Thematic Privacy & Personal Data Protection Policy—Processing Personal Data

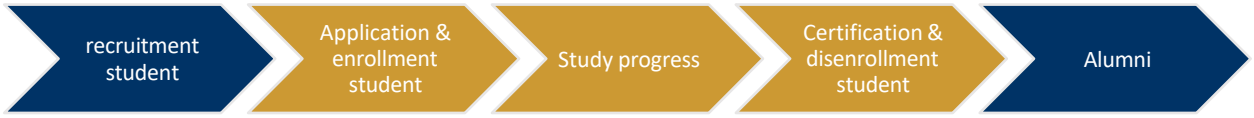
EDUCATION AND STUDENTS

Readers' Guide

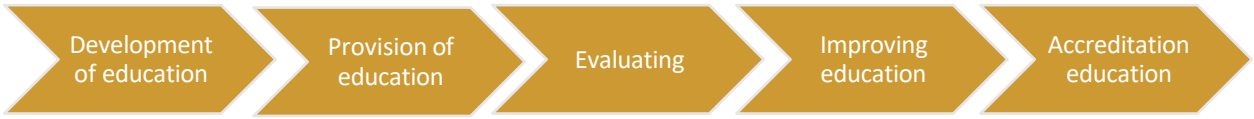
This Policy is part of the Privacy and Personal Data Protection Policy and describes the way in which Tilburg University implements the General Data Protection Regulation (GDPR) for the protection of Personal Data relating to education and students.

For the sake of readability, we have divided this Policy into 2 parts based on the life cycle of education and students.

Life cycle students



Life cycle education



All information regarding European legislation (GDPR) and the Protection of Personal Data is available on a **Tilburg University website**[1] including the Frequently Asked Questions. Practical details and examples can also be found on this website.

Each School/Division within Tilburg University has appointed Data Representatives. They are the first point of contact for employees in case of questions about the Protection of Personal Data. This Policy includes references to other policy documents. These are marked as "**referrals**". The applicable guidelines are set out 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/privacy.

Table of Contents

1. Introduction

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 (ANR), or other data that uniquely identifies an individual. However, it may also be a combination of a number of data that cannot be traced back to a person on their own but can be traced back in combination, or can be traced back to a person in the future in the form of, for example, technical possibilities, the so-called Traceable Personal Data. The combination of, for example, place of residence, age, and study program can be traced back to a person. When it comes to data that relates to an individual, it quickly becomes Traceable Personal Data.

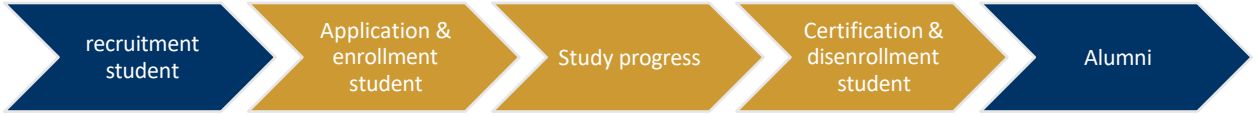
In education we are dealing with (prospective) students or course participants of whom we Process Personal Data. Tilburg University attaches great importance to the careful Processing of Personal Data in the context of education, for which we seek a good balance between privacy, security, and functionality because the misuse of data can cause major damage to students, employees, and Tilburg University. The GDPR talks about the Data Subject; in education this mainly concerns Students and Course Participants. In this Policy, both groups will be called Students.

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, providing (forwarding), distributing or making available, combining, shielding, or erasing data. It concerns paper files or archives, electronic 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 within the framework of Education and Students under the responsibility of Tilburg University and applies to everyone working under the responsibility of Tilburg University.

The further elaboration of this document is based on the so-called life cycle of a student and education.

Life cycle students



The process steps marked in blue are described in the **Thematic Policy on External Relations**.

Life cycle education

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 Students and Education, 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 Data Processing Register.

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

1. the enrollment for education;
2. the organization or provision of education, guidance (in education or careers) or study advice, and the issuing of diplomas or other certificates;

[2] Based on the exemption decree Personal Data Protection Act

3. Disclosure or provision of information and the communication with Data Subjects about the institution's products and services;
4. publicizing the activities of the institution or its partners;
5. keeping a record of the information transmitted;
6. calculating, recording, and collecting enrollment fees, school and tuition fees, and contributions or remunerations for educational resources and extracurricular activities, including placing claims in the hands of third parties;
7. dealing with disputes and arranging for audits to be carried out;
8. implementing or applying legal provisions;
9. granting electoral rights in the context of participation;
10. immigration purposes (making it possible or contributing to making it possible for (prospective) students to travel to the Netherlands).

Purpose limitation	• Processing of Students' Personal Data is permitted if the Processing is based on one of the purposes mentioned above. • If a Processing takes place on the basis of 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.

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

2.2. Students' Rights

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

Right	Students 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 relation to their person. **Please note** that there may be exceptions to this rule on the basis of the Dutch Medical Treatment Contracts Act.
Right of rectification	demand at all times to have incorrect Personal Data 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 to erasure	make an application to erase his Personal Data.
Right to object	indicate that he does not wish to have his data processed (anymore).

A student may exercise these rights and, for example, request access to the information of the data we have recorded about him or request that his data be erased. The request for erasure does not have to be complied with in all cases. Exceptions to this are data that Tilburg University must legally record, such as the recording of obtaining a diploma.

If a student invokes one of these rights, the employee must contact the Data Protection Officer (DPO). The latter will coordinate the requests and assess them. However, this does not apply to the right to rectification. Changes of contact details or other information must be made by the employee himself (or the student directly via *Studielink*).

Students' Rights	Students have the rights of Data Subjects as mentioned in the GDPR. For more details, please refer to the **Privacy & of Personal Data Protection Policy—Chapter 10.**
Responsible	Data Protection Officer: staff member must contact with the DPO if there is a request from the Data Subject (with the exception of rectification).
Right of access	Employees make various notes in the Students' files, for which Students have the right of access. It is important that these notes are made carefully and are factually correct and can be shared with the Student in case of access.

A person other than the Data Subject may request information. Think, for example, of parents who want to contact or receive a student's study details.

Request for information by PARENTS or THIRD PARTIES	In principle, requests from third parties (including parents/guardians) for information about students will never be granted (see exceptions below). **Please note**: Exception for student counseling provided the student has given his permission (see **Section 5.4**).
Informing the contact person indicated contact person and relevant authorities in the event of a life-threatening or medical emergency	In the event of a medical emergency, information about the student's medical emergency may be provided to parents and relevant emergency services. At the enrollment procedure, a student can provide contact details in case of a (life-threatening or medical) emergency.

2.3. Services to other Educational Organizations

Several units of Academic Services provide services to other legal entities. Think, for example, of TIAS or the TU Eindhoven. If we provide administrative services, we are the Processor and the other legal entity is the Controller, but, of course, the reverse is also possible: another entity provides administrative services regarding students for Tilburg. It is then important that we enter into a so-called Processing Agreement in which the agreements regarding the Processing of Personal Data are included. It is complex to determine what the role is and which agreement should be concluded. We refer to the **Privacy & Personal Data Protection Policy, Section 11.4.**

Services for or by third parties regarding STUDENTS	If Tilburg University is Processor for another organization or if the Controller appoints another organization as Processor, a Processing Agreement must be concluded.

