PRIVACY & PERSONAL DATA PROTECTION POLICY
TILBURG UNIVERSITY

Readers' Guide

This Policy describes the manner in which Tilburg University implements the General Data Protection Regulation (GDPR) with regard to the Protection of Personal Data. This Policy contains the main features regarding the Protection of Personal Data. Specific situations apply for certain themes and these specific situations are set out in **paragraph 11.1V**.

For the sake of readability, we have divided this policy into 3 parts:

- Part I - General: the scope of the policy and principles (basic assumption) regarding Personal Data Protection as included in the GDPR.
- Part II - Principles: elaboration of the Principles for Tilburg University in further guidelines.
- Part III - The way in which control and enforcement has been implemented.

All information relating to Personal Data Protection is included on a **website**[1].

Every Tilburg University School/Division has appointed so-called **Data Representatives**[2]. They are the first point of contact for employees if they have questions about Personal Data Protection.

The Policy includes references to other policy documents. These are marked as **references or indicated by a hyperlink**. The applicable guidelines are displayed in blocks to make them easy to find:

Subject	Guideline

This Policy contains many definitions (**Appendix 1**). The words in the definition list are written with a capital letter throughout the document.

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

For a quick overview, check the schemes and schedules on the next pages.

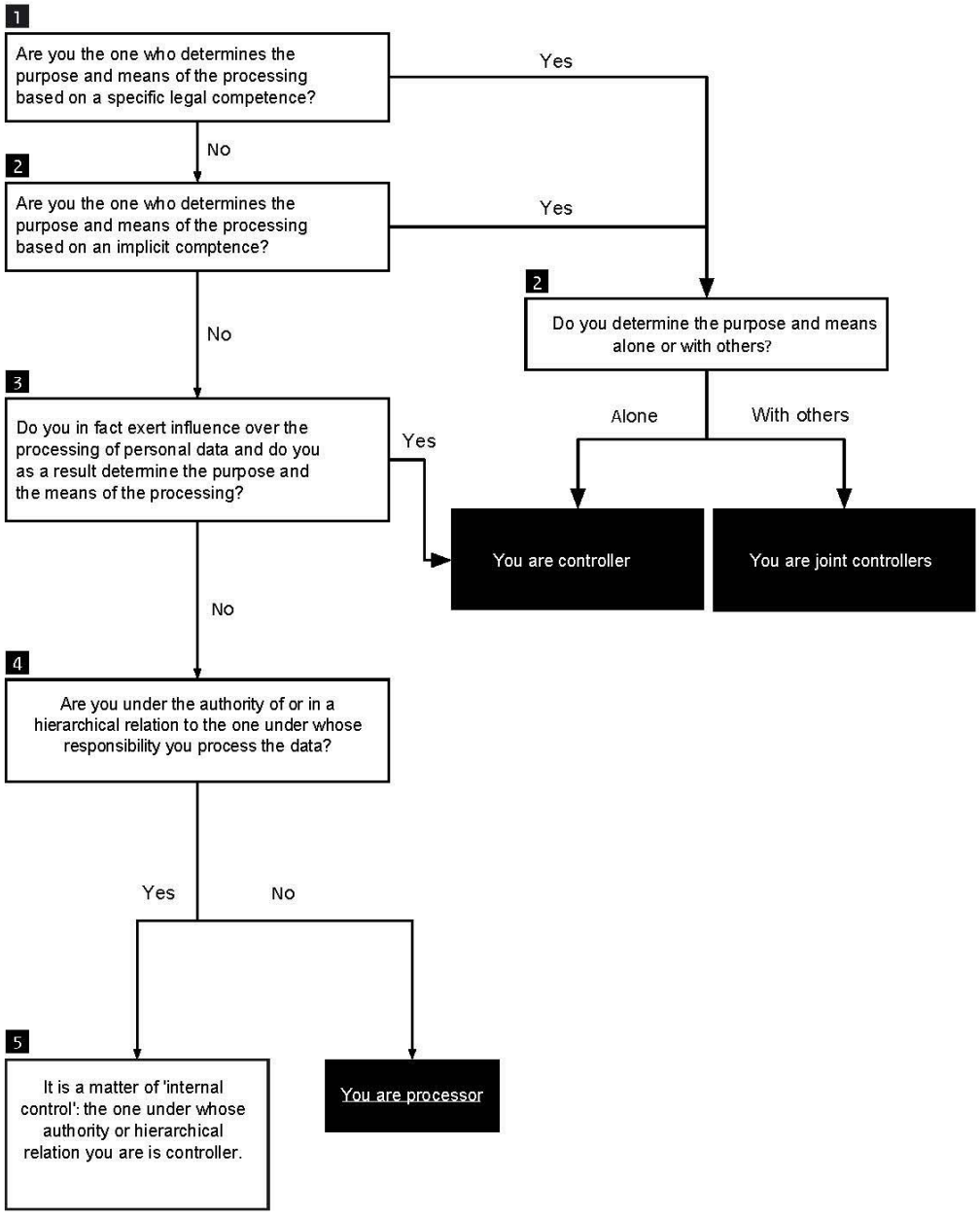
- Outline 1: Are you a controller or processor?
- Outline 2: Is your data processing legitimate?
- Outline 3: When do you have to inform the data subject of a processing of personal data?

This is a translation of the "**Beleid Privacy & Bescherming Persoonsgegevens**" and is translated with the utmost care. Should there however be any inconsistency, the Dutch version of this Policy prevails.

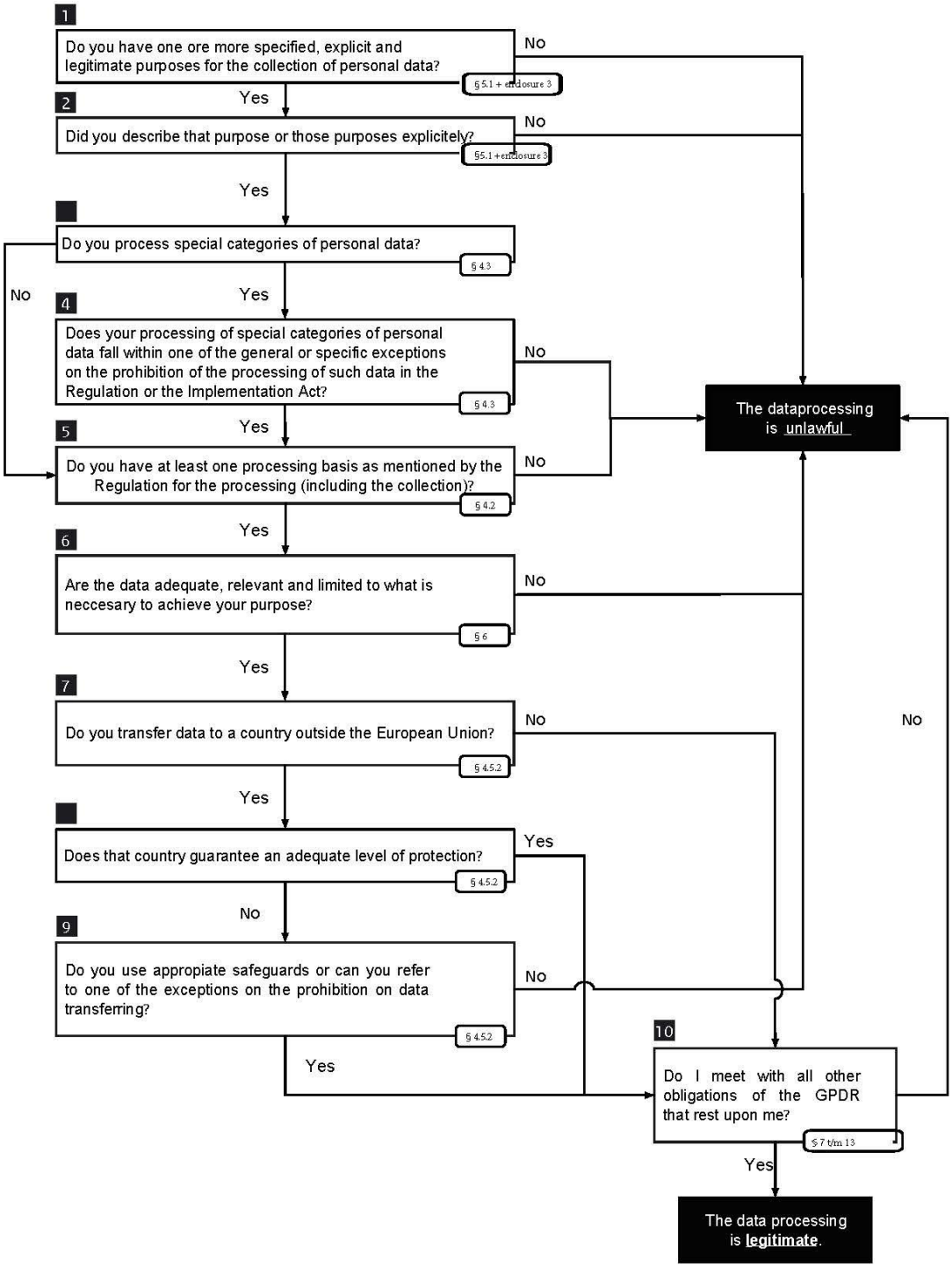
[1] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security
[2] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/careful-handling-personal-data/questions

Outline 1: Are you a controller or processor?

See also paragraph 11.4

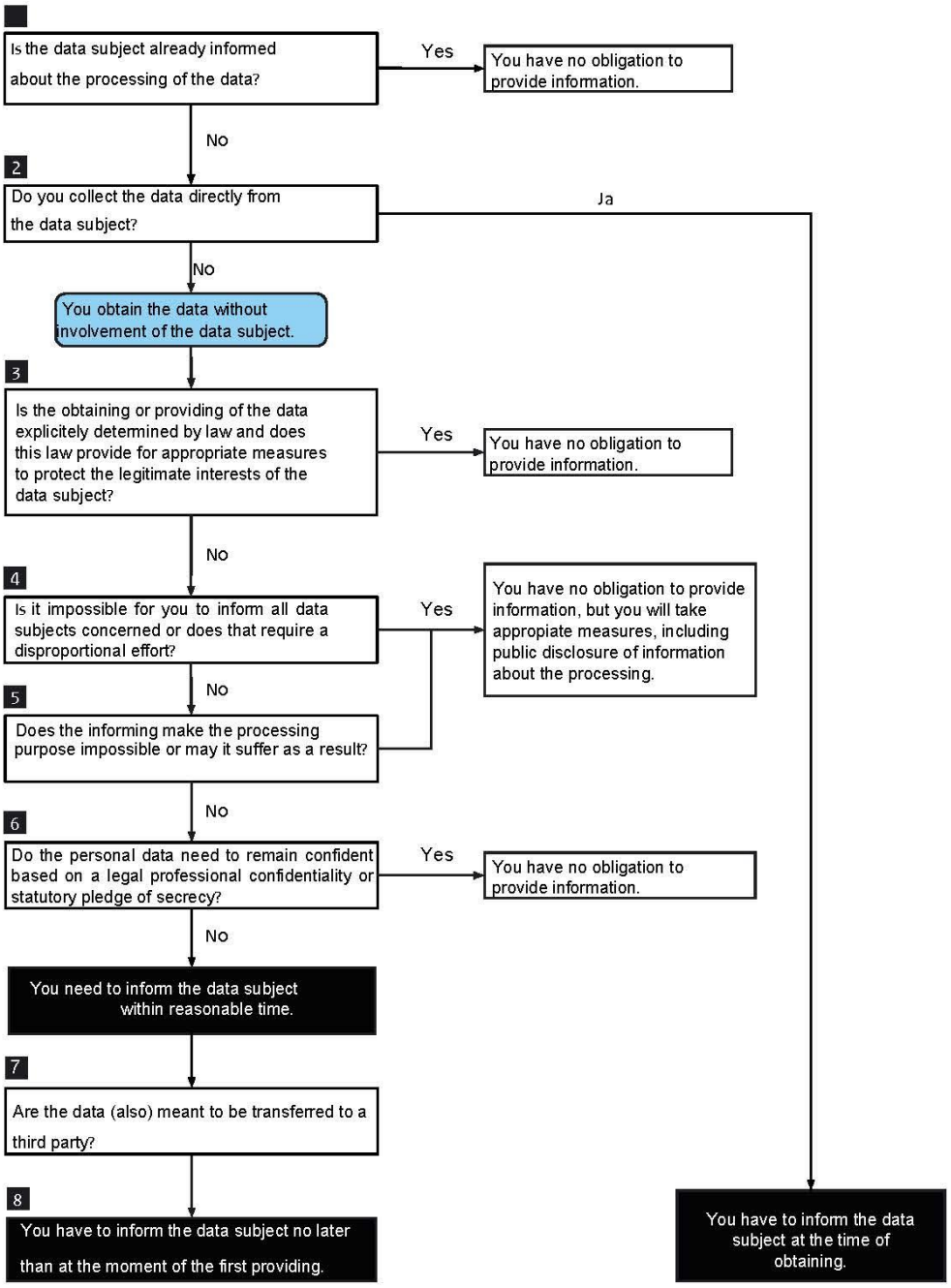


Outline 2: Is your data processing legitimate?



