termination of Employment

If a staff member leaves the university, he or she must be reported to the Tax and Customs Administration, the ABP, and the Employee Insurance Agency (UWV) under the law. If a residence permit has been applied for for a staff member, Tilburg University informs the IND about the termination of the contract. If the salary is attached, the attaching party is informed that the staff member is leaving the service. There is a legal basis for these data transfers.

Termination of employment is also passed on to *CZ*, *Loyalis*, and *Centraal Beheer*. These concern limited Personal Data that enable the external parties to assess whether the former staff member can still make use of the group discount. Tilburg University has a legitimate interest in providing Personal Data to these parties upon termination of employment.

From the time of the termination of employment, the supervisor no longer has access to the staff member's personnel file. HR will continue to have access to the personnel file for completing of the termination of employment. The personnel file is archived and destroyed in accordance with the storage periods laid down for that purpose. An exception is made for personnel files that are of historical importance to Tilburg University. If the file is of historical importance to Tilburg University, it can be assumed that Tilburg University has a legitimate interest in keeping these files longer than the regular personnel files.

Notification of termination of employment to the tax authorities, ABP and UWV	Tilburg University is required by law to notify the Tax and Customs Administration, the ABP, and the UWV of the termination of employment of a staff member. Only the Personal Data explicitly mentioned in the specific Article of the law will be provided.
Notification to IND in case of residence permit	Tilburg University informs the IND about the termination of employment of a staff member for whom a residence permit has been applied for based on the Dutch Aliens Regulations 2000 (*Voorschrift Vreemdelingen 2000*). This report is based on the Legal duty of information that Tilburg University has towards the IND.
Notification to CZ, Loyalis and Centraal Beheer	Tilburg University informs insurers (e.g., *CZ, Loyalis* and *Centraal Beheer*) about the staff member's termination of employment so that these parties can check whether the former staff member can still make use of the group discount based on justified interest.

Personnel file Storage period	From the time of the termination of employment, the supervisor no longer has access to the staff member's personnel file. HR will continue to have access to the personnel file for the completion of the termination of employment in accordance with the set storage periods. The storage periods are determined per document by the Executive Board based on the applicable legislation and with due observance of the applicable guidelines. In general, the following storage periods apply:
	• Up to 7 years after termination of employment: payroll administration
	• Up to 5 years after termination of employment:
	  ○ proof of identity
	  ○ payroll tax statement
	• Up to 2 years after termination of employment: other information
	
	These periods are in addition to those laid down in this Policy. See, among other things, the different deadlines for R&D interviews and situations in which Tilburg University's own-risk bearer status play a role (WW, ZW and WIA).
	
	The personnel file shall be stored and erased in accordance with the storage periods laid down for that purpose. In accordance with the provisions of the AP, an exception applies
	• to personnel files that are of historical importance to Tilburg University. If the file is of historical importance to Tilburg University, it can be assumed that Tilburg University has a legitimate interest in keeping these files longer than the regular personnel files. These files are kept for as long as they are considered to be of historical importance.
	• If there is or has been a conflict in the workplace, or if legal proceedings are underway. These files are kept for a period of 10 years from the end of the last transaction in the file.

9.1.1. Disclosure to the Employee Association

The Tilburg University Employee Association is informed about the termination of contract of an employee. If a member leaves the service, membership of the Employee Association ends automatically. There is a legitimate interest in informing the Employee Association of the termination of employment of one of its members. Only the necessary Personal Data are provided.

Former staff members who retire or retire early can remain or become members of the Employee Association. For this purpose, the former staff member fills out a form on the Tilburg University website. The completion of this form constitutes a contract between the former staff member and the Association. For the purpose of implementing this agreement, the Employee Association is entitled to process Personal Data. It concerns name and address details, date of birth, and contact details. Thes data are used to invite the member to activities. In this case, the basis for processing the Personal Data is the agreement.

9.1.2. Internal provision to Alumni Relations

HR passes on the contact details of full professors to Alumni Relations when they leave the service. The basis for this internal disclosure of data is justified interest. Tilburg University attaches great importance to a good relationship with former full professors and would like to keep them associated with the university. Alumni Relations uses the contact details to contact the full professors in the context of knowledge dissemination (such as organizing knowledge sessions and guest lectures). In this context, see also the thematic policy External Relations.

Commented [MB1]: NL link werkt niet, dit is het Engelstalig document

9.2. Unemployment

Based on article 72a of the WW, Tilburg University is obliged by law to bear its own risk for the WW. This means that the university pays the WW benefit and is obliged to support the former staff member in finding other work after the termination of his employment. In addition, a staff member may be eligible for an unemployment benefit over and above the statutory entitlement (*bovenwettelijke WW uitkering,* BWNU). In this context, Personal Data concerning the staff member's unemployment are exchanged with the UWV (the statutory body issuing the WW decision) and Raet (in the context of the payment of the supra-statutory BWNU benefit).