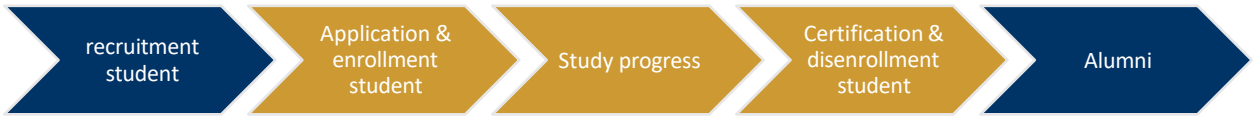
Tilburg University receives a lot of information about students via *Studielink*, which also includes links to the Dutch Education Executive Agency (DUO), the Dutch Personal Records Database, and the Dutch Immigration and Naturalisation Service (IND). This is a consequence of the **Legal Obligation** to provide and receive information. In this case, there is no need to conclude a Processing Agreement with these parties.

Part I: STUDENTS

This part elaborates on the guidelines for the Processing of Personal Data derived from the GDPR on the basis of the life cycle of a student.

Life cycle students

The life cycle of students includes the following phases:



3. Recruitment Student

The recruitment of students is part of the **Thematic Policy on External Relations**.

4. Application & Enrollment of the Student

The applications of students or course participants are made in various ways based on the type of application via *Studielink* or Tilburg University systems or forms. It concerns the following categories:

Prospective and new Bachelor's and Master's students
Pre-Bachelor's students
International Students
Course participants Language Center, Contract students, Minor students, Summer School students
Covenant students
Incoming Exchange students

4.1. Processing Bases

Tilburg University enrolls various categories of students and this enrollment is based on the performance of the Study Contract. For a number of aspects and Personal Data, the basis could also be "necessary to comply with a legal obligation," but, for the sake of simplicity, we opted for "**necessary for the performance of a contract**." We refer to **Appendix 2** for an overview of the Processing Bases.

Processing basis for application/ enrollment	The Processing Basis for student enrollment is "**necessary for the performance of a contract**." The Processing Basis must be stated in the Data Processing Register.

This basis applies only to the Processing of Personal Data that we need to have in order to perform the agreement. If we Process additional data, the basis for this is, in principle, legitimate interest, or permission from the student is required. Think, for example, of a photo he uploads on behalf of his university card (verification with a copy of his Identity Document when picking it up), or passing on information to the TOP Week Foundation to approach new students for the introduction week. The student's photographs can also be included in Osiris if he gives permission for this by means of a checkbox.

Processing basis additional information	The Processing Basis for additional data that is not necessary for the application or enrollment of the student is **legitimate interest** or **consent**. The Processing Basis must be recorded in the Data Processing Register.

4.2. Personal Data

Based on the GDPR, a number of requirements have been set for Personal Data in order to guarantee privacy interests, whereby a distinction is made regarding Special and Sensitive Personal Data.
When registering Students, we process the following Personal Data:

- General Personal Data: Name, sex, date of birth, place of birth, country of birth, first and second nationality, home address, correspondence address, and contact details (telephone, e-mail and correspondence language). These data are recorded in the Student Information System (Osiris or Mysas). In addition, a student number and an e-mail account will be generated.
- Citizen Service Number is supplied by the Personal Records Database (BRP) and is permitted on the basis of a legal obligation (HERA)
- Alien Registration Number from the IND via *Studielink* (if applicable)
- Admission tests (e.g., English and Mathematics) for the purpose of assessment against the educational requirements (for international and national students)
- Other information: Based on the BSN, DUO provides additional information such as the personal education number (OC&W number), previous education details (from the diploma register), and an indication of the tuition fees.
- For the purpose of admission, diplomas and grade lists (with certified translations) are also requested from international students for the purpose of the admission officers' assessment of the study program's requirements.
- In addition, data of the study program for which the student enrolls will also be included.

During the application process, it is always checked whether the prospective/potential student (applicant) meets all enrollment conditions. As soon as a prospective student has completed the entire application process and has met all the admission requirements, his applicant status will be changed to student (person enrolled).

Providing Personal Data by *Studielink*	The provision of Personal Data for the application and enrollment of students takes place on the basis of a **legal obligation**. It is, therefore, not necessary to conclude a Processing Agreement.
Citizen Service Number	The BSN may be processed based upon a legal obligation, for example: • for the application and enrollment of a student on the basis of Article 7.31 e of the Dutch Higher Education and Research Act (HERA). • For participants civic integration language training (article 49 Civic integration act).
Special Personal Data	For student applications and enrollments, it is **not permitted** to register the Student's **Special Personal Data**[3].
Copy passport	For the application and enrollment, the storage of a copy of the identity document is only permitted: • when the student does not have an EU nationality for the application of a visa with the IND.

[3] For more information, see **of the Privacy & Personal Data Protection Policy, Section 4.3.**

	• In the case of study abroad, Tilburg University will provide a copy of the Identity Documentation to the foreign institution[4]. Students give their **explicit consent** for this. For identification purposes, it is sufficient to see a proof of identity. Storage is only permitted if the copy is marked (reason stated) and masked (photo and BSN struck through). For more information, see **Privacy & Personal Data Protection Policy Section 4.4.2**.
Admission tests	Prospective students shall also provide information on admission tests (e.g., TOEFL, IELTS, statistics) if necessary for admission purposes.
Alien Registration Number	The Immigration and Naturalisation Service will add the Alien Registration Number via *Studielink* if this applies to the student in question.
International students	For admission purposes, international students provide a copy of their diplomas and grade lists (with a certified translation if necessary) and a copy of their identity documents (based on the legal obligation in the HERA). If they already have a residence permit, Tilburg University will also receive a copy of this (front and back).

During the period of their enrollments, students are expected to keep their contact details in *Studielink* up to date. If the student makes a mutation in *Studielink*, this Personal Data will be transferred to Osiris by *Studielink*. Even if the data of the Data Subject changes in the Personal Records Database, they are still entered into Osiris via *Studielink*.

4.2.1. Underage students

In most cases, students are over 16 years of age. However, it is possible that students are younger. Think, for example, of students who attend a few courses, or who have accelerated their pre-university education (VWO). In the GDPR, there are separate rules for students who are younger than 16 years.

Underage students	If a student is underage, the following rules apply: • Younger than 12 years of age: authorization by the parent/guardian. • From 12 to 16 years of age: authorization by the student and parent/guardian. • 16 years and older: authorization by the student

4.2.2. Update Personal Data

In general, students must inform *Studielink* of any changes in Personal Data. Data that are updated in the Personal Records Database are automatically updated in Osiris as well.

[4] This is at the partner institution's request to ensure that they provide this information. Tilburg University has copies of all its (international and national) students' identity documents at its disposal on the basis of a legal obligation under the HERA. Before providing information to the other university, the student must give explicit Consent for disclosing the information.

Updating Personal Data	Students are informed twice a year by the Student Administration with an e-mail from Osiris to check their Personal Data in *Studielink* and make corrections where necessary.

4.3. Transfer of Personal Data of Applicants or Enrolled Students

The Schools have access to the student data in Osiris and can generate application overviews from this system. The details of the students who have applied are provided to affiliated institutions such as the Top Week Foundation (for the purpose of the introduction), study associations, and student associations. The Sports Centre (part of Tilburg University) also receives this information.
Tilburg University also helps international students by providing contact details to the municipal health service (GGD) for the purpose of a TB check, the IND for the purpose of the visa application, the municipality for the purpose of registration, and housing agencies for finding accommodation.