Outline 3: When do you have to inform the data subject of a processing of personal data?

See also paragraph 10.2 and paragraph 10.3



Part I: IN GENERAL

1. Introduction

The processing of Personal Data is necessary for the business processes of institutions of education and research. Tilburg University (TiU) values the careful processing of Personal Data and has drawn up a **Data Protection Strategy**.
This also fits within the strategic plan "**Weaving Minds & Characters**" and the core values described therein. To meet its curiosity (**Curious**), it will be necessary for TiU to process Personal Data. The same goes for staying connected if it is in the interest of the person whose personal data we are processing (**Connected**). In doing so, TiU dares to take the space offered to it by European and national regulations if it is in the interest of the person whose personal data it processes (**Courageous**), but is also aware of its duty to do so with care and to handle with care the trust it has from those whose data it processes (**Caring**). Moreover, in view of that Caring, TiU even has a duty, for example in the context of student welfare, to process personal data.

This document (Privacy & Personal Data Protection Policy)provides a further elaboration of the values formulated in the **Data Protection Strategy**. and what implications the rules set out in the General Data Protection Regulation (GDPR) and the "Uitvoeringswet Algemene Verordening Gegevensbescherming" (UAVG) have for TiU. With this policy document, TiU guarantees the optimization of the quality of the processing of Personal Data and a good balance between privacy, security, and functionality. Abuse of Personal Data can cause serious damage to students, employees, and other Data Subjects, but also to TiU.

The concrete objectives of this Policy are as follows:

1. complying with European and Dutch legislation and regulations;
2. defining the principles for the processing of Personal Data;
3. providing a framework to measure (future) Processing of Personal Data against an adopted best practice or norm;
4. transparency as to what TiU does with Personal Data;
5. determining procedures concerning the processing of Personal Data; and
6. assigning tasks, powers, and responsibilities in the organization.

There is an important link between the Protection of Personal Data, on the one hand, and information management and information security, on the other hand. Information management and security are an important foundation for ensuring the Protection of Personal Data. In this document, therefore, regular reference is also made to the **Information Security Policy**[3] and the **Research Data Management Regulations**[4].

1.1. Legislation and Regulations

[3] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/securing
[4] https://www.tilburguniversity.edu/intranet/research-support-portal/rdm/regulation

The following legislation and regulations are applicable and have been taken into account in formulating this policy, which is based on the text in force on January 1, 2018:

Category	Legislation or Regulations
Legislation	General Data Protection Regulation (GDPR)
	General Data Protection Regulation Implementation Act (UAVG)
	Higher Education and Research Act (WHW)
	Telecommunications Act
Code of Conduct UNL	
	The Netherlands Code of Conduct for Research Integrity[5]
Standards framework	The SURF Framework of Legal Standards for (Cloud) Services[6]
Internal policy	Strategy Data Protection[7]
	Information Security Policy[8]
	Information Provision Protocol
	Research Data Management Regulations[9]

2. Scope of this Policy

This Policy applies to all Processing of Personal Data that take place under the responsibility of Tilburg University and applies to everyone working under the responsibility of Tilburg University.

When TiU holds or receives Personal Data it will often be considered Processing, because Processing has a very broad meaning. Processing is defined in the GDPR as:

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.

The definition above applies to the Processing Operations of Personal Data in a paper document (e.g., in an archive or cupboard), a digital file (e.g., MS Excel) or in a digital system (including in mailboxes and on computers or other data carriers such as USB sticks) and is applicable to personnel, whether or not in salaried employment, including student assistants, temporary employees or hired personnel and interns, external PhD candidates, and students. Therefore, it concerns all the Processing of Personal Data that we carry out

[5] https://www.universiteitenvannederland.nl/en_GB/research-integrity
[6] https://www.surf.nl/en/surf-framework-of-legal-standards-for-cloud-services
[7] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/careful-handling-personal-data/policy
[8] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/securing
[9] https://www.tilburguniversity.edu/intranet/research-support-portal/rdm/regulation

within the framework of our core processes education, scientific research, and impact (valorization) and the management and support processes.

2.1. Owner/Responsibility

This Policy often refers to a process or system manager or process owner. This refers to the person who determines the purpose and means of the process or system: this a position within TiU. In other words, this is the person ultimately responsible (accountable[10]) for this. See Section III for GDPR responsibilities.

The system manager is accountable (ultimately responsible) for the system in question but is often supported by functional managers or information managers who are responsible for these points. Some examples (not exhaustive):

System	System manager
Osiris	Academic Services
Canvas	Academic Services
SAP Success Factors	Human Resources
SAP FICO	Finance & Control
Raisers Edge	Marketing & Communication
Identity Management System (IDM)	Library and IT Services

The system managers are ultimately responsible for compliance with legislation and regulations and must take measures to this end, such as security measures. But even if an item of Personal Data is added to an existing system (e.g., Osiris), they must ensure that this is permitted on the basis of the GDPR. Think, for example, of adding a fingerprint for identification purposes.
In addition, we distinguish persons responsible for the process. They are accountable for a (partial) process. They are also supported by officers who have a responsibility in this respect (persons responsible). Some examples are:

Process	Process Manager
Enrollment student	Student Administration
Providing Education	Dean of a School
Performing academic research	Researcher

In these processes, such as student enrollment, Personal Data is also processed. The process owner is responsible for ensuring that the Personal Data he processes complies with the GDPR and with this Policy and is expected to guarantee this in his procedures. For example, he must ensure that they are correct and that if consent is withdrawn, this is processed.

It also happens that an organizational unit requests Personal Data from another unit. For example, a School that wants to have alumni's Personal Data for a mailing about an activity. The contact details of the alumni are managed by DARO. DARO is responsible for ensuring that the database containing this Personal Data complies with the GDPR and this policy. They should also determine whether there is a basis for providing these Personal Data for

[10] For an explanation regarding responsible and accountable, we refer to Part III, in which the RASCI model is explained.

this purpose. Does this constitute a legitimate interest or has the alumnus given his consent to this particular disclosure? This is DARO's responsibility.
The School is subsequently responsible for the protection of the Personal Data when processing this Personal Data in the mailing. For more details, see **paragraph 6.5 on internal disclosures**.

This responsibility for the various subareas is further elaborated in the thematic policy in **paragraph 11.7.**

3. GDPR: basic conditions

Personal Data is

---

any information relating to an identified or (in the future) identifiable natural person.

This means that the combination of data that cannot be traced back to a person separately can also be characterized as Personal Data because the link can be traced back to a natural person. All data belonging to this person to be traced are, therefore, Personal Data, e.g., some general characteristics in a small survey/research. In combination with of place of residence, age, number of children, and unit, you may already be able to trace a person and if you then register medical data, these are all Personal Data. Another example is information that can be traced back to a Data Subject in the future. You talk about the catering employee and, after he has delivered the coffee, it is known whom that is.
Therefore, when it comes to data relating to a person, it quickly becomes Personal Data since characteristics linked to each other can result in tracing it back to a person.

A number of basic conditions have been incorporated into the GDPR, which should be considered cumulatively as preliminary questions before one starts processing personal data:

- Necessity
- Proportionality
- Subsidiarity
- Effectivity

Principle processing by TiU	TiU only processes Personal Data if this complies with legislation and regulations and takes place on the basis of a specific purpose (purpose limitation). The data must be accurate, relevant, and not excessive in relation to the purpose for which it is processed. TiU will take appropriate technical and organizational measures to prevent unauthorized or unlawful processing of Personal Data.

The above-mentioned basic conditions are given shape in the GDPR by the so-called Principles .

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Storage limitation (retention period)
- Accuracy

Integrity & confidentiality (Security, training, awareness)
These principles are also reflected in the rights for data subjects and accountability for the organization.

- Rights of the Data Subjects
- Accountability

These Principles are further elaborated for TiU in the following chapters. An overview of all principles is given in **Appendix 2**.

Part II: GDPR: basic provisions

The basic provisions can be divided in three parts, namely the legal basis, the legal material requirements and the legal formal requirements.

A. Legal Basis: Lawfulness and Purpose Limitation

This section provides an elaboration of the Principles from the GDPR in the form of the guidelines for TiU. First, the Lawfulness (**Chapter 4**) and Purpose Limitation (**Chapter 5**) are tested. Each Processing must comply with these principles.

Chapter 4	Lawfulness including processing basis (**section 4.2**) and special requirements for **Special Personal Data** (**section 4.3**); **Sensitive Personal Data** (**section 4.4**); and in the event of **Transfer of Personal Data** (**section 4.5**)
Chapter 5	Purpose Limitation

B. Legal material requirements

If the Processing complies with the principles of lawfulness and purpose limitation, then this can take place and the following principles (**chapters 6 through 9**) must be observed in order to ensure that we handle the data with care.

Chapter 6	Guidelines on **data minimization** and necessary Personal Data, including Guidelines for **internal disclosure**
Chapter 7	Guidelines on **storage and archiving** of Personal Data (Storage Limitation)
Chapter 8	Guidelines on safeguarding the **accuracy** of the Personal Data
Chapter 9	Guidelines on integrity and confidentiality including the **organizational and technical security** of the Personal Data

C. Legal formal requirements

In addition to the more substantive - material - requirements, there are also some formal requirements, namely the rights for data subjects and accountability for the organization.

Chapter 10	Guidelines on safeguarding the compliance with the **Rights of the Data Subjects**
Chapter 11	Guidelines on compliance with the Principles on **Accountability** including **DPIA** and **DTIA** (**section 11.2** and **section 11.3**), **Data Processing Register** (**section 11.4**), **Agreements** (**section 11.5**), **Data Breaches** (**section 11.6**) and Guidelines on the preparation of **Privacy Statements** (**section 11.7**) and **Policies** (**section 11.8**)

4. Lawfulness

4.1. Principle

The first principle based on the GDPR is **lawfulness**:

Tilburg University will only process Personal Data if this is lawful.