Personal Data are also processed in order to support the employee in finding another job. These data may include the employee's performance (to find out what type of job is suitable) and salary (to assess the level at which a job should be sought). Usually the counseling of the former staff member is done by the HR advisor. Personal Data that are processed in the context of unemployment counseling are only visible to this HR advisor. In an individual case, an external party may be called in to carry out Tilburg University's obligation to assist in finding a new job. If this is the case, it will be investigated beforehand whether this party acts in accordance with GDPR and the due care with regard to the processing of Personal Data will be laid down in a contract.

Processing basis	Legal obligation (Article 72a WW) Implementation of the employment contract (CLA, BWNU)
Content of the processing	The former staff member's Personal Data are processed necessary for the execution of the legal obligation under Section 72a of the WW. This may include performance data (in the context of reintegration counseling) and salary data (for the purposes of being able to pay the unemployment benefit).
Data exchange Tilburg University with UWV	The former staff member applies for unemployment benefit from the UWV. The UWV provides Tilburg University as an interested party (because of its legal obligation) with a copy of the WW decision. Tilburg University is entitled to pass on Personal Data of the former staff member to the UWV upon a request for advice on a reintegration measure to be used (training or start-up facility), upon a request for exemption from the obligation to apply for a job, and in the event of culpable behavior on the part of the employee.
Data exchange Tilburg University with RAET	The ex-staff member applies to Raet for a non-statutory benefit himself. Part of this form is completed by Tilburg University as an employer or

	former employer. Raet provides Tilburg University as an interested party (in connection with payment of the benefit) with a copy of the BWNU decision.
Involvement of external counseling services	If a Third Party is called in to support the reintegration of a former employee, the agreements regarding the processing of Personal Data are recorded. In most cases, there will be two separate Controllers.
Storage period	Personal Data that are specifically processed in the context of the WW and/or BWNU benefit will be kept for the duration of the benefit.

9.3. Own-risk Bearer Status for the Sickness Benefits Act and WGA

In addition to its own-risk bearer status for the Unemployment Insurance Act, Tilburg University is also its own-risk bearer for the Sickness Benefits Act and WGA. This means that Tilburg University retains obligations to its ex-staff members in situations of incapacity for work. In the Chapter Sickness, Absenteeism, and Medical Records of this Policy, the Personal Data that are processed in this context are discussed in more detail.

9.4. Pensioners

Tilburg University attaches great importance to maintaining contact with retired employees. In the letter that employees receive at the end of their employment, they are asked for consent to be included in the relationship file. The data is only used to invite former staff members to the annual day that Tilburg University organizes for pensioners.[5]

Processing basis	Consent
Content relationship file	Contact details (name, address, e-mail).
Access to relationship file	Organizers of the pensioners' day. Access is necessary for the execution of the work.
Withdrawal consent	If a pensioner withdraws his consent, his data will be erased from the relationship file.

9.5. Death of a Staff Member

In the event of the death of a staff member, Personal Data is processed at various levels, such as the processing of the date of death in the Personnel Administration and contacting the next of kin. The procedure for this is elaborated in the protocol for dealing with the death of a (former) member of staff. A next of kin or supervisor may wish to have access to the mailbox or files of the deceased staff member. See in this context **Section 8.3.2**.

Section 9.1 of this Policy (where applicable) also applies to the processing of the employment of the deceased staff member.

[5] For retired full professors, this processing of Personal Data applies in addition to Section 9.1.2.

9.6. Disclosure of Information to or about Former Members of Staff

Former members of staff will no longer have access to their own personnel files from the date of their termination of employment. Employees are informed of this in a letter that they receive prior to leaving the service.

Request for information from a former staff member	If a former staff member requests a copy of (part of) his staff file (e.g., contract of employment, salary slip, or annual statement), he must submit a request in accordance with the relevant procedure. The requested information will not be provided until after the identity of the applicant has been verified by checking a masked copy of the identity document. The copy will be destroyed after verification.
Request for information about former staff member by Third Parties	Information about a (former) staff member to a Third Party (such as reference check by a potential new employer) is only provided with the written consent of the (former) staff member concerned.
Testimonial	A testimonial is drawn up at the request of the staff member. This testimonial contains only the following information: name, date of birth, nature of work, working hours, date of commencement of employment, and date of termination of employment. This may be supplemented, at the request of the staff member, by additional information concerning the manner in which he carried out his duties and the reason for his termination of employment.