Right to be informed	Students are informed about the transfer of Personal Data by means of a Privacy Statement on the website and during the application process.
Direct access to Student data by the Schools/Divisions	Employees of Schools and Divisions have access to their Students and the necessary Personal Data in Osiris. This is safeguarded by means of authorization profiles, which ensure that employees only have access to their students and the necessary Personal Data. An audit should be carried out periodically to determine whether employees still have the right profile.
INTERNAL occasional disclosure to School and/or Divisions	In **occasional cases**, Academic Services discloses Personal Data to the School. Please refer to the guidelines for occasional disclosures under the **Privacy & Personal Data Protection Policy—Chapter 12.**
EXTERNAL disclosure contact details to TOP WEEK FOUNDATION STUDY ASSOCIATION STUDENT ASSOCIATION	The transfer of Personal Data of new students concerns contact data and study data and will **only be provided once** on the grounds of the Processing Basis of **legitimate interest** and for the purpose of providing and facilitating education-related activities. There are two options for this (the first being the preferred one) 1. Tilburg University informs the new students about the study associations, student associations, and the Top Week foundation, for the purpose of introduction, with information about how they can register for this (in this way, no Personal Data has to be provided to the third party). 2. Tilburg University provides the student's contact details only once at the start of the study program. Thereafter, these parties will be responsible for the administration of their participants/members. • Do not disclose more Personal Data than strictly necessary. • No Processing Agreement is necessary because these foundations and associations are Controllers themselves. However, contractual agreements must be made about the

	Personal Data they receive and what they may and may not do with it. • Students are informed that we share contact details with the relevant affiliated institutions by means of a Privacy Statement and in application documentation (with the possibility of indicating if they do not wish to do so via so-called opt-out). For more details, we also refer to the **Thematic Policy on External Relations**.
EXTERNAL disclosure to IMMIGRATION AND NATURALISATION SERVICE (IND)	• The transfer to the IND regarding international students is based on the Processing Basis **legal obligation** (Foreign Nationals (Employment) Act) and is, therefore, permitted. • Students are informed that data are shared for the sake of transparency. • There is no need to conclude a Processing Agreement.
EXTERNAL disclosure to GGD	• The transfer of Personal Data of international students to the GGD is done on the basis of the Processing Basis legal obligation for the purpose of the TB inspection. • Students are informed that data will be shared for the sake of transparency. • There is no need to conclude a Processing Agreement.
EXTERNAL disclosure to MUNICIPALITY	• The transfer of Personal Data of international students to the municipality is done on the basis of the Processing Basis of legitimate interest[5]. • Students are informed that data will be shared for the sake of transparency. • There is no need to conclude a Processing Agreement.
EXTERNAL disclosure to HOUSING AGENCY	• In a number of cases, Tilburg University (International Office) passes on personal data of international students to housing agencies (as a service). The basis for this is Consent. This consent is given by the student in the MySAS environment. • A Processing Agreement must be concluded with the relevant housing agency.
EXTERNAL disclosure to PARTNER UNIVERSITIES	• In the case of a joint program and other exchange programs, Tilburg University transfers Personal Data to a partner university. The Processing Basis for this is the **performance of a contract**. • Students are informed that data will be shared for the sake of transparency. • A Processing Agreement must be concluded with the relevant partner university[6].
EXTERNAL disclosure to GRANT PROGRAMS (E.G., Erasmus plus)	• Processing basis is the student's **Consent**. • Students should be informed that data are shared for the sake of transparency. • The grant provider is the Controller. There is no need to conclude a Processing Agreement, but the license/core

[5] It is a legally required for international students to be registered with the municipality (condition for their visa) and to be issued with a BSN. In order to streamline this process and reduce the risks for international students, Tilburg University passes these data on to the municipality.
[6] If it is an occasional exchange concerning an individual student, this obligation does not apply. However, Consent must be obtained from the student, and the transfer of Personal Data must take place safely.

	agreement must contain due diligence agreements (such as use, security, etc.).
Security	When disclosing Personal Data to third parties, it is important that this is done **securely**. See **Chapter 9 of the Privacy & Personal Data Protection Policy** for more information.

4.4. Communication with Applicants or Enrolled Students

During the application and enrollment period, we request information from the student for the purpose of enrollment. Please refer to **Section 4.3** for more information.

During the application and enrollment period, we communicate with the student about, for example, information regarding activities and services. The basic rule when communicating to students is that communication must be necessary and you must ask yourself whether communication is not possible by means of a less intrusive method. If it is necessary for you to know that the student receives the information, then an e-mail is justified. If this is not necessary, communication should be carried out in a less intrusive manner (e.g., via information boards or Canvas). Communication about changed opening hours of the library, for example, should not be sent by e-mail. Please refer to the **Thematic Policy on External Relations**.

Students also report to the Student Desk for questions or by telephone or e-mail. In that case it is important that the employee in question, in the case of Personal Data, establishes whether it is the person in question by means of verification.

Identification enrolled students	Students can request information from the Student Desk, for example. It is important that we verify the identity of the student so that we do not disclose the information relating to Personal Data to third parties. This can be done by means of: • Physical identification, for example, by showing a university card (with a photo) or passport so that the identity can be established. • Telephone/e-mail: determine the identity through verification questions or a masked/marked version of a copy of the ID.
Change of bank account number	Changing bank account numbers is risky (fraud) and, therefore, extra measures have been implemented to ensure that this is done carefully. • The students must identify himself the way it was mentioned above. After identification, the copy of the identity document must be removed. • The student provides a copy of his bankcard with the details of his new bank account. This copy will be archived in connection with the audit trail (proof of modification). **Please note**: if the bank account belongs to another person (authorized by the student), a marked/masked copy of the identity document of this third party, and a copy of his bankcard must also be provided. The copy of the identity document must be removed after processing.

4.5. Storage Period

The basic rule for the storage of Personal Data is that they may **not be kept for longer than is necessary or required by law**.

If a prospective student has not met all the admission requirements at the end of the application process, he will not be enrolled and will be given the Inactive status. In case an enrolled student terminates his studies prematurely, the Inactive status will also be given. The storage periods for this are as follows:

Storage period	The storage period is **no longer than necessary or required by law**. The storage period is laid down in the **Selection list Universities and University Medical Centers 2020** (S*electielijst Universiteiten en Universitair Medische Centra 2020*, a guideline for storage periods of student data, only available in Dutch). The most important retention periods and a reference to this document are included in Appendix 3.
Erasure	Erasure of Personal Data must be done securely. See **the Privacy & Personal Data Protection Policy – section 7.2.**

5. Study Progress

If a student is enrolled in a study program, he will go through a number of phases in which Personal Data will also be processed. This chapter describes the most important guidelines.

5.1. Participating in Education

For the logistics and content support of Education, relevant student data is shared with various internal parties, such as the Schools. A number of examples of this are Personal Data for scheduling and seminars, lecturers about students participating in their courses, and Departmental secretary's offices for collecting and signing for receipt of papers and work assignments. Partly, this information is provided automatically, and, partly, this data transfer takes place on request.

Lecturers may only receive the necessary Personal Data from their students.

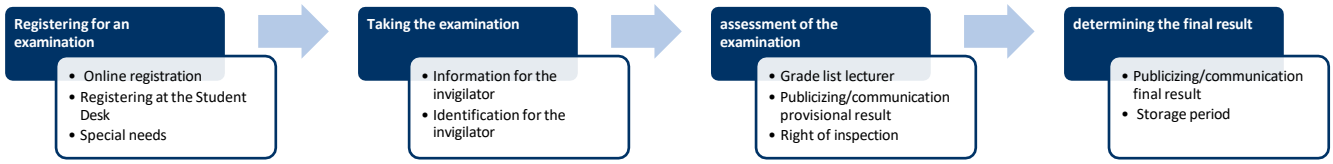
Information lecturers	Lecturers only receive a student number and the student's name and Tilburg University e-mail address.