- TiU **lawfully** processes Personal Data only if there is a legal basis for this (**Section 4.2**):
  - The Data Subject has given consent for the Processing of the Personal Data for one or more specific purposes, or
  - Processing is necessary for the performance of an agreement to which the Data Subject is a party, or for the purpose of concluding an agreement, or
  - Processing is necessary in order to comply with a legal obligation applicable to TiU, or
  - Processing is necessary to protect the vital interests of the Data Subject or another individual, or
  - Processing is necessary for the performance of a task carried out in the general interest or in the context of public authority assigned to TiU, or
  - Processing is necessary for the representation of the legitimate interests of TiU or of a third party, except where the interests or fundamental rights or freedoms of the persons whose Personal Data are processed outweigh those interests, especially when the Data Subject is a child.
- TiU will not process any **Special Personal Data** unless there is an exception as referred to in the GDPR (Article 9). One of the exceptions is, for example, scientific research. Strict requirements apply to the processing of Special and Sensitive Personal Data (**Sections 4.3 and 4.4**).
- TiU will, in principle, not transfer Personal Data to **third countries or international organizations** unless there is an adequate level of protection (Chapter V of the GDPR) (**Section 4.5**).
- **Direct marketing (Dutch Telecommunications Act)**: TiU will comply with the obligations of the Telecommunications Act, which means that in the case of direct marketing:
  - Only persons who have given specific consent will be approached;
  - It is guaranteed that persons who have not given their consent or who have withdrawn it are not approached or are no longer approached.
  - See **thematic policy External Relations**

4.2. Processing Basis

Any Processing of Personal Data requires a Processing Basis. These principles are exhaustively included in the GDPR. If there is no Processing Basis (Article 6 of the GDPR) for the Processing, it is unlawful and may not take place.

Processing Basis	Explanation
Necessary for statutory duty	• This principle applies if the Processing is based on a statutory obligation; • In case of Processing based on this principle, the Data Subject does not have the right to erasure of data (right to be forgotten): *Example: the disclosure of certain Personal Data of employees to the Tax Administration or the disclosure of Personal Data to the external auditor for auditing purposes.*
Necessary for performance of an agreement	• The Data Subject must be a party to the agreement; • Only if the agreement cannot be properly fulfilled without the Processing taking place, "necessity" applies. The fact that something is useful does not automatically 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 Operations necessary for the performance of the "study contract" between TiU and the student.*
Necessary for the task of public interest/public authority	• Public authority is involved in the performance of a public service task: a task of a government body that is regulated by law; • In the event of Processing on this basis, the Data Subject will not be entitled to erasure of data. *Example: awarding a degree and awarding a diploma to a student.*
Necessary for vital interests	• In principle, an appeal can only be made on this basis if the Processing cannot be based on any other basis; • A vital interest touches on the life of a person. *Example: Disclosure of Personal Data in the event of an accident or humanitarian emergency such as a major fire.*
Necessary for a legitimate interest	• The Processing must be necessary for the representation of the legitimate interests of TiU or of a Third Party; • A balancing of interests 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 TiU or of a Third Party; Possible aspects of the balancing of interests include the consequences for the data subject, additional safeguards put in place, the seriousness of the interference and whether the data subject can reasonably expect the processing to be carried out for that purpose. • These 3 aspects (justified, necessary and the balancing of interests) should be substantiated.

	• The Data Subject may object to the Processing at any time, after which TiU 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;
Consent	• The Data Subject must be well (clearly) **informed in advance** of the Processing for which he gives his consent. See **Section 10.2** for more information. • Permission must be actively given. That is to say, no use should be made of a check box that is filled in beforehand. • TiU must be able to demonstrate consent after the event; • 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 as to distinguish it clearly from other matters. Think, for example, of including a separate check box on a form; • Consent may be withdrawn by the Data Subject at any time, and should be as simple as giving it. *Example: Processing Personal Data for future students who have given consent to be approached for university activities.*

Processing Basis	Processing of the Personal Data is **only permitted** if one of the above **bases** is **met**. The ground must be stated in the Data Processing Register (**Section 11.4**)..

In addition to these general requirements of lawfulness, additional requirements of lawfulness apply:

- Processing of Special and Sensitive Personal Data (**Sections 4.3 and 4.4**)
- Transfer of Personal Data (**Section 4.5**).

4.3. Lawfulness: Special Categories of Personal Data

The law provides for a number of Special Categories of Personal Data that are extra protected by the legislation because of the protection of the Personal Data of the Data Subject, in which, in principle, a ban on processing applies, but in which exceptions are possible (e.g., for scientific research). There are, therefore, a number of additional requirements to the general ones on the Processing Basis in the context of lawfulness.

Special Categories of Processing Personal Data	Data are considered to be Special Personal Data if they indicate: • Racial or ethnic origin • Political views • Religious or philosophical beliefs • Trade union membership and • Genetic data • Biometric data for identification purposes • Health data (medical data) • Data relating to sexual behavior or sexual orientation
Rules for Processing	Special Personal Data may **not** be processed **unless** an **exception** applies as referred to in Article 9 of the GDPR: • The Data Subject's explicit Consent is given; • The Processing is necessary in connection with an obligation laid down by a collective labor agreement or by legal duty or rights in the field of social security and social protection legislation; • The Processing is necessary to protect the vital interests of the Data Subject unless the Data Subject is in a position to give his Consent; • The Special Personal Data were obviously made public by the Data Subject;[11] • The Processing is necessary for establishing, exercising, or substantiating a legal action; the (preparation of) a judicial proceeding; • The Processing is necessary for a substantial public interest laid down in a law;[12] • The Processing is necessary for the assessment of an employee's fitness for work, health care, and a number of related matters specifically indicated. Only if determined by law or in a medical treatment contract and only by professionals who have a legal professional confidentiality such as doctors or psychologists; • Processing is necessary for public health; • The Processing is necessary for scientific research that serves a public interest. This exception may only apply if it proves impossible to obtain Consent or if it involves a disproportionate effort. Safeguards must also be provided in such a way that the privacy of the Data Subject is not disproportionately harmed. For more information, see the **Thematic Policy on Scientific Research**. **Caution**! Naturally, all other Principles mentioned in Part II for the Processing of Special Categories of Personal Data also apply. So there is also a need for a Processing Basis: there must be Purpose

[11] It must be an obvious disclosure, such as indicating on the internet or TV to be homosexual and not, for example, by placing that information on a non-public dating site;
[12] For example, to fulfil an obligation under international law or if the Processing of data revealing racial or ethnic origin is unavoidable for the purpose of identifying the Data Subject.

	Limitation et cetera. In addition, there is a stricter requirement regarding Security (**Chapter 9**).

Below are a number of elaborations for specific categories of Special Personal Data, for which additional rules apply.

4.3.1. Data regarding health (medical data)

TiU registers medical data in a number of cases, for example, in the context of scientific research concerning employee absenteeism (e.g. the Dutch Absenteeism Reduction Act and the occupational health physician), in response to a request for help from an employee or student (e.g., from a dean of students or health and safety officer), or in response to a student's request for extra facilities during lectures or examinations (e.g., in the case of dyslexia). These are Special Personal Data. Therefore, processing is, in principle, unlawful unless one of the above exceptions applies. In most cases, this should be the exception of "explicit Consent." In scientific research it may be the exception "necessary for scientific research" (**see Thematic Policy Scientific Research**). Once the applicability of one exception has been established, the compliance with the other principles can be verified.

Medical data are included in the Special Personal Data and are, therefore, particularly sensitive.

Medical data	The recording of medical data is permitted if this is **necessary**, for example, in the following situations: ○ Scientific research ○ Additional student facilities during lectures or examinations (e.g., due to dyslexia) ○ Request for care from a student or employee (dean of students, health and safety officer) ○ Employee sickness absence Only with the specific permission of the person concerned (recorded and provable, erasure of the data if requested by the person), unless another legal basis for the specific processing is established such as reintegration employees (Art 30(1) sub b UAVG). **Caution**! Naturally, all other Principles mentioned in **Part II** for the Processing of Special Categories of Personal Data also apply. So there is also a need for a Processing Basis: there must be Purpose Limitation et cetera. In addition, there is a stricter requirement regarding Security (**Chapter 9**).

The use of special Personal Data in scientific research is subject to special legal provision (see **Thematic Policy on Scientific Research**).

4.3.2. Biometric data (regarding identification)

Biometric data may include fingerprints, portraits or facial images, voice recognition, and face scans. The Biometric Data are Special Personal Data only if these means are used for identification purposes. For example, a passport photo on an identity document is a Special item of Personal Data, but a holiday photo with a face that is recognizable on it is not.

When TiU uses Biometric data for identification purposes (for example, the use of a finger scan to access a facility such as the Sports Center), this constitutes a Processing of Special Personal Data.

In principle such Processing is unlawful, unless one of the exceptions applies. This will often be “explicit Consent.” The Consent must be given specifically and consciously (i.e., not as part of general terms and conditions) and, in order to ensure that the Consent is given freely, an alternative must be offered (e.g., identification by student card). Once the applicability of an exception has been established, the compliance with the other privacy principles can be verified.

Biometric data serving as identification	Biometric data may be used for **identification** purposes only if: • The person specifically (consciously) gives consent for this. • The usage is not made compulsory (an alternative is offered). • The storage of the Biometric data must be adequately secured (confidentiality, secret) according to security grade high (for more details on the requirements, see the **Information Security Policy[13] and Appendix 2**). **Caution!** Naturally, all other Principles for the Processing of Special Categories of Personal Data also apply. So there is also a need for a Processing Basis: there must be Purpose Limitation et cetera. In addition, there is a stricter requirement regarding Security (**Chapter 9**).

Only biometric data for identification purposes are Special Personal Data. Biometric data in the context of scientific research are, therefore, legally not regarded as Special Personal Data but are still sensitive. For more details, we refer to the **Thematic Policy on Scientific Research**.

4.4. Lawfulness: Sensitive Personal Data

In addition to Special Personal Data included in the GDPR, there are also Sensitive Personal Data.

Sensitive Personal Data	Personal data that can be regarded as sensitive: • citizen service number (BSN) or alien registration number (V number), • copy of identity document/residence permit, • Personal Data of minors, • Information about the performance of an employee or student, such as appraisal forms or examination results.
Rules regarding processing	In addition to specific requirements regarding BSN, copy of identity document as mentioned here, a stricter requirement regarding security applies (**Chapter 9**), with extra attention to both the storage (see **Section 9.3**) and the method of delivery / retrieval (see **Section 9.4**) of the data.

13

4.4.1. Citizen Service Number (BSN)

The BSN is a Sensitive Personal Datum. It is, after all, a very important identification number, which can be misused and which can have major personal consequences (identity fraud). Additional requirements have been imposed by law on the use and registration of this BSN by organizations. The following rule applies:

Citizen service number (BSN)	The BSN is only processed by TiU if there is a legal basis for this or if this is permitted by a General Administrative Measure. This is the case for: • Employees in the context of the Dutch Wages and Salaries Tax Act (including keeping a copy of the identity document stating the BSN); • Students (on the basis of the Dutch Higher Education and Research Act); • Participants in civic integration language courses (on the basis of the Civic Integration Act). Reasons must be given for the processing of the BSN in the Data Processing Register (reference to the (legal) basis). In addition, of course, all other principles apply.
Access to BSN	The BSN may only be visible to employees for whom this is necessary in the context of their jobs. This must be recorded in the Data Processing Register, stating the reasons. *Example: If an employee of the Student Desk does not need the BSN on the basis of a legal ground, he is also not allowed to see this field.*

4.4.2. Identification and copy of the identity card

Although a full copy of an identity document can be made quickly, this is only permitted in a limited number of cases because the risk of identity fraud is high, for example, by having the BSN and a passport photo on the identity document.

Identification	If it is sufficient to show an identity document, it is **not permitted** to make a **copy/scan** of it or to copy the data. Think of: • participation in an examination • suppliers who want access to the campus.
Identification document	A full copy of the identity document must be kept if there is a legal basis for doing so. This applies to • employees in the context of the Wages and Salaries Tax Act (including keeping a copy of the identity document with the BSN); • students (on the basis of the Higher Education and Research Act); • participants in civic integration language courses (on the basis of the Civic Integration Act); • hired or subcontracted personnel who do not have the nationality of one of the EEA countries (Dutch Foreign Nationals (Employment) Act (Article 15(2));

	• international students with a non-EU nationality (for the purpose of applying for a residence permit/visa (on the basis of the Aliens Act); and This registration must be recorded in the **Data Processing Register** stating the reasons and on the basis of the law (see **Section 11.4)**. **SUPPLEMENT**: The Data Subject may provide TiU with a copy of his identity document if he has marked it (statement that it has only been provided for a specific legitimate purpose, e.g., booking business trips) and masked it (passport photo and BSN crossed out). It is better to just write down the information you need (e.g., passport number and name) securely (e.g., in a file). Tip: use the copy ID app to do this.
Marking and masking the identity document	• If a copy of the identity document has to be kept, it must be clearly stated on the copy for which purpose it is kept. • If there is no legal obligation to keep a complete copy of the identity document, the Data Subject must mask (make invisible) the BSN and, if desired, the passport photo.