10. External Employee (PNIL)

This Thematic Policy does not only concern persons who have an employment contract with Tilburg University; it also concerns persons who carry out work for Tilburg University in a different way. This could include (unpaid) trainees, volunteers, employees of a temporary employment agency (or KCS), freelancers, seconded staff, or specific types of professors. Together, these categories are known as "external employees" or PNIL (in Dutch: Persoon niet in loondienst).

10.1. Pre-contractual Obligations

Before starting work, a PNIL employee fills in a form and sends it to Tilburg University with an original, undisguised copy of the identification document. The copy of the identity document is necessary for Tilburg University to carry out its statutory verification obligation. Tilburg University checks both whether the person actually is who he says he is and the validity of the identity document. The Personal Data are transferred from the identification document to the Tilburg University administration in accordance with the legal obligation. This concerns the name and address details, the date of birth, the BSN, nationality and type of identity document, number, and period of validity. After performing this duty, the copy of the identification document will be destroyed.

The name and contact details are also used for the execution of the specific agreement and thus making the Tilburg University facilities and provisions available. This concerns access to the intranet, a Tilburg University e-mail address, wireless access, the employee printers, Tilburg University SharePoint, Tilburg University card, and/or the library's lending system.

Processing basis	Legal obligation (verification obligation) Execution of the contract
Content of the processing	Name and address details, contract details, date of birth, BSN, and nationality.
No copy identity document	Copy destroyed after performing verification obligation and taking over data. No copy will be included in the administration. There is a legal obligation to register the type of identity document, number, and period of validity.
Storage period	Seven years, starting after the end of the calendar year in which the PNIL relationship ended.

10.2. International PNIL

For persons who do not have the nationality of one of the countries of the EEA, the legal obligation to make a copy or scan of the identity document and to keep it in the administration applies pursuant to Article 15 of the Foreign Nationals (Employment) Act. This is, therefore, an exception to the main rule that no copy of a PNIL's identity document is kept.
In addition, Tilburg University has the legal obligation to copy and keep in the administration a possible A1 certificate, the residence permit and work permit of the international PNIL (Article 28, paragraph 1(f) Salaries Tax Act 1964).

Processing basis	Legal obligation (Foreign Nationals (Employment) Act + Salaries Tax Act 1964)
Content of the processing	Copy of identity document, A1 certificate, residence permit, and work permit.
Storage period	Five years, starting after the end of the calendar year in which the PNIL relationship ended.

10.3. Additional Processing of Personal Data on the Grounds of Legal Obligation

For all categories, a copy of the agreement (such as an assignment agreement for a self-employed person and the secondment agreement with a seconded person) is kept in the administration. In accordance with tax legislation, the agreements are kept for seven years after the end date of the PNIL relationship.

In addition, the following Personal Data will be processed:

- In the case of a self-employed person: if the self-employed person has a Declaration of Independent Contractor Status (VAR Declaration), there is a legal obligation to include the VAR Declaration in the administration, including the number and period of validity.
- In the case of a hired employee (temporary employee such as a KCS employee): data of the supplier + specification of the hours worked.

Processing basis	Legal obligation (payroll administration, Collection of State Taxes Act 1990 + Wage-Benefit Linkage and Exceptions Act (WKa))
Contents	- The specific agreement(s) - Self-employed: VAR Declaration (including number and period of validity) - Hired employee: name, address, and place of residence of the supplier and registration number of the supplier at the Chamber of Commerce + specification of hours worked
Storage period	Seven years, starting after the end of the calendar year in which the PNIL relationship ended.

10.4. PNIL Full Professors

This section deals specifically with Tilburg University's relationship with PNIL full professors, i.e. professors who do not have an employment contract with Tilburg University, but who are connected to the university in a different way.

10.4.1. Endowed professors

An external organization may request the establishment of an endowed chair at Tilburg University. A professor is sought to fill in the chair. The endowed professor is appointed as a professor by the Endowed Chair Foundation for a period of five years. The way in which the employment relationship with the endowed professor is structured depends on the actual situation. In addition to an employment contract, an appointment as a PNIL is an option (secondment or hospitality agreement). The provisions of Section 10.4 apply to the PNIL endowed professor with respect to the processing of Personal Data.

In the diagram below, the focus is only on the additional Personal Data that Tilburg University processes.

Processing basis	Implementation of the agreement (+ Higher Education and Research Act)
Contents	- the appointment proposal (advice from the Dean, report from the Selection Committee including advice from three external professors, the CV, and the publication list); - the appointment decision; - The agreement (hospitality or secondment agreement)
Storage period	Five years, starting after the end of the calendar year in which the PNIL relationship ended.