For the following subjects we refer to **PART II—life cycle education**:

- Scheduling of lectures (composition of tutorials groups) (**Section 7.1**)
- Learning analytics (**Section 8.1**)
- Video lectures (**Section 7.4**)

5.2. Examinations

Before a student is actually credited with an examination result in his study progress overview, a number of stages are followed, in which the overview below also indicates the points for attention regarding the Processing of Personal Data:



5.2.1. Processing Basis

During this process, the students' Personal Data is processed a number of times. In principle, the Processing of this data stems from the Higher Education and Research Act (HERA). After all, in this Act, it is stipulated that Tilburg University must award a degree to students who have successfully completed the examination of one of the study programs offered. In order to determine this, the assessments of the examinations the student has taken must be attributed to him and must be recorded in some way.

Processing basis examination	The Processing Basis for examinations is **necessary in order to comply with a legal obligation** in connection with the awarding of the degree. Tilburg University processes the student number and name of the student in connection with the examination in order to avoid personal confusion and errors in the mere handling of the student number.
Purpose limitation	Determining whether a diploma or certificate can be awarded.

5.2.2. Registering for an examination

A student can register for an examination via the online exam registration system or via the Students Desk.

Personal Data online registration	The student logs in with his username and password (Single Sign On). The following Personal Data are registered: • Student number • Name
Personal Data registration at Student Desk	When registering at the Student Desk, the student must identify himself with his Tilburg University card with a passport photo or an identity document. The following personal data will be registered:

	• Student number • Name
Regular examination scheduling	The examination-scheduling unit then schedules the Student for the examination in question. The student is automatically assigned a place by the system (so-called seating). The schedulers see the student number and name of the student.
Examination scheduling for students with special needs	For Students with Special Needs, the examination-scheduling unit only receives the facilities that the student needs and **never** the reasons for this.

5.2.3. Taking an examination

At the time of the examination, the student reports to the examination location, identifies himself to the invigilators, and takes the examination.

Identification with the invigilator	A student identifies himself with the invigilator by means of a valid identity document (for more details see **Rules and Guidelines of the Examination Boards**). The invigilator will check this using the information on the attendance list.
Digital assessments	The student logs in to the relevant workstation to take a digital assessment and thus gains access to the examination intended for him in the digital assessment environment.
Attendance lists	The invigilators have an attendance list on which the students are listed: Student number, name, and date of birth for checking the identification. The attendance list goes to the lecturer and an unsigned copy to the Student Administration. The Student Administration and lecturers keep this attendance list for a maximum of 1 year.
Examination package	The examination package is not personal. The Student will indicate his name and student number. The Students with Special Needs are given an individual cover page. It only states to which provision they are entitled.

5.2.4. Assessment of the examination

The examination is then assessed by the examiner, after which a provisional result is generally announced. In view of the nature of this information (i.e., an indicator of the student's competence in a certain area), this is a Sensitive Personal Data and must be handled very carefully. After this, the student is entitled to inspect his work, in which case he has the opportunity to ask questions with regard to how it was assessed.

Assessment by the lecturer	The lecturer assesses the examinations, which include the student number and the student's name[7].
Publicizing/communication of the provisional result	• Provisional examination results may **never** be published publicly via a digital notice board, Canvas, etc. because of their sensitive nature. • The Pseudonymization of the results (i.e., only stating the student number and the result) is not sufficient, as this student number can easily be traced back to a specific person. • The (provisional) examination results may therefore be published so that it is only visible for the student in question.

5.2.5. Determining the final result

Ultimately, the final results is determined and recorded in the study progress system (Osiris)

Determining the final result	The lecturer records the final study result on a list that contains the student number and name[8]. This list is sent to the Student Administration for Processing into the study progress system (Osiris) and (digitally) archives the grad lists. In exceptional cases (e.g., oral and individual examinations), examination results are provided to the Student Administration by means of an exam slip. The lecturer gives the student a copy of this exam slip. The Student Administration processes this in Osiris.
Communicating the final examination result	• Final examination results may **only be communicated to the Student personally** on the basis of Osiris and may never be published in public. • Examination results are visible for students in an application for which he personally logs in.
Audio recording oral examinations	Oral examinations can be recorded (see **Rules and Guidelines of the Examination Boards**). • Storage and archiving of these audio recordings must be done securely (centrally at a Department) and only be accessible to lecturers and Departmental secretary's offices. • The storage period is equal to written examinations.

5.2.6. Access

The HERA stipulates that the Education and Examination Regulations must lay down the manner in which and the period within which students can gain access to their assessed work. However, on the basis of case law, it has become apparent that the student's answers and any examiner's comments must be regarded as Personal Data within the meaning of Directive 95/46/EC (predecessor of the

[7] In connection with due diligence to avoid errors and confusion of persons when exclusively using the Student number, the name of the student is also processed.
[8] In connection with due diligence to avoid errors and confusion of persons when exclusively using the Student number, the name of the student is also processed.

GDPR)[9]. It is therefore obvious that these data are also Personal Data in the sense of the GDPR. This means, therefore, that as long as the student's work is stored, students can request these answers at any time, regardless of the relevant provisions in the EER.

However, the term “access,” as used at Tilburg University, also includes the possibility for the student to become acquainted with the questions and/or assignments asked or given in the context of a written examination, the standards on the basis of which the assessment was made, and to request clarification from the teacher about the assessment. The EER may, however, specify the period during which or the moment at which the student is entitled to these parts of the inspection.

Inspection examination	In principle, students have the right to inspect examinations on the basis of the EER and have the opportunity to appeal against the results established. Certain periods apply (see EER and the HERA). On the basis of the GDPR, students are also entitled to inspect examinations and receive a copy. The following guidelines apply: • Students have the right to inspect and receive a copy. However, there is **no need to provide a copy of the exam questions or the example answers**, only of the student’s answers. In the case of audio recordings, students are also allowed to view (hear) these recordings. • The student is also allowed to view the notes made by the lecturer for the answers (e.g., feedback). • If a student requests for right of access (GDPR) insight in the examination outside the periods mentioned, this does **not** mean that the student can communicate about the content of the examination with the lecturer or that the results can still be adjusted.

5.2.7. Storage period examinations

Examination results should be stored in connection with objection and appeal procedures and educational accreditation (Accountability). The following guidelines apply.

Storage period examination results	The retention periods for exams are as follows: • Made work: 2 years after taking the exam; • Exam protocol, test key, caesura, test/assignment, evaluation: 7 years after taking the exam;[10] • Graduation work: see section 5.2.8. If a complaint, objection, or appeal procedure is in progress, this term will be extended to a maximum of the end of the appeals procedure.
Erasure examinations	The Department is responsible for the erasure of the examinations.

[9] HvJ EU 20 December 2017, C-434/16, ECLI:EU:C:2017:994 (*Nowak*).
[10] On the basis of § 2.2.4 (process 54) and § 3.4 of the Selection list Universities and University Medical Centers 2020, see Appendix 3.

	Erasure of examination materials must be carried out securely. See **Privacy & Personal Data Protection Policy, Section 7.2**.

5.2.8. Bachelor's and Master's theses

The Bachelor's and Master's programs are concluded with a thesis. This thesis is, in fact, a special examination form. Therefore, the rules as stated in **Section 5.2** apply to this. The thesis does, however, have a number of special characteristics, which are explained below.