4.4.3. Minors

TiU also offers services to minors under the age of 18. Think, for example, of the Children's University or minors who follow some subjects (for example, in the case of a program for highly gifted children). Minors are, in principle, competent to perform legal acts and, therefore, to give consent for a certain Processing of Personal Data, provided that the minor acts with the consent of his or her parent/guardian. In the case of an act for which it is customary in society that minors of the related age perform this independently, the consent of the parent/guardian may be assumed to have been given for that purpose.

Consent minors	The registration of Personal Data of **children younger than 16 years of age** for which the basis "Consent" applies **is only permitted if explicit Consent** has been obtained from the parent/guardian. This Consent must be recorded so that it can be demonstrated afterwards at any time.
Marketing	The parents' or guardian's Consent can be given by stating so or providing a signature. *For example, invitations to Children's University or open days*.
Scientific research	For this, see the specific guidelines in the **Thematic Policy scientific research**

4.4.4. Data on performance

TiU processes data on the performance of employees (appraisal) and students (examination results). These data are obviously very sensitive and should be treated with care.

Data on performance	Data concerning the performance of the employee/student may only be visible to employees for whom this is necessary in the context of their jobs. This must be registered in the Data Processing Register,

employee/ student	stating the reasons. For specific guidelines see **Thematic Policy Personnel** and **Thematic Policy Education/Students.**

4.5. Lawfulness: Transfer of Personal Data

The transfer of Personal Data to Third Parties, Processors, or other Controllers entails risks for the Data Subjects. Although the GDPR offers the countries within the European Union some room for maneuver in the implementation of certain matters, the implementation of the GDPR means that virtually the same legislation applies to the countries within the European Union. Outside the European Union, however, different rules apply. This means that different rules apply regarding transfers of Personal Data to various countries.

4.5.1. Transfer to third party/parties within the European Union and the European Economic Area

The level of data protection within the European Union is (almost) the same. This also applies to the countries that are members of the European Economic Area (EEA), Norway, Liechtenstein, and Iceland.

Requirements to transfer within the EU/EEA	The transfer (or Processing) of Personal Data within the EU or EEA is subject to the normal privacy rules. This means that the GDPR and all previous Privacy & Protection of Personal Data Principles must be complied with. There must be a Processing Basis and established legitimate purpose. Also think about registering in the **Data Processing Register (Section 11.4)**, concluding an Agreement with the other Party, for example a Data Exchange Agreement or a Processor Agreement **(Section 11.5)**, et cetera.

4.5.2. Transfer to third party/parties outside the European Union and the European Economic Area

For the transfer and Processing in countries outside the European Union and the European Economic Area, separate rules apply because the level of security may not be equal to the level of security within the EU and EEA based on the GDPR.

Requirements for transfer outside the EU/EEA	For the transfer (or Processing) of Personal Data outside the EU/EEA, an adequate level of protection must be implemented. The GDPR has described the cases in which this applies: • If the country is on the European Commission's country list that is published on the website of the Dutch Data Protection Authority[14]. • If appropriate safeguards have been put in place and the Data Subjects have enforceable rights and legal remedies at their disposal. Article 46 of the GDPR contains the conditions for this exception. This exception may apply, for example, when binding corporate rules exist or Standard Contractual Clauses (SCC) have

[14] https://autoriteitPersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu#faq

been agreed upon (standard provisions of the European Commission or a data protection supervisory authority).
A Data Transfer Impact Assessment (DTIA) may need to be carried out where a risk assessment is conducted (**Section 11.3**). This involves looking at the service, technical, organizational and contractual measures, and legislation in the recipient country.

- If the above does not apply, the transfer may only take place under one of the following conditions:
    - The Data Subject has unambiguously given Consent, whereby TiU informed the Data Subject of the level of protection of the country in question;
    - Transfer is necessary in order to perform an agreement between TiU and the Data Subject (e.g., booking a flight);
    - Transfer is necessary in order to perform an agreement to which the Data Subject is not a party, but in which the Data Subject has an interest (for example, in the context of an insurance policy);
    - transfer is necessary for important reasons of public interest (e.g., international exchange between financial supervisory authorities);
    - transfer is necessary for the establishment, exercise, or defense of a legal claim (e.g., transfer to an international collection agency);
    - transfer is necessary because of vital importance for the Data Subject (for example, in the event of a foreign hospitalization of one of our students);
    - Transfer takes place from the register established by statutory regulation (e.g., a public register of members of regulated professions such as psychologists);
    - If one of the above conditions is not met, the transfer may, nevertheless, take place in the case of an occasional transfer, if it concerns a limited number of Data Subjects, if it is necessary in the interests of TiU that outweigh the interests of the Data Subject, and if TiU takes appropriate safeguards for the protection of the Personal Data and informs the Authority for Personal Data and the Data Subject thereof.

If the transfer is permitted, all (other) obligations from the GDPR and all previous Principles must be complied with. There must then be a Processing Basis and established legitimate purpose. Also consider registering the Processing activity in the Data Processing Register, concluding an Agreement with the other party such as, for example, a Data Exchange Agreement or a Processor Agreement, and possibly Standard Contractual Clauses (section 11.5) , et cetera.

5. Purpose Limitation

5.1. Principle

The second Principle based on the GDPR is purpose limitation:

Tilburg University will only process Personal Data if there is a legitimate purpose.

TiU will only process Personal Data if:

- TiU is clear why and how Personal Data are processed: there is a specified, explicit, and legitimate purpose.
- TiU guarantees that if Personal Data are used for a purpose other than that for which it was collected, this new Processing will also meet the requirements. In doing so, TiU will take into account that further Processing with a view to scientific research will not be considered incompatible with the original objective. This includes, for example, further processing of Personal Data that have already been collected (see explanation in the table).

Specified and explicit	Specific purposes must have been established before the Processing is started. A vague description or description that is too broad does not suffice.
Legitimate purposes	The fact that a Processing is lawful is not sufficient for assuming that a legitimate purpose exists. Especially when using the legitimate interest basis, but also in doubtful cases regarding other bases, a balancing of interests between the interests of TiU and the Data Subject should take place.
Not incompatible	Processing of Personal Data for a purpose other than that for which it was collected is permitted if the purpose of further Processing is compatible with the purpose previously established. This depends on, among other things, a possible link between the two purposes, the framework in which the data were collected, the Data Subject's reasonable expectations, the nature of the data, the consequences of the intended Processing for the Data Subject, and the extent to which appropriate technical and organizational protection measures are provided.
Scientific research	The further Processing with a view to scientific research is **always** considered **compatible** and is in principle also permitted if this purpose is not explicitly mentioned in the original processing (**Thematic Policy Scientific Research**) In this case, however, the purpose must be laid down for the new Processing. Of course, all other principles as discussed in the Policy Privacy & Personal Data Protection also apply to further Processing, including requirements of the legal processing base and disclosure requirements. On this basis, it is strongly recommended that any further Processing in follow-up research is identified in initial research.

Appendix 3 contains the list of purposes for which TiU processes Personal Data, including the categories of Data Subjects. The most current list is included in the Data Processing Register. Any additions or other legitimate purposes on this list shall be subject to the approval of the Data Protection Officer.

Purpose limitation	The processing of Personal Data shall only be allowed if one of the purposes specified for the category of persons in question is fulfilled (**Appendix 3: Purposes for processing**). (Detailed) further specification of the purposes must be included in the **Data Processing Register (Section 11.4)**.
Responsibility	The process or system owner is responsible for establishing and recording the purpose of the Processing. Additions or changes to purposes for processing (**Appendix 3**) may only be made with the permission of the Data Protection Officer.

6. Minimal Processing of Data (Data Minimization)

6.1. Principle

The third principle in the GDPR is data minimization or minimal processing of data (Article 5 (1) I of the GDPR)

Tilburg University guarantees that Personal Data are adequate, relevant, and not excessive in relation to the purpose(s) for which they were collected.

- TiU does not process more Personal Data than is necessary in relation to its purpose (data minimization, **Section 6.2**).
- TiU guarantees that it processes the Personal Data that are the minimally necessary to realize a correct picture of the Data Subject (**Section 6.3**).
- If possible, TiU will Aggregate, Anonymize or Pseudonymize the Personal Data (**Section 6.4**).
- TiU does not store Personal Data for longer than is necessary for the purpose for which it was processed or for which there is a statutory storage period (**Chapter 7**).

6.2. Data Minimization

Data minimization is collecting information with as much limitation as possible. It is important that no more Personal Data are processed than necessary in relation to the purpose(s) for which they were collected. This is described in the principle of minimal data processing as set out in **chapter 3**. The principles of proportionality and subsidiarity apply. If Processing can or may be done without certain data, then you should not process that data. And if the purpose intended by the Processing can be achieved by not processing any or fewer Personal Data, than you should work accordingly. Handy to have data is not the same as necessary.

Data Minimization	TiU does **not process more Personal Data** than is **necessary** in relation to the purpose (minimization).

6.3. Necessary Data

Some Personal Data are necessary for the purpose for which you process the Personal Data. This also means that you must not collect too few Personal Data. After all, this can lead to an incorrect picture of the Data Subject.

Necessary Data	TiU guarantees that it does not collect **too few Personal Data** to avoid an incorrect picture of the Data Subject.

6.4. Aggregation, Anonymization or Pseudonymization

Aggregation, Anonymization and Pseudonymization are proven methods of making Personal Data untraceable, or as little traceable as possible. Personal Data are not required for the entire retention period in all cases, but it is important to retain the corresponding data. Think, for example, of data for scientific research, where the data are necessary (for accountability purposes), but the contact data (name, address, place of residence, and telephone number) not anymore at a certain moment. The responsible party can then Aggregate, Anonymize or Pseudonymize the data.[15] See also **Chapter 7 on storage/archiving and the Research data Management Regulations.**

Methods	If Personal Data are no longer necessary, but the data cannot yet be erased, the Personal Data must be aggregated, anonymized or pseudonymized at the earliest possible stage.
Aggregation	**Aggregation** is the merging of data, for example by counting, summing or averaging underlying data.
Anonymization	**Anonymization** means that data about a person is no longer traceable to the individual.
Pseudonymization	**Pseudonymization** is concealing a per'on's identity.

The purpose of Pseudonymization is to conceal a per'on's identity from third parties. Pseudonymization separates identifying data from non-identifying data and replaces the identifying data with artificial identifiers. An example of Pseudonymization is the replacement of a respond'nt's data in a medical examination by a unique respondent number. The medical data will then be linked to this respondent number instead of a name, address, and place of residence. As a result, outsiders cannot see whom the person is to whom the medical data belong. Only the person who can make the link between the respondent number and the name (e.g., the researcher) is able to link the medical data. However, sufficient (organizational and technical) measures must be taken so that unauthorized persons cannot link these files (**Chapter 9 Security**).

Pseudonymized data should not be confused with Anonymous data. Because it is possible to link up Pseudonymized data, the GDPR is fully applicable.

For Anonymous data, the GDPR is no longer applicable. Please note that with Anonymous data, there is no longer any possibility for identification or tracing back to persons.

[15] The information in this explanation on Pseudonymization and Anonymization is derived from the Dutch GDPR (AVG) Manual of the Ministry of Justice and Security.

Anonymization is a processing operation and still falls under the GDPR. If data can still be traced back to a person, Anonymization does not apply, but it is Pseudonomyzation.