10.4.2. Emeritus professors

If Tilburg University wishes to commit an emeritus professor more closely to the university, a hospitality agreement or an unremunerated appointment as a full professor (PNIL) are possible. The provisions of this section apply to the emeritus PNIL regarding the processing of Personal Data.

10.4.3. Ancillary activities

The Sectoral Scheme Covering Ancillary Activities has been declared applicable to PNIL professors. As a result, professors who are not employed are also obliged to apply to Tilburg University for permission to perform ancillary activities. As a result, the provisions of Section 4.5 of this Policy apply equally to PNIL professors.

10.5. The PNIL Relationship and the Processing Agreement

Under the GDPR, the conclusion of a Processing Agreement is mandatory in the case of an exchange of Personal Data with a Processor. KCS and other temporary employment agencies and the Endowed Chair Foundation are independent Processors. In the main contract, agreements are made with these parties about the division of responsibilities within the framework of the GDPR. In the case of secondment, there are two separate Controllers as well and the necessary agreements are made in the main contract.

Whether a Processing Agreement should be concluded with a self-employed person depends on the effective relationship with the self-employed person. If Tilburg University is able to give specific instructions for the execution of the assignment, the self-employed person will not easily be regarded as a Processor and a Processing Agreement is not required. In order to ensure that a self-employed person handles the data correctly, the contract for the assignment contains provisions on the handling of Personal Data. If the self-employed person carries out a specific assignment remotely, Tilburg University has no authority of any kind, and the instructions that Tilburg University may give for the performance of the agreement are limited, the self-employed person qualifies as a Processor and a Processing Agreement is required.

PNIL professors always carry out work under the authority of Tilburg University. No Processing Agreement is required. The agreement concluded with the PNIL professor includes a confidentiality clause.

Processing Agreement possible required	Self-employed person
Processing Agreement not required	Temporary employment agency (including KCS), seconded people, PNIL professor, (unpaid) trainees, volunteer.

Appendix 1: Definitions

Concept	Definition
Anonymizing / Anonymous data	Information that does not relate to an identified or identifiable natural person or to Personal Data rendered anonymous in such a way that the data subject is not or no longer identifiable (for example, for statistical or research purposes)
Policy	This Policy with regard to the processing of Personal Data at Tilburg University (Privacy & Personal Data Protection Policy)
Personal Records Database	The Personal Records Database is a central database with Personal Data of the inhabitants of the Netherlands. It also contains data on Dutch nationals abroad. The Personal Records Database is the successor to the Municipal Database Personal Records.
Data Subject	An identified or identifiable natural person to whom personal data relates
Special Personal Data or special categories of Personal Data	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership; and genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a person's sex life or sexual orientation
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data
Data leak (i.e., Personal Data breach)	A breach of security which accidently or unlawfully results in the destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to personal data transmitted, stored, or otherwise processed
Third Party	Any natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process Personal Data
Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (PIA)	An assessment of the impact of the envisaged processing operations on the protection of Personal Data that helps to identify privacy risks and offers ways to reduce the risks to an acceptable level.
EU-US Privacy Shield	The privacy shield has been in effect since July 2016 and aims to ensure a level of protection of Personal Data exchanged with the U.S. that is essentially equivalent to that within the European Union (EU). Organizations in the U.S. certifying to the Privacy Shield offer an adequate level of protection (for the duration of the certification). The privacy shield replaced the Safe Harbour Agreement, which was declared invalid by the European Court of Justice on October 6, 2015.

Identity Document	The legal identity papers (a passport, a Dutch identity card, an ID card or a passport from an EEA country, or a Dutch aliens' document). At Tilburg University, employees and students can also identify themselves with a driving license and the Tilburg University card with passport photo.
Taskforce Data Protection	The Taskforce Data Protection consists of representatives in the following disciplines: • Legal Affairs • Governance, Risk & Compliance • Information Security • Information Awareness Depending on the subject matter, other employees or organizational units can participate.
Personal Data	Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, particularly 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
Data Protection by design and by default	The implementation of appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this EU General Data Protection Regulation and protect the rights of data subjects.
Pseudonymizing	The processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person
Right to restriction of processing	The right to restriction means that the Personal Data may not be (temporarily) processed or modified. The fact that the processing of Personal Data is limited must be clearly indicated in the file by the controller so that this is also clear to recipients of the Personal Data. If the restriction is lifted again, the data subject must be informed accordingly (Article 18 GDPR).
Right to object	On grounds relating to his particular situation, a data subject can make use of the right to object to processing of personal data concerning him when the requirements of the Regulation are met. If a data subject objects, the controller ceases processing, unless compelling justified grounds provide otherwise (Article 21 GDPR).
Right to data portability	This means that a data subject shall have the right to receive the personal data concerning him from the controller in a structured, commonly used, and machine-readable format and shall have the right to transmit or have the data transmitted directly to another controller unless this adversely affects the rights and freedoms of others. A data subject has the right to data portability for data provided by himself (Article 20 GDPR).