Rights regarding research	In the context of theses/papers, it is possible that Personal Data of respondents will be processed. All the rules that apply to this (such as the rights of the respondents) are described in the **Thematic Policy on Scientific Research**[11], unless specifically stated otherwise here.
Personal Data thesis	Insofar as the student does not add other Personal Data himself, the thesis will only contain the following information: • Name Student • Student number • Degree program • Year of graduation • Name Examiner • Name of second assessor
Storage period	The retention period for the Bachelor and Master theses is set at 7 years after the assessment.[12]

A special aspect of the Master's thesis is that it can be published in the Tilburg University library. The procedure is described at the Tilburg University website.[13] For this publication, a number of Personal Data are recorded in the database of the library, i.e., name, student number, study program, and the year of graduation. This is because the thesis is made publicly available online in full text (and can be found, for example, on Google).

Publication Master's thesis in the library	Students must give explicit consent for their thesis to be published in the library (opt-in). If consent is given, the following Personal Data will be processed: • Name Student • Student number • Degree program • Year of graduation • Name examiner • Name of second assessor. Students may, at any time, indicate that their thesis may no longer be stored in the library.

[11] This Thematic Policy is based, among other things, on the Code of Conduct for Using Personal Data in Scientific Education of the Association of Universities in the Netherlands (VSNU).
[12] On the basis of § 2.2.4 (process 59) of the Selection List Universities and University Medical Centers 2020 (process 59), see Appendix 3.
[13] https://www.tilburguniversity.edu/students/studying/university-library/writing-and-information-skills/publishing-theses/

5.2.9. Disclosure of study results

In the case of some grant programs, the grant provider requires access to the study results. It also happens that results are shared with partner universities if a student is here on exchange.

Disclosure of study progress to IND	For students with a visa for the residence purpose "study," Tilburg University annually issues a statement to the IND based on the legal obligation[14] to declare that they have insufficient study progress to keep their residence permit.
Disclosure of study results to THIRD PARTIES—grant organization/partner universities	The general principle is that the Student himself is responsible for disclosing study results to third parties. In principle, Tilburg University does not provide these directly to third parties unless the student has specifically given **Consent**.

5.3. Internships and Study Trips

In some cases, student data are shared with external parties in the context of study trips or internships. The following guidelines apply:

Disclosure of study results to THIRD PARTIES—study trip / internship	The general principle is that the Student himself is responsible for disclosing the information to third parties. In principle, Tilburg University does not provide these directly to third parties unless the student has specifically given **Consent**. If it is an occasional disclosure (individual student with occasional organization), there is no need to conclude a Processing Agreement. If there is more structural (more frequent) cooperation with an organization (e.g. internship agency, travel agency), a Processing Agreement must be concluded.

5.4. Student Counseling

Before, during and after their study period, students can receive counseling from a mentor, program coordinator, dean of students, top-level sports coordinator, student psychologist, student chaplain, and career advisor.

Processing basis and purpose	The Processing Basis for Processing Personal Data regarding student counseling is **legal ground** for some parts of the counseling, such as issuing a Binding Study Advice (BSA). For the other Processing: **based on a study contract**. The purpose of the Processing of these Personal Data is the counseling of Students or providing study advice.

[14] Article 4.43 paragraph 1 of the Aliens Decree in conjunction with Article 4.17 in conjunction with Article 4.20 paragraph 1 under e of the Regulations on Aliens in conjunction with Article 5.5 of the Code of Conduct for International Students in Higher Education.

Special Personal Data	In principle, the law prohibits Processing of Special Personal Data. Exceptions for Student counseling are: • Student psychologist: exception based on medical legislation. • Other: exception with regard to medical data and the Processing with regard to counseling of Special Needs students, or to take the necessary measures that are applicable because of their health situation. Explicit Consent must be given for this by the Student for the Processing of Special Personal Data (Informed Consent).
Personal Data registering	Students register online or via the Student Desk for counseling and only provide the necessary information: Student number, name, and e-mail address/telephone number.
Citizen Service Number	Deans of students also receive the Student's Citizen Service Number when it comes to the procedure of financial compensation via DUO. The dean of students only signs and stamps the form and sends it to DUO. There is a copy with the BSN in the archive.

During the counseling contacts (face to face, by e-mail, or by telephone), the student may provide Special or Sensitive Personal Data. (See **Privacy & Personal Data Protection Policy, Section 4.3**).

Processing Personal Data during counseling	The counselor Processes Personal Data during the counseling and records this in the counseling file: • Only necessary Personal data will be recorded (data minimization). • Special Personal Data may be Processed if it is necessary for the counseling and the student gives his specific Consent. • Sensitive Personal Data (such as, bank account numbers) may be processed if necessary. • Accompanying documents must only be accessible to the counselor and colleagues with the same function. An exception are Student Psychologists, who work in accordance with the law, BIG and NIP codes. • Accompanying documents (digital and/or paper) must be kept securely (see **Chapter 9 of the Privacy & Personal Data Protection Policy**). **Please note**: the chaplain does not record notes in a counseling file.
Storage period counseling files	For student psychologists there is a retention period for supervision files of 20 years after the last change in the file.[15] For guidance files of the welfare team (student deans and top sports coordinator) a retention period of 10 years after the deregistration of the student applies in connection with the possibility of diploma extension.[16]

[15] On the basis of article 454 paragraph 3 Book 7 of the Dutch Civil Code.
[16] On the basis of article 5.16 of the Student Finance Act.

	For the other guidance files (e.g. of educational coordinators, career advisors, etc.) a retention period of 2 years after deregistration of the student applies.[17]

(Special) Personal Data can be exchanged, both occasionally and structurally, between the various (internal) disciplines and with relevant external parties with the express Consent of the student. This is done with as little information as possible and only to the extent that it is necessary for the purpose.

Exchange Personal Data between internal disciplines	Exchange (written or oral) with other internal disciplines: • Only if necessary for the counseling of the Student and/or the provision of Student Advice, **or** • only with the explicit (written) Consent of the Student.
Exchange Personal Data between external organizations	Exchange (written or oral) with other external organizations: • Deans of students exchange information with DUO and process the Citizen Service Number in this process. • Other exchanges of Personal Data: Only if necessary for the counseling of the Student, **and** ○ only with the explicit (written) Consent of the Student. **EXCEPTION**: Only in the event of a (medical) emergency may the information be provided within the framework of the processing basis of **vital importance**.
Right of access	For the main rule on the right of access, we refer to the **Privacy & Personal Data Protection Policy, Chapter 10**. Students have the right to access the Personal Data recorded about them in their Student File, with the **exception** of **internal notes that contain the personal thoughts of the staff members and that are exclusively intended for internal consultation and deliberation**. As soon as internal notes are further disclosed, these notes will no longer fall under this exception and the right of access will apply. The internal notes covered by this exception should only be accessible to those colleagues with whom internal consultation must take place.

In some situations, external counselors are used, like, for example, coaches.

External counselors	It concerns internal management and thus there is no Controller-Processor relationship. A self-employed person should be regarded as an employee, so there is no need to conclude a Processing Agreement.

[17] On the basis of § 2.2.4 (process 57) of the Selection List Universities and University Medical Centers 2020, see Appendix 3.