6.5. Internal Disclosures of Personal Data

The principle of data minimization also applies to the internal disclosure of or access to Personal Data. This means that only employees who need access to certain Personal Data may have access to them. The Data Processing Register (**Section 11.3**) must state which employees have access to which Personal Data and/or which internal disclosures take place on a structural or occasional basis.

6.5.1. Occasional Disclosure

The following applies to the disclosure of information on an occasional basis, for example in the context of monitoring, reporting, or communication:

Requirements of internal occasional disclosure	The disclosure of Personal Data on an occasional basis is only permitted if there is a Data Processing Basis for this (**Section 4.2**) and there is a Purpose Limitation (**Chapter 5**): the disclosure must be necessary (which is not the same as 'handy'). The following applies: • The request for an occasional disclosure must be made using the **model form internal transfer Personal data**. and • The Data Representative of the provider must check whether the previous requirements have been met before the data are provided. If the disclosure does not meet the above requirements, the disclosure will not take place. • The disclosure must be occasional (non-recurring). If the disclosure is of a structural (regular) nature, the Processing must be recorded in the Data Processing Register.
Advice	The Central Privacy Officer and/or the Data Protection Officer may be asked for advice by both parties.
Responsible	The requesting party is responsible for ensuring compliance with this directive.
Audit trail	Forms must be archived by the requesting party.

6.5.2. Structural Disclosure

In addition to the ad hoc disclosure of Personal Data, certain information is also provided structurally (regularly) to other parts of the organization. Think, for example, of Human Resources providing Personal Data to supervisors.

Requirements to structural disclosure	If Personal Data are disclosed to other organizational units on a structural basis, this must be registered in the Data Processing Register (**Section 11.3**).

7. Storage/Archiving of Personal Data (Storage Limitation)

7.1. Principle

The fourth principle from the GDPR is: storage limitation (Article 5(1)(e) of the GDPR).
It is important that Personal Data is not stored longer than is legally required or necessary in relation to the purpose for which it was collected. Handy is not the same as necessary here. A maximum storage period must, therefore, be determined in advance for each item of Personal Data (**Section 7.1**) and erasure must take place safely (**Section 7.2**).

7.2. Maximum Storage Period

To be able to guarantee compliance with the GDPR principle regarding storage limitation, TiU determines the storage period of Personal Data.

Maximum Storage Period	• Personal Data may not be kept for longer than is necessary for the purpose for which they were processed or for a statutory period. • Personal data that are no longer necessary for everyday operations should be archived, which requires more limited access measures. This can be done by establishing authorization profiles (in the case of digital files) or access control (physical archives). This should be regulated procedurally. • From the moment that the Processing of an item of Personal Data is no longer necessary or the statutory period has expired, this item of Personal Data must be erased or made unrecognizable.
Responsible	The person responsible for the processes is responsible for determining the maximum storage period and the compliance of this by means of control and monitoring.
Audit trail	The maximum storage period is recorded in the Data Processing Register. In the event of a statutory period, reference should be made to the relevant section of the law.

This means that for each system, Personal Data file, and archive, the person responsible must determine a maximum storage period in advance, which must be recorded in the Data Processing Register.

7.3. Erasure of Personal Data

In the interests of the Data Subject's privacy risks, the erasure must take place safely.

Requirements for erasure	Erasure of (files or archives of) Personal data should be kept secure, namely: • Automated, or • in case of physical erasure always in the presence of several persons, and • by a safe method (e.g., through a specialist company)

Responsible	The person responsible for the process is responsible for the timely and safe erasure.
Audit trail	A justification must be drawn up for the erasure of archives or digital files: • Manual erasure of physical archives: erasure protocol • Ad hoc erasure of digital archive (manual): erasure protocol • Automated erasure: description of selection criteria and erasure program.

This means that the erasure must be carried out safely: for example, shredding or incineration in closed containers in the case of an archive, or, in the case of erasure of data carriers, automated according to properly tested programs.
The Data Protection Officer may be asked to give advice on erasure.

8. Accuracy of Personal Data

8.1. Principle

The fifth principle from the GDPR is **accuracy of Personal Data** (Article 5(1) (d) of the GDPR).

Tilburg University guarantees on the basis of reasonableness that the Personal Data are correct.

TiU will take all reasonable steps to guarantee that the Personal Data are accurate and will update or erase these if necessary.

If incorrect or outdated Personal Data are used, this can have annoying consequences for the Data Subject. Therefore, based on the Principle of Accuracy, it is required that the data must be correct and accurate. This is subject to a far-reaching, best-efforts obligation. The principle is further elaborated in the right to rectification (**Section 10.5**), but there is also an independent obligation for TiU to actively ensure the accuracy of the data. It is, therefore, not permitted to wait passively for the Data Subject to report himself.

Accuracy	TiU takes all reasonable measures to guarantee that the Personal Data are correct and will correct them where necessary. TiU will: • communicate data modification procedures to employees, students, and other people concerned in an accessible manner; • regularly request students, employees, alumni, and corporate relations to update Personal Data. This can be combined with regular communication (e.g., in a newsletter); • ensure that old mailing lists are not used (e.g., a copy from the past); • Set up procedures to check mail returns and bounced emails: ○ Employees/students: to be corrected.

	○ Alumni and others: if we do not have any new details to erase contact details.
Responsible	The process owner/system owner is responsible for this.

It is therefore important, on the basis of the GDPR, to guarantee that for mailings, for example, recent data is used and not old lists. Not all data need always be up to date. An example is the expiry date of an identity document. On the basis of legislation, this must, in certain cases (for identification purposes), be laid down at the start of the relationship (commencement of employment as an employee or enrollment as a student), but need not be updated from a legal point of view.

Finally, we need to set up procedures for returned mail and email in order to correct or erase these data.

9. Integrity and confidentiality

9.1. Principle

The sixth principle from the GDPR is that **appropriate technical or organizational measures** (Article 5(1)(f) AVG) need to be in place, such as adequate **security** (Article 32 of the GDPR), clear policies and procedures, attention to training and awareness.

Tilburg University shall take appropriate technical and organizational measures against unauthorized and unlawful processing of Personal Data and against the accidental loss, erasure, or damage of Personal Data.

This means that:

- TiU has set up the organization of information security in such a way that it is suitable for the Personal Data that is being processed. It shall mainly take the risks into account, in particular those resulting from accidental or unlawful destruction of, loss of, alteration of, unauthorized disclosure of, or access to the data processed.
- TiU guarantees the foregoing with adequate procedures and guidelines and well-trained personnel.
- TiU has clearly laid down who is responsible for information security.
- TiU has set up a system that guarantees that information security incidents are followed up quickly and effectively.

TiU and its employees must treat Personal Data with care. Adequate security (both technical and organizational) and careful handling are logical requirements. Data Leaks are often caused by inadequate security or by human error. It is, therefore, of great importance that Personal Data are stored and retained in a secure manner and that employees are aware of the risks and their responsibilities (attention to awareness). In determining the guaranteed level of security, it is also important whether Special or Sensitive Personal Data are being processed. A number of important rules have been included in the following paragraphs. For

the detailed regulations, we refer to the 'iU's **Information Security Policy**[16], which includes, among other things, the CIA classification.

9.2. Access Security & Authorization

Archives or files containing Personal Data must be adequately secured by means of authorization profiles or other security measures. Only those employees for whom access is necessary for their work are allowed to have access. A point of attention here is personnel changes: if an employee leaves TiU or is given another job, the rights must be changed/removed.
This means that access to Personal Data included in systems (e.g., SAP and Osiris) must be arranged by means of authorization profiles. However, there are also several MS Office tools (Word, Excel) in which Personal Data are stored. These should be protected by strong passwords.

We also refer to the **Information Security Policy**[17].

Access to digital Personal Data file	• Personal data files are only accessible to employees who need to have access in the context of their jobs. This should be secured by means of authorization profiles (for each position) or the use of strong passwords (MS office). • Changes in the authorization profile may only be approved by the data owner (audit trail) with advice from the functional manager.
Access log files	• Access to applications/systems that include Personal Data should require logging in, and approved and denied access attempts should be recorded. • In the case of changes in personnel, access rights must be adjusted. • These log files will be kept for a minimum of 3 months and a maximum of 12 months unless otherwise required by law or unless the log files are necessary for the investigation of a (suspected) security incident.
Access to physical archive	• Only employees who need to have access to a physical archive as part of their jobs are authorized. • In the case of changes in personnel, access rights must be adjusted. • Authorization for access to an archive may only be granted by the owner of the archive (audit trail).
Audit trail	The granting of authorization must be recorded.

9.3. Storage of Personal Data

The storage of Personal Data must be adequately secured so that only authorized persons have access to the data. Think of encrypting files, authorization profiles, or locking physical archives.

[16] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/securing
[17] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/securing

Local hard drive (laptop, PC etc.), USB stick or other data storage device	If Personal Data are recorded on a laptop, tablet, USB stick, or other data storage device, it must be **encrypted**. According to current standards (in accordance with advice from LIS), this encryption must be sufficiently safe for data that are being protected.
Use of shared workstations / flex workstations	With shared workstations / flex workstation, storing files to **C and D drives** means that files are stored locally on the hard drive. If someone else logs into your computer, he will have access to these files. Therefore, files with Personal Data may **not** be stored here. Please note Take care if you download data from the workplace in question, the data remains on the computer's hard disk , making it accessible to others who have access to this computer.
Shared Network Drives	For shared network drives, such as the O and P drives, careful attention must be paid to authorizations when storing personal data. Among other things, ensure that the folders in which personal data are placed are only accessible to the employees who actually need access to the data in question. In addition, care must be taken to keep authorizations up-to-date (for example, when a colleague leaves or changes position) and to check these authorizations periodically.
Storage media (in the cloud)	Various applications are provided by the organization in which Personal Data can be stored safely (in the cloud). If you wish to use any other application for Personal Data, you must comply with the terms of this Policy. Think of security, but also, for example, of a Processing Agreement (**Section 11.5**). For the overview and a need for another application, contact your school/division's Information Manager.
Physical access security archive	Archives with Personal data should be kept locked and only be accessible to employees who, in the course of their duties, need to have access to them. If there are archives in a common room (cabinets), these must be locked. **Please note**: this also means that no unauthorized people are allowed access during the working day.
Logical access security data files	Personal Data files must be adequately protected with a login name and password. Only employees who need access as part of their jobs are given login credentials. **Please note**: this means that employees must lock their computers if they leave their workstations.
Home networks	The use of Personal Data files on private laptops or computers is only permitted if they are adequately protected. This means (not exhaustive) that the private laptop or computer must be equipped with: • a current virus scanner,

	• software that is supported, i.e., the latest updates of the operating software (e.g., Microsoft) have been made, • adequate access security to computer and files (encryption, with a password, or another technique).

9.4. Transmitting Files with Personal Data

It is important that the transmission of (files containing) Personal Data is done in a secure manner. This concerns both the transmission within TiU and the transmission to Processors or Third Parties.

Transmitting Personal Data Externally	If **Personal Data files** are transmitted (via mail or other medium) to external parties, the information must be adequately protected by means of encryption or password protection. **Please note**: Send the password separately via another medium.
Transmitting Personal Data INTERNALLY (to @uvt.nl)	If **files with Special or Sensitive Data** (**Sections 4.3 or 4.4**) are transmitted internally, they must be adequately protected by means of encryption or password protection. **Please note**: Send the password separately via another medium, for example, by phone or texting.
Application	A secure and recommended application is SURFfilesender[18].

9.5. Clean Desk & Clear Screen

It is important that Personal Data are stored securely during the working day, but also after the working day is over. This means, therefore, that no documents or files containing Personal Data may be accessible to others: in other words, clean desk/clear screen.

Clean desk and clear screen	If Personal Data files or documents are used by employees, they should not be accessible to others when leaving the workplace. This means: • Lock screen: The computer (or room) is locked when leaving a workstation. TIP: Use the hotkey combinations Windows logo key + L (for Windows PCs) or control + command⌘ + Q (for Macs) to lock your computer. • Clean desk: when leaving a workstation, the room is locked or the documents are stored in a lockable cabinet.