Right to erasure /right to be forgotten	The controller is obliged to erase the Data Subject's Personal Data without undue delay, amongst other things, on the following bases: • the Personal Data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; • the data subject withdraws his consent and no other legal ground for the processing exists; • the data subject objects to the processing; • the personal data have been unlawfully processed (Article 17 GDPR)
Right to be informed	A data subject must be informed of the fact that the processing of his Personal Data is being or will be carried out and for what the purposes this is done. The GDPR indicates which information must in any case be provided, for example, information on the period, the rights of the data subject, the source of the data and the legal basis for processing. If the purpose of the processing changes, information about this must also be provided (Articles 13–14 GDPR).
Right of access	The data subject has the right to know whether his Personal Data are being processed by the controller. The GDPR contains an enumeration of the information for which the right of access applies. The controller must provide the data subject with a copy of the Personal Data that are being processed (Article 15 GDPR).
Right to rectification	The data subject has the right to rectification of inaccurate personal data concerning him or the right to provide a supplementary statement if the processing takes place on the basis of incomplete data. The rectification needs to take place without undue delay. The controller is obliged to inform every person who received the Personal Data of every rectification, unless this is impossible or would involve a disproportionate effort (Article 16 GDPR).
Consent (of the Data Subject)	Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him (Article 4(11) GDPR).
Processor	A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the controller
Processor contract	The contract between a controller and processor in which agreements are made regarding the processing of Personal Data aiming to safeguard the data protection of the data subject (Article 28, Section 3 GDPR)
Processing	An operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data.
Processing basis	A condition for the lawful processing of personal data as specified in Article 6 GDPR (e.g., consent, legal obligation).

Data processing register	The records of the processing activities as referred to in Article 30 GDPR that must contain certain data for the purpose of accountability
Controller	The natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State (Dutch) law, the controller or the specific criteria for his nomination may be provided for by EU or Dutch law

Appendix 2: Processing Bases

Processing basis	Explanation
Necessary for legal obligation	• This basis applies if the Disclosure is based on a legal obligation; • In the event of Processing on this basis, the Data Subject has no right of data erasure (deletion);
Necessary for the execution of a contract	• The Data Subject must be a party to the contract; • Only if the contract cannot be properly executed without the Processing taking place, "necessity" applies. The fact that something is handy does not necessarily mean that it is necessary; • Processing operations that are necessary prior to the conclusion of a contract may also be covered by this Processing Basis, provided that they are carried out at the Data Subject's request;
Necessary for task of general interest/public authority	• Public authority is involved in the performance of a public service task; a task of a public authority that is regulated by law; • In the event of Processing on this basis, the Data Subject will not be entitled to data erasure (deletion);
Necessary for vital interests	• In principle, an invocation can only be made on this basis if the Processing cannot be based on any other ground; • A vital interest touches on the life of a person.
Necessary for legitimate interest	• The Processing must be necessary for the representation of the legitimate interests of Tilburg University or a Third Party; • A balance of interest also applies: the Processing may not take place if the interests or fundamental rights and freedoms of the Data Subject outweigh the aforementioned interests of Tilburg University or a Third Party; • The Data Subject may object to the Processing at any time, after which Tilburg University discontinues the Processing or puts forward compelling justified grounds for disregarding the objection; • Examples of legitimate interests are fraud prevention, direct marketing, and network security. Depending on the balance of interests, Processing for these purposes may or may not take place; • When weighing up the interests, consideration will be given to whether the Data Subject can reasonably expect Processing to take place for that purpose.

Consent	• The Data Subject must be properly (clearly) informed in advance of the Processing for which he gives his Consent. See the **Privacy & Personal Data Protection Policy Chapter 10.3** for more information. • Consent must be actively given. That means no use of a pre-filled check box. • It must be possible to demonstrate the Consent afterwards; • Is Consent given by means of a statement that also relates to other matters? In this case, the request for Consent must be presented in a comprehensible and easily accessible form and in plain language in such a way that a clear distinction can be made from other cases. Think, for example, of including a separate check box on a form; • Consent may be withdrawn by the Data Subject at any time and must be as simple as granting it.