	Example: instruction in which the procedure is also given to self-employed personnel as to how to do it.
External counselors—Self-employed person whose primary task is to process Personal Data but who is not instructed	If Tilburg University instructs a self-employed person to Process Personal Data but does not provide the instruction how to do so (e.g., coach for students) then the relevant self-employed person is a Processor. In this case, a Processing Agreement must be concluded. See for more detail **Privacy & Personal Data Protection Policy, Section 11.4.**
External counselors—Self-employed person whose primary task is not to process Personal Data and who is not instructed	The primary assignment is not the Processing of Personal Data: and the self-employed person himself is the Controller—No Processing Agreement is necessary, but, with regard to due care, contractual agreements in the assignment are required. See for more detail **Privacy & Personal Data Protection Policy, Section 11.4.**

5.4.1. Central Disputes and Complaints Desk

Students can submit a complaint, objection, or appeal to the Central Disputes and Complaints Desk. These complaints are not anonymous and are forwarded by the complaints manager to the person who has to deal with them. Anonymity is not possible because the principle of hearing both sides of the argument must be applied. The following guidelines apply to the handling of complaints, objections, and appeals.

Processing basis and purpose	The Processing Basis for Processing Personal Data relating to complaints is a **legal ground based on the HERA**. The purpose of the Processing of this Personal Data is to handle complaints and disputes.
Personal Data registration	Students can register online with a complaint, objection, or appeal providing only the necessary information: Student number, name, and e-mail address/telephone number, education and faculty, start of education, de event for which they want to issue a complaint / objection or appeal and the grounds. In case of off line submission they should provide a signature.
Referral	The complaints officer will refer the complaint to the relevant internal unit for handling. Only the necessary Personal Data will be mentioned. An objection or appeal will be transferred completely.
Processing personal data during the handling of a complaint	The complaints officer Processes Personal Data during the handling of the complaint, objection, or appeal and records this data in the file: • Only necessary Personal Data will be recorded (data minimization). • Special Personal Data may be Processed if it is necessary for the handling of the complaint and the student specifically gives his Consent. • The complaint file must only be accessible to the counselor and colleagues with the same position.

	• Complaint files (digital and/or paper) must be kept securely (see **Chapter 9 of the Privacy & Personal Data Protection Policy**).

5.5. Issuing a Diploma

Issuing diplomas within the framework of the Bachelor's program is currently done administratively within Tilburg University. As soon as the diploma administration establishes that the student has met all the conditions for a diploma, the diploma documents are produced. These documents also contain, in part, Sensitive Personal Data, such as results and distinctions. Diplomas are awarded at the student's request during the graduation ceremony organized by the Education Support Team (EST).

Bachelor's diplomas	The Bachelor's diplomas contain Personal Data as well as Sensitive Personal Data and therefore the following guidelines apply: • Only accessible to necessary employees (Student Desk, Student Administration, and Education Support Teams employees). • Store and deliver to EST for diploma award ceremony and must be well secured. • Unissued diplomas are stored at the Student Desk (adequately secured).

Diplomas in Master's programs are generally awarded on an individual basis: the student submits an application to the Student Desk. If the Follow-up Administration establishes that the student meets the requirements for certification, the documents will be produced (some of which are extra sensitive information) and sent to the Examination Board (Please note: this is the examination board that makes the assessment regarding the specific student).

Master's diplomas	The Master's diplomas contain Personal Data as well as Sensitive Personal Data and, therefore, the following guidelines apply: • Only accessible to necessary employees (Student Desk, Student Administration, and Education Support Teams employees). • Store and deliver to Examination Board for diploma award ceremony and must be well secured.

5.5.1. Diploma verification

It happens regularly that applications are received to verify diplomas from Tilburg University. The guidelines for this are set out below:

Disclosure of information to external parties for diploma verification	For privacy reasons, Tilburg University never discloses information about (former) students to other persons or organizations without a signed authorization from the student in question.

	A request for verification of a diploma will, therefore, only be taken into consideration if a written statement is also attached in which the alumnus concerned gives his Consent. In that case, the degree obtained and the date on which it was obtained will be provided. Please note: The signature on the consent form must be verified with a copy of the ID (marked and masked). (**Privacy & Personal Data Protection Policy, Section 4.4.2**)

5.6. Student Disenrollment

A student can disenroll during a program or after successfully completing a program via *Studielink*. *Studielink* still exchanges data with Osiris until the student's account has been deleted (no active enrollment anymore) or until the Student Administration disconnects the relationship via the annual clean-up.

Storage period disenrolled students	See the **Osiris archiving protocol**, which formalizes the storage periods of Personal Data in Osiris. For the other student data, see the **guideline on storage periods for student data**[18].
INTERNAL disclosure of information to DARO	DARO structurally receives the following information from Students: Student number, contact details, and study program details.

5.7. Alumni

The management of alumni is described in the **Thematic Policy on External Relations**.

[18] See Appendix 3 for more information.

Part II: Education

This part elaborates on the guidelines for processing Personal Data derived from the GDPR on the basis of the life cycle of education. This part of the Policy focuses on the use of the student's Personal Data.
This cycle contains the following phases:

The Tilburg Education Profile (TEP) assumes that students at the university develop their Knowledge, Skills, and Character. A student attends courses to this end. Attending education is part of the agreement concluded between the student and the university: the student pays tuition fees and the university provides education in return and insight into the student's progress.

6. Developing Education and Education Policy

Before a student can attend courses at the university, the courses must be developed. This development starts with the establishment of clear frameworks and policy for education. This is done both at an institutional level and at the level of the Schools. To develop policy for education and courses, education data is used. Education data is all the different information that can be used to improve the quality, effectiveness and efficiency of education.
We use this education data for:
- Management information: general information and descriptive statistics that are necessary for university or faculty management, quality assurance, and accountability (to, for example, UNL, OCW, and accreditation committees). For example: dropout rates or study efficiencies.
- Student Analytics: data from various administrative sources to analyze student intake, progress, and outflow. For example: linking student success rates to the educational background in order to ensure alignment with different pre-college programs.
- Learning Analytics: data about students and their learning environment, with a view to understanding and optimizing learning and the learning environment. For example: understanding the use and viewing of video lectures to better understand the optimal amount and format for video lectures in education.
Analyzing education data contributes to impartial and inclusive participation in education by providing information and insights that contribute to the quality of education and educational support.

A list of processing operations that occur on a regular basis is included in the privacy statement on the website.

Education data are analyzed in such a way that:

1. it never acts contrary to the GDPR and the rights and interests of students are always paramount and respected;
2. when using education data, a balance is always made between advantages and disadvantages; and
3. there is never a disproportionate intrusion regarding the privacy of students.

Processing basis and purpose	• The Processing Basis for the use of Personal Data for the development of education is **legitimate interest**[19]. • The purpose of the Processing of Personal Data is management information, educational development and improvement. • In the exceptional case health related data (which are Special Personal Data) are used, this will be reviewed by the Privacy Officer Academic Services prior to the processing of the health related Special Personal Data. This will include a check on whether there is a legal processing basis and whether the processing of this data is necessary with regard to the specified purpose. Other Special Personal Data are not processed for developing education and education policy.

Access to Personal Data	• The Personal data for the analyses come from source systems and surveys. • The Personal Data will be Anonymized or Pseudonymized as early as possible. • In most cases the data is presented on an aggregate level and not traceable to individuals. • In exceptional cases the data might identify an individual. Access to that data is restricted. **Please note**: if this information is aggregated by an external party, a Processing Agreement must be drawn up (see **Privacy & Personal Data Protection Policy, Section 11.3**).

The use of education data as research data in the development of education (e.g., the use of scientific research in an educational environment or the provision of scientific research to students) is subject to the rules laid down in the **Thematic Policy on Scientific Research**.

[19] Student and Learning Analytics offers evidence-based, action-oriented insights for the improvement of intake, progression, outflow, and success on the labor market of students in Tilburg University's Bachelor's, pre-Master's and Master's programs. The university's interest is to prevent study delays, unnecessary dropouts, and wrong study choices; to make well-founded policy choices; and contribute as much as possible to Tilburg University's strategic objectives.