9.6. Training en Awareness

Employees need to be well informed concerning their obligations in the context of the GDPR and the security risks in everyday practice.

[18] https://filesender.surf.nl

Privacy & Security portal	All information regarding Privacy and Protection of Personal Data will be included on the **Privacy & Security Portal**[19] in an accessible and understandable way.
Training and awareness	Employees (with access to Personal Data) must be regularly informed about the obligations in connection with the GDPR, as well as the digital threats, and how to protect data properly.
Support	Employees who process Personal Data can contact the Sch'ol's or Divis'on's **Data Representative** for advice on the GDPR's obligations and security.
Responsibility	• The supervisor is ultimately responsible for the internal communication of guidelines and procedures and the training of personnel. • The Data Protection Officer and Central Privacy Officer ensure awareness. This is done in close cooperation with Information Security Officers and the Data Representatives. • The Central Privacy Officer and Information Security Officers provide the content to facilitate training and education.

9.7. Other Organizational and Technical Security

For the other technical and organizational measures, such as change management, guaranteeing continuity, and access security, we refer to the **Information Security Policy**[20].

[19] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security
[20] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/securing

10. Rights of the Data Subjects

10.1. Principle

The seventh principle from the GDPR is the **Rights of the Data Subject** (Chapter III of the GDPR)

Tilburg University guarantees that action will be taken in line with the rights of the individual whose Personal Data TiU processes.

These rights are elaborated in the following paragraphs:

- **Right to Be Informed**: TiU informs the Data Subject of the Processing and provides the information pursuant to Article 13 or 14 of the GDPR (**Section 10.3**)
- **Right of Access**: TiU provides access to the Personal Data at the Data Subj'ct's request (Article 15 of the GDPR), (**Section 10.4**).
- **Right to Rectification:** TiU rectifies incorrect Personal Data at the Data Subject's request (GDPR Article 16), (**Section 10.5**).
- **Right to Erasure**: TiU erases Personal Data at the request of the Data Subject if this is legally permitted (GDPR Article 17), (**Section 10.5**).
- **Right to Restriction**: TiU restricts the processing of Personal Data at the request of the Data Subject (Article 18 GDPR) **(Section 10.6**).
- **Right to Data Portability**: TiU guarantees the Data Subject's right to Data Portability (Article 20 GDPR) (**Section 10.7**).
- **Right to Object:** TiU will deal with objections by the Data Subject as referred to in Article 21 of the GDPR (if the Processing is based on a "task of public interest" or "necessary for the representation of a legitimate interest" or in the case of direct marketing) in accordance with Article 21 of the GDPR (**Section 10.8**)

10.2. Guidelines Applicable to all the Rights of the Data Subject

The guidelines mentioned below are applicable to all the Data Subject's rights.

Clarity	• All communications concerning the Data Subj'ct's rights should be available in a concise, transparent, comprehensible, and easily accessible form. • The information should be provided in clear and simple language. This applies both to information about how the rights can be exercised (e.g., on the Internet) and to the response to the Data Subject's requests.

For all the rights (with the exception of the right to be informed) the following also applies.

Who can make a request?	The request may only be made by the Data Subject personally, in which case identification must be sufficiently verifiable.

	For some requests, such as a removal request from a prospect student, contact details may suffice as identification, in other cases identification may be established by means of a TiU card or a valid and masked Identity Document.
Methods of disclosure	Disclosure (reaction) is free of charge and takes place • in writing, or • when appropriate, electronically (for example, when the Data Subject makes the request electronically and does not request any other arrangement), or • orally at the request of the Data Subject.
Rejection	In principle, a request is always granted. A rejection of a request is only allowed if TiU can demonstrate that • the application is manifestly unfounded or excessive (for example, if the Data Subject repeatedly submits the same request). If an excessive request is honored, a reasonable fee may be charged; or • the request cannot be processed (properly) because one of the procedural conditions below is not met: • the request does not comply with the regulations as set out in this Policy; • the request is not sufficiently specific; • the identity of the Data Subject cannot be established. Scientific research is subject to restrictions on the rights of the Data Subject pursuant to Article 89(2) of the GDPR and Article 42 of the GDPR Implementation Act. **Thematic Policy Scientific Research**. In addition, Article 23 of the GDPR contains a number of restrictive grounds for refusal, for example, the refusal of a request is permitted in the interests of public safety. The Central Privacy Officer must be consulted in advance for rejection. Within one month of receipt of the request, the rejection must be sent to the Data Subject in writing, **stating the reasons**, and pointing out the possibilities of complaint and appeal to the Data Protection Officer, the Authority for Personal Data, or the judge respectively.
Response period	As soon as possible but no later than one month after receipt of the request. In the case of a complex or large number of requests (this must be substantiated), the time limit may be extended by two months. In that case, the Data Subject must be informed of the extension within one month.
Person responsible	The request and its processing must take place in accordance with the standard procedure for the rights of the Data Subjects and is coordinated by the Central Privacy Officer and the Data Protection Officer (with the exception of the rectification of

	incorrect data). He will contact the following organizational units for a substantive response: • Human Resources is responsible for handling: (former/future) employees/temporary employees: • Student Administration: (future) students. • DARO: alumni and corporate relations: • Dean: (former) research respondents: • Other requests: Division/School with which the person has been in contact: The Data Protection Officer monitors the response periods. The responsible unit is required to ensure that the handling takes place promptly. If information from others is required in this respect, it is self-evident that they must provide this information on time.
Audit trail	All the Data Subjects' requests and the documents relating to the handling thereof, must be archived.

10.3. Right to Be Informed

The Data Subjects have the right to be well informed about which Personal Data are processed by an organization. See also **Section 10.2 for general guidelines**.

Obligation for the inclusion of a privacy statement	TiU informs the Data Subjects of the Processing of Personal Data by means of a **Privacy statement** that is easily found and accessible on the website.
Content of the privacy statement	The privacy statement contains at least the following information: • the identity and contact details of TiU; • the contact details of the Data Protection Officer; • the purposes for which these data are processed; • the legal basis for Processing Operations (Processing Basis); for Processing Data for which the Processing Basis "necessarily for legitimate interest" applies, the interest of TiU or the Third Party is also included; • where applicable, the (categories of) recipients of the Personal Data; • if the Personal Data are transferred outside the EU, on what grounds this is done; • the categories of Personal Data to be processed; • the storage period or, if that is not possible, the criteria for determining that period; • that the Data Subject has the right to request access, rectification, or erasure of the Personal Data; restriction of the Processing that concerns him; the right to object to the Processing; and the right to data portability; • that if the Processing is based on Consent, that the Data Subject has the right to withdraw the Consent at any time without prejudice to the lawfulness of the Processing prior to the withdrawal of the Consent;

	• that the Data Subject has the right to lodge a complaint with the Authority for Personal Data; • whether the Disclosure is a legal or contractual obligation or a necessary condition to conclude an agreement, and whether the Data Subject is obliged to provide the Personal Data and what the consequences will be if it is not provided; • if, in a particular case, the Personal Data have not been obtained from the Data Subject, the source from which the Personal Data originate. **The privacy statement is drawn up on the basis of the information in the Data Processing Register (Section 11.4).**
Responsibility	The Deans and Directors of the Schools and Divisions are responsible for including the mandatory information in the Data Processing Register (**section 11.4**). The general privacy statement is drawn up on the basis of this information and published by the Central Privacy Officer and the Data Protection Officer.

The content of the privacy statement is created by the information contained in the Data Processing Register. It is possible that this will be achieved in a multilayered way: more detail, for example, for a School or organizational unit and less detail at a TiU level.

Privacy Statement Division/School	Each Division/School can draw up a separate privacy statement in line with the model. The following conditions apply: • The privacy statement must be compliant and linked to the TiU policy; • The privacy statement must be approved by the Data Protection Officer prior to implementation.
Responsibility	The management of the organizational unit (Dean, Managing Director Division) is responsible for the privacy statement of the Division/School. The Data Representative will draw up this report.
Audit trail	The privacy statement needs to be published on the Division's or School's TiU website.

10.4. Right of Access

In the context of accountability, each Data Subject is entitled to obtain a definitive answer to the question of whether TiU processes his Personal Data. If this is the case, the Data Subject will have the right to access the Personal Data processed concerning him. See also **Section 10.2 for general guidelines**.

Request	The request must be made using the form "Request for Access to Personal Data."
Access to	The Data Subject will be given access to the Personal Data and to the following information: • the processing purposes;

	• the categories of Personal Data concerned; • the (categories of) recipients to whom the Personal Data have been or will be disclosed; • if the Personal Data are transferred outside the EU, which appropriate safeguards have been put in place; • the storage period or, if that is not possible, the criteria for determining that period; • that the Data subject has the right to request rectification or erasure of the Personal Data or restriction of the Processing that concerns him and the right to object to the Processing; • that the Data Subject has the right to lodge a complaint with the Authority for Personal Data; • if, in a particular case, the Personal Data have not been obtained from the Data Subject, all available information about the source of the Personal Data.
Responsible person	See **Section 10.2**.

10.5. Right to Rectification or Erasure

The right to correction or deletion is referred to in the GDPR as rectification or erasure. A Data Subject may demand that his or her Personal Data be rectified or erased, on the grounds of inaccuracy, incompleteness, or not allowed to be processed on the basis of the GDPR or this Policy. Such a request often follows a right of access. See also **Section 10.2 for general guidelines.**

Request	The application must be made on the form **Request for Rectification or Erasure**[21].
Grounds	TiU is only obliged to comply with the request for: **Rectification** of Personal Data if these are • factually incorrect; • incomplete. **Erasure** of Personal Data if • they are not or no longer relevant to the purpose for which they were collected/processed; • the Data Subject withdraws his Consent and there is no other Processing Basis for the Processing; • the Data Subject lodges an objection to the Processing and there are no compelling, justified grounds for the Processing or the Data Subject lodges an objection in cases for which the Processing takes place for the purpose of direct marketing; • these have been unlawfully processed; • these must be erased in order to comply with a legal obligation of TiU.

[21] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/what-your-details/my-rights

Rejection	In addition to the grounds for rejection referred to in **Section 10.2**, the request may be rejected if the Processing is necessary • for exercising the right to freedom of expression and information; • for the performance of a statutory duty of TiU or a task of public interest/the exercise of public authority of TiU; • for the public interest in the area of public health; • with a view to scientific research (See also **Thematic Policy on Scientific Research**); • for establishing, exercising, or defending a legal claim and the (preparation of) a judicial procedure.
Granting	In case of granting the rectification or erasure, this will be carried out.
Processing period	• Rectification: with immediate effect (without delay) • Erasure: without unreasonable delay
Information to other recipients	• If TiU has provided Personal Data to other recipients, TiU must inform them about the rectification or erasure of the Personal Data, unless this requires a disproportionate effort or turns out to be impossible. • If the Data Subject so requests, TiU must provide information about the other recipients.
Public information	If the Personal Data have been made public by TiU, TiU must make reasonable efforts to inform other Controllers of the request.
Person responsible	Rectification: the organizational unit that processes the data must also process rectifications. Erasure: see **Section 10.2**.

10.6. Right to Restriction

A Data Subject may demand that the Processing of his Personal Data be restricted, for example, in anticipation of the outcome of an objection. Restriction means that Personal Data will be marked and may not be edited or shared during this period. So this is not the same as erasing the data. See also **Section 10.2 for general guidelines**.

Request	The request must be made by means of the form **Request for Restriction of the Processing**[22].
Grounds	TiU is only obliged to comply with the request if: • the accuracy of the Personal Data is disputed by the Data Subject during a period that enables TiU to verify their accuracy; • the Processing is unlawful and the Data Subject request restriction instead of erasure; • the personal Data are not (or no longer) relevant for the purpose for which they were collected or are processed, but

[22] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/what-your-details/my-rights

	are necessary for the Data Subject to institute, exercise, or defend a legal claim. • the Data Subject has objected to the Processing, pending an answer to the question of whether the legitimate grounds of TiU outweigh those of the Data Subject.
Restriction period	The restriction shall be lifted as soon as the examination of the request to which the restriction relates has been completed.
Consequences	If the Processing is to be restricted, the Personal Data (with the exception of the storage) will only be processed • with the Data Subject's Consent, or • for the purpose of establishing, exercising, or defending a legal claim, or • to protect the rights of another (legal) person, or • for important reasons of public interest to the EU or to a Member State.
Person responsible	See Section 10.2.

10.7. Right to Data Portability

A Data Subject may request a copy of his Personal Data that is processed by TiU in a "structured, commonly used, and machine-readable format" so that he can easily transfer it to another service provider. This is referred to in the GDPR as the right to data portability. The Data Subject must not be hindered in this process. Therefore, no additional conditions may be imposed by TiU. See also **Section 10.2 for general guidelines**.

Request	The request must be made by means of the form **Request for Data Portability**[23].
Grounds	TiU is only obliged to comply with the request if: • the Processing is based on Consent or is necessary for the performance of an agreement; and • the Processing is carried out by means of automated procedures; thus the right exists only for automated Processing Operations and does not apply to occasional manual Processing Operations, for example.
Particulars	At the Data Subject's request and if technically possible, TiU must send the information directly to the other Controller.
Person Responsible	See Section 10.2

10.8. Right to Object

If a Data Subject objects to a Processing, TiU must investigate this further. See also **section 10.2 for general guidelines**.

[23] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/what-your-details/my-rights

Objection	The request must be made by means of the form **Objection to Processing Personal Data**.[24]
Grounds	TiU must discontinue the Processing as a result of an objection if • this takes place on the ground of the Processing Basis "Necessary for task of public interest/public authority" or "Necessary for representation of a legitimate interest." **Unless** TiU brings forward compelling justified grounds that outweigh the Data Subject's interests, rights, and freedoms or are connected with the establishment, exercise, or defense of a legal claim. **Exceptions**: • Processing for the purpose of direct marketing to which objection is made must always be discontinued (see the **thematic policy External Relations** • In the case of scientific research, the Data Subject will also have the right to object, unless the Processing is necessary for the performance of a task of public interest (see the sub-policies on Scientific Research).
Person responsible	See **Section 10.2.**

11. Accountability

11.1. Principle

The seventh principle from the GDPR is **Accountability** (Chapter III of the GDPR).

Tilburg University can demonstrate that it complies with the above obligations.

A major difference between the old privacy legislation and the GDPR is that the GDPR sets far more requirements for being able to demonstrate that the legislation is being complied with. For this reason, Accountability is included in the GDPR. On the basis of this obligation, TiU must be able to demonstrate that it complies with the privacy legislation, i.e., among other things, with all of the above. This means:

- **Security**: TiU takes appropriate technical and organizational security measures. This could include the pseudonymization and encryption of Personal Data, the use of a good password policy, and organizing authorizations but also the establishment of a procedure for the regular testing, assessment, and evaluation of the effectiveness of the security measures taken. (**Chapter 9**)
- **Privacy Statement**: TiU provides information about all processing activities on its website by means of a Privacy Statement (**Section 10.3**).

[24] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/what-your-details/my-rights

- **Data Protection Impact Assessment**: TiU conducts in specific situations a Data Protection Impact Assessment (DPIA) (also called Privacy Impact Assessment (PIA)) (**Section 11.2**).
- **Data Transfer Impact Assessment**: TiU conducts in specific situations a Data Transfer Impact Assessment (DTIA). (**Section 11.3**)
  Data Processing Register: TiU keeps a register of all processing activities and documents all additional information in accordance with the documentation obligation. (**Section 11.4**
-)
- **Data leaks**: Data leaks are reported to the Dutch Data Protection Authority (DPA) and, in some cases, to those involved in accordance with the DPA guidelines. (**Section 11.6**)
- **Data Protection Officer**: TiU has appointed a Data Protection Officer (**Strategy Data Protection**).
- **Codes of Conduct**: TiU subscribes to sector-specific codes of conduct.

It is important that in the event of changes or projects, the Protection of Personal Data is properly arranged, by design and by default, or **Privacy by Design** and **Privacy by Default**. This means that we have to do this carefully: for example, we have to properly adjust the authorizations when setting up or modifying systems and document them. This is guaranteed in a process-based way by, for example, Project Management and DPIA.

Finally, TiU must make sound (contractual) agreements if it collaborates with other parties with regard to the Processing of Personal Data (**Section 11.5**).

11.2. Data Protection Impact Assessment (DPIA) (Article 35 GDPR)

It is important that it is determined promptly whether there is an impact (risk) on Personal Data in projects or changes in the business operations/activities. This is to guarantee that sufficient measures are taken in good time to limit the risks for the Data Subjects. To determine this, a so-called Data Protection Impact Assessment must be carried out and recorded.
It is difficult for an organizational unit to assess whether a DPIA should be carried out for projects and research. Therefore, an estimate should already be made in the preparation phase as part of the Project Initiation Document (PID) and research application in the form of a so-called pre-DPIA in which an initial estimate is made as to whether a DPIA is necessary, or whether it does not need to be made. This will be based on a questionnaire.

Obligation determining whether a DPIA is necessary	A pre-DPIA must be drawn up and recorded in advance for each project and research. This should take place as early as possible in the project/research and will be based on a **questionnaire**[25] drawn up by the Data Protection Officer.[26]
Obligation for a Protection Impact Assessment (DPIA)	Performing a DPIA using the standard questionnaire during the design phase or when writing a research proposal is mandatory if one of the following criteria is met:

[25] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/careful-handling-personal-data/policy/models-and-procedures
[26] The Authority for Personal Data establishes a list of Processed Data for which a DPIA is mandatory. This list, if known, will be included in the questionnaire.

	• When assessing people on the basis of personal characteristics (making prognoses and profiling). • When making automated decisions, unless they have a minor/no impact on people. • In the case of systematic and large-scale monitoring (e.g., camera surveillance in publicly accessible areas). • When processing Special Personal Data, BSN, or other sensitive data such as financial data. • In the case of large-scale Data Processing, this can be assessed on the basis of the following criteria: a) the number of people whose data are processed, b) the amount of data and/or the variety of data processed, c) the duration of the data processing, d) the geographical scope of the data processing. • Linked databases. These are data sets that are either linked together or combined. For example, databases that arise from two or more different data processing operations with different purposes and/or are carried out by different persons responsible, in a way that the Data Subjects involved cannot reasonably expect. An example of this is Osiris, which is linked to Studielink etc. • Data on vulnerable persons. For the processing of this type of data, a DPIA may be necessary because of an unequal power relationship between the Data Subject and the Processing Responsible. As a result, Data Subjects are not free to give or refuse Consent to the Processing of their data. This may include, for example, employees, children, and patients. • Use of new technologies. • Blocking of a right, service, or contract. This is the case, for example, if TiU processes Personal Data in order to determine whether it can admit someone to contract education. The **DPIA procedure** must be followed. A DPIA is not mandatory if the intended Processing is not likely to present a high level of privacy risk or is very similar to another Processing for which a DPIA has already been carried out.
Model DPIA	The DPIA must be performed on the basis of the model established by the Data Protection Officer. This model shall include at least the following elements: • A systematic description of the intended Processing Operations, their purposes, and the Processing Basis. • An assessment of the necessity and proportionality of the Processing. This means: is the processing of Personal Data in this way necessary in order to achieve the objective? And is the invasion of the privacy of the

	Data Subjects not disproportionate in relation to this objective? • An assessment of the privacy risks for the Data Subjects. • The intended measures to (1) address the risks (such as safeguards and security measures) and (2) demonstrate compliance with the GDPR.
Responsible for the implementation of the DPIA	The person responsible for the process/project is responsible for the implementation of a DPIA. The Data Representative may facilitate on request.
Mandatory recommendations Data Protection Officer	After the person responsible has drawn up the DPIA, it is mandatory to consult the Data Protection Officer. He will render advice.
Audit Trail DPIA	All DPIAs performed must be recorded in accordance with the DPIA procedure.

This means that for new activities, projects, or research, the involvement of Personal Data must be considered in good time (at the design stage), and the impact of this must then be determined so that timely measures can be taken to safeguard the privacy risks of the Data Subjects. Much of the information that is collected in the context of a DPIA is also included in the Data Processing Register.

A number of examples of situations in which a DPIA must be performed are

- scientific research for which we are going to collect certain biometric information for the first time by means of wearables;
- a system with which we measure the number of students sitting in a lecture hall;
- a vitality program in which we want to measure the medical data of our staff members.

11.3. Data Protection Transfer Assessment (DTIA)

Personal data may be transferred to a country outside the European Economic Area (EEA) if appropriate safeguards are in place. What appropriate safeguards organisations can put in place follows from Chapter V of the General Data Protection Regulation (GDPR).

One of the most commonly used appropriate safeguards is the closure of SCCs.

Obligation Transfer Impact Assessment (DTIA)	The CJEU ruled July 2020 in case C311/1“ ("Schrems ”II") that the conclusion of an SCC is not sufficient. A risk analysis will have to be done for each transfer: a contractual agreement is no longer sufficient, especially if the legislation in the recipient country is not protective enough. This is also known as the Data Transfer Impact Assessment (DTIA). The DTIA must show why t46nonymizatioion uses a supplier based in a third country, and how it ensures that the privacy of data subjects is safeguarded.
Model DTIA	The DTIA includes at least the following elements: • Services The DTIA must contain a description of the services offered by the supplier based in a third country.

	• Appropriate safeguards What appropriate safeguards will be put in place? Consider the closure of SCCs or perhaps personal data will be transferred on the basis of Binding Corporate Rules. • Technica47nonymization47nal and contractual measures Not entirely unimportant, of course, is what measures are taken to protect personal data, in addition to the SCCs. Consider da47nonymizatioion, encryption and t47nonymization47onion or perha47nonymizationion of personal data. Another measure is for parties to contractually agree that personal data will be hosted within the EEA. • Legislation in the host country To arrive at a thorough DTIA, it is important to look at the national legislation of the suppl'er's country. It is virtually impossible to have knowledge of all laws and regulations. If you are using a US supplier, for example, the Foreign Intelligence Surveillance Act (FISA) plays an important role. Any ICT service provider based in the US is bound by FISA. One of its provisions states that a special court can order surveillance. Besides FISA, the USA Freedom Act also contains a variety of provisions on surveillance. • Risk assessment Ultimately, a risk assessment follows. Is the use of, say, a US supplier necessary? Or can a party based in Europe or perhaps even in the Netherlands be used? What risks are involved in the third country and are those risks acceptable?
Responsible for the implementation of the DTIA	The person responsible for the process/project is responsible for the implementation of a DTIA. The Data Representative may facilitate on request.
Mandatory recommendations Data Protection Officer	After the person responsible has drawn up the DTIA, it is mandatory to consult the Data Protection Officer. He will render advice.
Audit Trail DPIA	All DTIAs performed must be recorded in accordance with the **DTIA procedure**.

11.4. Data Processing Register (Article 30 of the GDPR)

One of the important elements with regard to accountability is the so-called Data Processing Register, which provides insight into which Personal Data are processed, together with the purpose limitation and lawfulness. This is mandatory under the GDPR for each Processing. The Data Processing Register shall be managed by the Central Privacy Officer and the Data Protection Officer and updated by the Data Representatives based on the information provided by the process owner.