7. Provision of Education

7.1. Composition of Tutorial Groups (student scheduling)

When scheduling the lectures (per semester), the schedulers process the student number, the name, and the availability of the lecturer. For lectures, in order to assign the rooms to a particular course, they will make estimates of the expected group size in advance.
The tutorial groups are not composed by the schedulers but by the Education Support Teams within the School. Non-first-year students register in the available tutorial groups themselves.

Processing basis	Processing basis for scheduling lectures is **compliance with a contract** in connection with attending courses.
	Tilburg University processes the student number and name of the student in connection with due care in order to avoid personal confusion and errors in the mere handling of the student number.
Purpose limitation	the organization and provision of education
Personal Data	Only the following Personal Data may be processed for the purpose of scheduling: • Student number (ANR) • Student name • Name of lecturer Measures are adopted for any necessary steps (facilities) for students with medical problems and these are communicated to the schedulers. The medical data will never be shared[20].

7.2. Use of Case Studies, Examples, and Research Data in Education

Education uses case studies, legal judgments, examples and research data in which Personal Data can be involved. As with the development of education, it also applies to the provision of education that, as far as possible, reference should be made to other sources of information so the university does not actually record and process the Personal Data itself. When it is still necessary to include data in education, for example in PowerPoints, examinations, or material published within an LMS, this must be anonymized beforehand. This is also the case when using the data of the student population present. The data used may not be traceable to the various individual students. If the data can be traced back to the various students, for example, if there is a small group, this is only possible if the individual student has given his explicit prior written Consent.

[20] In exceptional cases, students themselves report to a scheduler with (temporary) medical problems and request that this be taken into account when scheduling. In this case, the student gives his implicit Consent. It is also possible for lecturers to request the schedulers for specific rooms in connection with facilities. In this case, the lecturer gives Consent.

Use Personal Data in case studies	The basic rule is that when using case studies, Personal Data may never be processed/used or traced back to individual Persons. The information must be completely Anonymized. Only if the Data Subject has given his explicit written consent may identifiable Personal Data be used. *Examples* • *If the case study arises from a public source, and this person has consciously made it public, the Personal Data may be used* • *News items are allowed to be used.* • *For a study program, video recordings of Respondents in a scientific study are used. This is only permitted if the Respondent has given specific consent for this. See **Thematic Policy on Scientific Research**.* • *For statistics, the aim is to use up-to-date data from students (e.g., student analytics). This is not permitted unless specific consent has been obtained from the students concerned.*
	Please note: if Personal Data is aggregated, the size of a "group" may mean that the data can still be traced back to an individual person. This is not permitted.

7.3. Student Lists, Attendance Registration, Registration of Assignment Components

When lecturers make use of student lists, attendance registration, or assignment components during a study program, data minimization must be used. Only those data that are **necessary** for the provision of the education can be registered on the basis of the Processing Basis **legitimate interest**, meaning name and student number. For this, it expressly applies that the recording and storage of Sensitive or Special Personal Data is excluded.

Student lists and attendance registration	• The processing basis is the **legitimate interest** for the purposes of providing education (purpose). • Lecturers may only dispose of the student number and name of a student (both details are necessary to prevent errors) and no additional Personal Data.
Special Personal Data	Lecturers **never** register a student's Special Personal Data.

If student details are recorded within the framework of conditional criteria (conditional for passing the examination), the same rules are followed as for the registration of examination results.

7.4. Audio and Video Recordings within the Framework of Carrying out Education

Tilburg University offers video lectures as a service in a number of cases. Because people are filmed here, we are dealing with Personal Data to which this Policy applies.
When recording a video lecture, students are prevented from being portrayed as much as possible. In 90% of cases, the students are filmed from behind and are not recognizable. However, there are

situations in which it is impossible to prevent students from being portrayed in a recognizable manner. For example, many lecturers value interaction with the audience and they want to see this reflected in the video lecture. Sometimes a lecturer brings a student forward during the course of the lecture and then portraying the student is unavoidable. Even if a lecturer walks into the lecture room and the camera follows him, it is unavoidable that students will be in the picture in a recognizable way.

The following guidelines apply to making video and audio recordings of lectures.

Processing basis VIDEO lectures	Processing basis of **legitimate interest** for carrying out educational (purpose) as a service to the student.
Information to STUDENTS/video lectures	Students are informed in advance about video recordings: • in the general policy that lectures can be recorded; • in the privacy statement, it is stated that video lectures can take place; • at the start of the lecture by the lecturer.

Assignment by a Lecturer	Video lectures may only be performed on the instruction of or with the permission of a lecturer.
Recording - **By LIS AV using mediasite** - **By lecturer himself using mymediasite**	• During recording, students are prevented from being recorded as much as possible. However, this cannot be completely prevented, for example, because a lecturer brings a student forward or because there is interaction with the audience. • Recordings are made from the back of the room so that students are filmed from behind in order to prevent the risk of recognition as much as possible. Video recordings are edited, in which breaks (in which students are often recognizably portrayed) are removed.
Publicizing video lectures	• After editing, video lectures will be made available to the lecturer. • The lecturer decides to publish in Canvas[21].
Objection student or lecturer	If a student objects to the video recordings, they must be modified, for example by • removing the part in which the student is in the picture (editing) • removing the video lecture • Blurring the face of the student if technically possible
Storage period video lecture	For the storage period of video lectures, we refer to the **supplementary policy Footage**[22].

The system includes extensive analytics for which the following guidelines apply.

[21] Student must log in to gain access to Canvas.
[22] Expected in the spring of 2021.

Analytics video lectures	Student analytics on video lectures will be anonymized as much as possible. Personal data **may only** be used for checking **attendance**. In that case, the lecturer may only see the student's student number and name. Students are informed about this in advance, for example by providing information when logging in to the system. Student analytics for video lectures should **never** include: • other Personal Data of the student; • duration of the student watching the video lecture; • IP addresses and providers.

For the making of recordings during lectures by students, please refer to the **House Rules of Tilburg University**[23] and **Studenten Charter.**[24]

7.5. Logging in to Systems in the Context of Providing Education

Students need to use different systems in order to be able to take part in the education. Think of the use of an LMS, the use of possible (management) games, digital tools in the lecture hall, et cetera. When students are asked to make use of this as part of the course, a Processing Agreement must be concluded with the companies that offer these tools.

Tilburg University advises or requires a product for which logging in is required or if Personal Data are processed in any other way	The Processing Basis is **performing the contract** and with the purpose of providing and facilitating educational activities. 1. Do not process more Personal Data than strictly necessary. 2. A Processing Agreement is necessary. In addition, contractual agreements must be made about the Personal Data they receive and what they may and may not do with it. (**Privacy & Personal Data Protection Policy Section 11.4**). That is why Tilburg University uses the following principles for log-in applications: • Use link with Tilburg University e-mail address and password and NO social login (in connection with Tracking). • If linking with Tilburg University e-mail address is not possible, use Tilburg University e-mail address with ANOTHER password (application-specific).

[23] https://www.tilburguniversity.edu/about/tilburg-university/conduct-integrity/house-rules/
[24] https://www.tilburguniversity.edu/students/studying/regulations/charter/

8. Evaluating Education

8.1. Evaluation Education Based on Student Evaluations

After the education has been carried out, the education is evaluated with the aid of student evaluations. This takes place in a different way and with the help of a different system in the various Schools. To this end, students are asked to complete a questionnaire, either digitally or on paper. When these questionnaires are completed in paper form, these data are then digitized. If Personal Data are filled out on paper in the questionnaires, they will be erased after Processing. The use of the data for educational evaluations is subject to Anonymization and may no longer be traced back to individual students.

Processing basis and purpose	Processing Basis for inviting participation in the evaluation is **legitimate interest**. Participation is based on **Consent** for the purpose of educational development and quality assurance.
Evaluation forms	• In digital evaluations, students log in to the questionnaire. • The response is only systemically linked to the student number (ANR) and therefore not visible.

Processing Personal Data for the purpose of evaluations	• The evaluation forms should never contain Student Data. Nevertheless, they may be traced back to individuals. This can happen, for example, in the case of small group sizes or with personal explanations (which can be traced back by the lecturer). • Special Personal data may never be processed. • Only the employee who makes the management report on the basis of the evaluations has access to the evaluation forms and thus to Personal Data. • The management information must be at an aggregated level and it must be guaranteed that Personal Data can be traced back as little as possible to individual persons (preferably Anonymized). If Processing is carried out by a third, external party, a Processing Agreement must be concluded. (**Privacy & Personal Data Protection Policy Section 11.4)**

8.2. Evaluation Education Based on Learning Analytics

In addition to student evaluations, learning analytics are used to evaluate education. This involves looking at the effectiveness of education at a higher level of aggregation. As with previous comments on learning analytics, it is important to ensure that only those who fill and maintain the system have access to the actual data at a personal level. Processing that takes place afterwards is based on anonymous, pseudonymous and/or aggregated data. In exceptional cases the data might identify an individual and access to that data is restricted. For guidelines, please refer to **Section 6**.

8.3. (External) Market Research Students

See **Thematic Policy on External Relations**

8.4. Evaluation of Lecturers

Results from student evaluations and learning analytics are recorded in reports. These reports form the basis for the further improvement of education but are also used as management information with regard to the functioning of lecturers. For more details, we also refer to the **Thematic Policy on Personnel**.

It also happens that lectures are included for assessing the quality of lecturers within the framework of the University Teaching Qualification (UTQ). The following guidelines apply

Processing Basis quality assessment Lecturer	The Processing Basis is a **statutory task** for the assessment of the quality of the lecturer in the context of the University Teaching Qualification.
Information for STUDENTS	Lecturers **inform** students **prior to the lecture** that the lecture will be recorded. This can be done during an earlier lecture, by publication on Canvas, or at the start of the lecture.
Consent of the Lecturer	Recordings for assessment purposes may only be made **on the instructions of or with the permission** of the instructor.

Recording - **By LIS AV using mediasite** - **By lecturer himself using mymediasite**	• During recording, students are prevented from being recorded as much as possible. However, this cannot be completely prevented, for example, because a lecturer brings a student forward or because there is interaction with the audience. • Recordings are made from the back of the room so that students are filmed from behind in order to prevent the risk of recognition as much as possible.
Access to video recordings	Recordings are only accessible to the assessor, the lecturer, and his supervisor.
Storage period	Video recordings are erased after the evaluation is completed.

9. Improving Education

Education data are also used for the improvement of education at this level. This is subject to the same rules as for policy-making and education development (see **Section 6**).

10. Accreditation Education

The university and within it the various Schools and programs have a legal obligation to provide data within the framework of accreditation. This includes a precise description of the type of information involved, such as making theses available for inspection and providing information about the panels. In addition, for the preparation of the accreditation, overviews are made using Personal Data of

students and lecturers to ensure that the organization of the site visit runs smoothly.

External Disclosure to NVAO and international accreditation institutions (EAPAA and AACSB)	The transfer to the accreditation body within the framework of (re)accreditation is based on the Processing Basis **legal obligation** and is therefore permitted. There is no need to conclude a Processing Agreement.
External Parties who help with the preparation	If cooperation takes place with an external party (Visiting and Reviewing Authority) that assists with the preparation for a site visit and/or accreditation, a Processing Agreement must be concluded with this party. See also **Privacy & Data Protection Policy section 11.4**.
Internal recording in connection with the preparation of the accreditation	The internal registration of student data and lecturer data in the context of the preparation and organization of a site visit is based on the Processing Basis of **legitimate interest**. This recording of data is for internal use only.

Appendix 1: Definitions

Concept	Definition	Chapter Principal Policy
Anonymizing/ Anonymous information	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).	6.4
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.	4.3.2
Consent (by 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).	4.2
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.	11.4
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.	13
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.	11.3
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.	11.1

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. This is referred to as Data Protection Impact Assessment in the GDPR.	11.2
Data Subject	An identified or identifiable natural person to whom personal data relates.	
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.	4.5
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.	4.4
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.	3
Personal Records Database	The Personal Records Database is a central database containing Personal Data of the inhabitants of the Netherlands. It also contains data on Dutch people living abroad. The BRP is the successor of the Municipal Database Personal Records.	
Policy	This policy with regard to the Processing of Personal Data at Tilburg University (Privacy & Personal Data Protection Policy).	
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).	4.2

Processor	A natural or legal person, public authority, agency, or other body that processes Personal Data on behalf of the controller.	11.4
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).	11.4
Pseudonymization	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.	6.4
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).	10.4
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).	10.3
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).	10.7

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)	10.5
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).	10.8
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).	10.5
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).	10.6
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.	4.3

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.	
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.	

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); *Example: the disclosure of certain Personal Data of students to Studielink for the purpose of the application and enrollment.*
Necessary for performance 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; *Example: the Processing necessary for the performance of the "study contract" between Tilburg University and the student.*
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); *Example: the awarding of a degree and the issuing of a diploma to a student.*
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. *Example: the disclosure of Personal Data in the event of a medical emergency.*
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. *Example : the use of student analytics to evaluate programs.*
Consent	• The Data Subject must be well (clearly) informed in advance of the Processing for which he gives his Consent. See Chapter 10.2 for more information. • Consent must be actively given. That is to say, no use of a check box already filled out. • 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. *Example: Processing Personal Data for prospective students who have given permission to approach them for university activities. Or Processing of Personal Data by the student psychologist or confidential advisor.*

Appendix 3: Retention periods

Tilburg University complies with the retention periods as defined in the "Selection list Universities and University Medical Centers 2020".

This Selection List describes the defined retention period for information objects containing personal data, as processed in the processes that take place within the universities. These retention periods are elaborated per process in the Selection List and have a legal character.

Broadly speaking, the following substantiations can be distinguished for the retention periods for personal data in the Selection List:

- 1 or 2 years for limited evidentiary interest;

- 2 years after deregistration for data about students in case they re-enroll within a short period of time;

- 5 years in the case of information objects that give grounds for legal claims;

- 7 years for information objects that can be included in the accreditation (based on the six-year course accreditation, with one additional reserve year);

- 7 years for information objects from financial reporting;

- 10 years for information objects with a heavier legal basis, for which the institutions have a custody obligation;

- 50 years for information objects that entitle the graduate to his or her degree or propaedeutic year.

If in the Selection List another term or substantiation than the above is used, this will be explained in the notes to the process in question.

The Selection List can be consulted via this link (only available in Dutch):
https://www.nationaalarchief.nl/archiveren/kennisbank/selectielijst-universiteiten-en-universitair-medische-centra-2020.

Document management				
Version	**date**	**distribution**	**status**	**Changes on main points**
1.0	14-06-2018	intranet	Final	n.a.
1.1	13-01-2021	internet	Final	Retention periods due to BSD, adaptation used applications.
1.2	01-04-2023	internet	Final	Use of identifiable education data and health related data for education development of education and education policy (section 6).