Mandatory registration Processing Operations of Personal Data	Every structural Processing of Personal Data carried out by TiU (i.e., both Processing Operations for which TiU is (co-)responsible and Processing Operations for which TiU is Processor) must be recorded in a Data Processing Register. The record must be made in accordance with the **procedure Data Processing Register**.
Updating in case of changes	In the event of a change, the Data Processing Register must be updated. Changes are understood to include, for example, the adjustment of the processing purposes, the adjustment of the categories of Personal Data, the engagement of a Processor, and the adjustment of the storage period.
Responsible for registration	The person responsible for the process (system owner) is responsible for registering and updating the Data Processing Register.
Management of the Data Processing Register	The Central Privacy Officer and the Data Protection Officer monitor and direct the register. They determine which fields must be recorded.
Mandatory content Data Processing Register for the Controller	For each structural Processing for which TiU is the Controller, the Data Processing Register must at least contain • the name and contact details of TiU, the Data Protection Officer, and the organizational unit responsible for the Processing; • in the case of joint Controllers, the name(s) and contact details of the other Controller(s); • the processing purposes; • A description of the categories of Data Subjects and the categories of Personal Data; • The Processing Basis for the Processing; • which (groups of) employees have access to the Personal Data; • the categories of recipients to whom the Personal Data have been or will be provided, both internally and externally; • if applicable, transfers of Personal Data outside the EU, including an indication of the country or international organization to which the Personal Data will be provided and, if appropriate, the documents concerning appropriate safeguards; • whether there is a Processor, and if so, the data of the Processor and a copy of the Processing Agreement; • The presence and location of other relevant agreements; • if possible, the storage periods of the different categories of Personal Data; • if possible, a general description of the technical and organizational security measures; and • if applicable, the results of the DPIA carried out;. • if applicable, the results of the DTIA carried out.

Mandatory content Data Processing Register for Processor	In the event that TiU carries out the Processing as Processor, the Data Processing Register must contain at least • the name and contact details of TiU and the Data Protection Officer, the organizational unit responsible for the Processing, and the name(s) and contact details of the Controller(s); • the Processing Basis; • the categories of Processing Operations; • if applicable, transfers of Personal Data outside the EU, including an indication of the country or international organization to which the Personal Data will be provided and, if appropriate, the documents concerning appropriate safeguards; and • if possible, a general description of the technical and organizational security measures. • The presence and location of other relevant agreements;

This means that all Processing Operations of Personal Data must be registered in the Data Processing Register. This must be up to date at all times.

11.5. Agreement & Processing Agreement (Article 26–28 GDPR)

It is important that, if TiU and another organization exchange, provide, or receive Personal Data, proper contractual agreements are made in this context. For example, when you are going to use a program or app that is not managed by TiU and in which you are going to store Personal Data, or when you are housing an archive externally. Of course, it must also be checked whether the provision/disclosure of Personal Data is in line with all other principles as included in the GDPR and this Policy, now that it concerns a Processing Activity. See also **Section 4.5 on external disclosures and Section 6.5 on internal disclosures** and **Chapter 9 on security**.

What kind of agreement needs to be concluded depends on the role of TiU and the role of the other party (Controller, Processor, or Joint Controller). The Definitions include the legal descriptions of these roles.

Role	Explanation
Controller	This person determines the purpose and the means of the Processing.
Processor	This applies when an organization processes Personal Data on behalf of the Controller. This organization is not involved in determining the purpose and means of the Processing. In practice, a Processor often chooses its own means, but the final responsibility lies with the Controller. The Processor shall not use the data for its own purposes or for purposes other than those determined by the Controller. **Please note** that within an organization itself there are no Processors. This only applies when an external party is engaged to Process Personal Data. In some cases, TiU is also the Processor for another Controller, for example, for TIAS BV.

	***Example**: Outsourcing of the personnel administration of TiU (Controller) to an administrative office (Processor).*
Joint Controllers	This situation occurs when two or more Controllers jointly determine the purposes and means of the Processing. ***Example**: Occupational health and safety services: TiU provides some Personal Data of a sick employee to the occupational health and safety service and is, therefore, the Controller, the occupational health and safety service is the Controller responsible for opening the medical file and the obligation to store it, for example.*
Two separate, independent Controllers	When two or more Controllers each seperataly determine the purposes and means of the Processing. ***Example**: Sports association ,GGD, Tax Administration, auditor*

In order to determine the roles of the parties involved, the following questions can be helpful:

- Who decides on storage periods, disclosures, access request, etc.? This will be the Controller.
- Is it permissible for the party involved to store the data at the end of the agreement? A Processor may not do this. If a Processor intends to do so and is permitted to do so under privacy laws, then we speak of Joint or independent Controllers.
- Does the party involved use the data for its own purposes? This may only be done by a Controller. Again, if both parties use the data for their own purposes, we speak of Joint or independent Controllers.
- If a Processor nevertheless determines the purpose and means, he automatically becomes the Controller.

The following most common situations involve the following agreements:

Situation	Mandatory agreement
TiU is the Controller	Processing Agreement in accordance with an established model.
Tiu is Processor for another Contoller	Processing Agreement in accordance with an established model.
TiU is a Joint Controller	Arrangements in a (main) agreement or in a separate agreement on the division of responsibilities. Think of: • Who arranges the rights of the Data Subjects (Access, rectification, etc.), who provides information about the Processing (privacy statement) and, possibly, a redress scheme? • What are the parties involved allowed to do with the data and does confidentiality apply, for example?
Two separate Controllers	When personal data are provided to or received from another independent controller, a data transfer agreement should be concluded.

	***Example**: dataset external researcher, GGD, sports association.* If the Processing Basis is based on a statutory task or vital interest, TiU, as the Controller, may provide Personal Data to another Controller without this being based on a contractual agreement. However, the Disclosure of Personal Data must be carried out in a secure manner. ***Example**: Tax Administration, auditor, paramedic*
Transfer	For transfer (or Processing) of Personal Data outside the EU/EEA, an adequate level of protection must be guaranteed. A commonly used method is to enter into 'Standard Contractual Clauses (SCC).

Deviate from the model agreement	If the process owner wants to deviate from the model agreement, he can ask for advice from: • the Data Representative and Central Privacy Officer • the IT Security Officer/Chief Information Security Officer in the event of a deviation from the security standards set out in Appendix B of the Processing Agreement. • Legal Affairs (only mandatory if authorization by Executive Board is required) The process owner must provide a motivation to the director responsible as to why he deviates from the model agreement and inform the Central Privacy Officer and the Data Protection Officer of this. The agreement must be authorized by an authorized signatory.
Responsible for the realization and content of the agreement	The responsibility for concluding the agreement lies with the process owner, whereby the Data Representative can facilitate (support) this.
Registration/audit trail	The Agreement (including a motivation in case of a deviation) should be archived centrally (central register of contracts).

11.6. Data breaches

A Data breach is a breach of security as a result of which Personal Data is lost, can be seen unlawfully, or is processed unlawfully. Examples of (possible) data breaches are a lost USB stick on which Personal Data was stored, a stolen laptop or telephone, leaving examination results on the train, a hard drive that is discarded without properly erasing the research data on it, a virus on a computer that has access to Personal Data, a database being hacked, and an error on a website that shows person A's Personal Data to person B. Also think of an e-mail with a Personal Data file that is sent to a wrong recipient.

TiU is obliged to register data breaches and (in a number of cases) to report it to the Dutch Supervisory Authority. There is a short statutory deadline for this: the report must be made within 72 hours of the discovery. In some cases, TiU will also have to inform the Data Subjects about the data breach. In addition, it is important that we learn from data breaches and, where necessary, take measures to prevent data breaches or minimize the damage.

Duty to report (suspected) Data breach	Anyone working under the responsibility of TiU who knows or suspects that there is a (possible) Data breach must report this as soon as possible in accordance with the standard reporting procedure [27]. **Please note**: In case of doubt, always report internally.
Responsibility	• Every employee is personally responsible for reporting. • The Central Privacy Officer and Data Protection Officer are responsible for the analysis, registration, and possible notification to the Dutch Supervisory Authority.
Audit trail	All Data breaches are registered by the Central Privacy Officer and the Data Protection Officer.

For more information on Data breaches, reporting of such, and its handling see the **Data Breach Procedure and Protocol.**

11.7. Policy

Processing Personal Data is a continuous process. Technological and organizational developments within and outside TiU make it necessary to periodically review whether the university is still sufficiently on course regarding the Policy. Therefore, this Policy will be reviewed and revised every two years unless earlier revision is necessary on the basis of amended legislation and regulations or amended policy viewpoints.

11.7.1. Thematic policy

The following areas have been identified for which more detailed policies need to be developed.

Scientific Research	Further elaboration of the guidelines for the Protection of Personal Data in the context of Scientific Research
Education/Students	Further elaboration of the guidelines for the Protection of Personal Data in the context of Education and Students
External Relations	Further elaboration of the guidelines for the Protection of Personal Data in the context of management of External Relations (Marketing & communication and alumni)
Surveillance	Further elaboration of the guidelines for the Protection of Personal Data in the context of Surveillance

[27] https://www.tilburguniversity.edu/about/conduct-and-integrity/privacy-and-security/data-breach

Personnel	Further elaboration of the guidelines for the Protection of Personal Data in the context of Personnel

Part III: Responsibilities, Control, and Enforcement

12. Responsibilities

This Chapter includes the responsibilities with regard to the Protection of Personal Data within TiU. **Appendix 4** contains the so-called RASCI matrix, including for each component:

- ***R (Responsible)***: The person responsible for the implementation. He shall be accountable to the accountable person.
- ***A (Accountable/Ultimate Responsible)***: The person who is (ultimately) responsible and authorized and gives approval to the result. When it matters, he must be able to make the final judgement and have the right of veto. There is only one person accountable.
- ***S (Supportive)***: This person gives support regarding the result. He may facilitate and be asked for advice (no obligation).
- ***C (Consulted)***: This person (partly) gives direction to the result. He is consulted (mandatory) prior to decisions or actions. This is a two-way communication.
- ***I (Informed)***: Someone who is informed about the decisions taken, the progress made, the results achieved, etc. This is a one-way communication.

13. Monitoring and Enforcement

13.1. Monitoring

TiU monitors compliance with the GDPR and internal policy in various ways. TiU does this by means of the three-lines model, among other things.

First line: Responsible School/Division

The School/Division is responsible for compliance with regulations regarding Data Protection. This means, among other things,

- Structurally ensuring communication to employees about the correct application of the GDPR and TiU compliance policy;
- Adequate education and training of staff;
- Appointment of a Data Representative: first point of contact for questions related to privacy; and
- Control and monitoring of compliance with this Policy.

Second line: Central Privacy Officer

The Central Privacy officer is responsible for advising the organisation on privacy and protection of Personal Data. This means he will:

- Ensures training and awareness sessions for the various units;
- Advises organisational units;
- Participates in projects with privacy aspects;
- Participates in carrying out DPIAs.

Third line: Data Protection Officer and Internal Audit

The Data Protection Officer is responsible for monitoring compliance with legislation and regulations in the area of the protection of Personal Data. This means he:

- Reports periodically to the Supervisory Board and Executive Board;
- Provides solicited and unsolicited advice to the Supervisory Board, Executive Board and management;
- Performs checks on compliance with this policy by, among other things, drawing up a control plan containing the checks and monitoring to be carried out. In cooperation with the Governance, Risk & Compliance Officer, he reports the results in line with the **Risk & Control Charter**.

Internal Audit can carry out independent checks (audits) on compliance with this policy in line with the **Internal Audit Charter**.

13.2. Enforcement

If compliance with the protection of data and privacy details is seriously deficient, TiU can impose a sanction on the responsible employees involved within the framework of the Collective Labour Agreement (CLA) and the legal possibilities.

14. Policy Adoption

14.1. Decision-making

The Privacy & Personal Data Protection Policy is drafted by the Central Privacy Officer, consulting the Data Protection Officer. In the drafting process, the Central Privacy Officer has support from Policy Staff, the Marketing and Communications Department and the Data Protection Core Team if requested.

After consultation with the Data Protection Officer, the Policy is proposed for adoption by the Executive Board. After adoption, the following bodies/persons/organisational units are informed (in any case):

- Directors' consultations
- Executive Board & Deans consultation
- Data Representatives
- Research Data Office

14.2. Version Management

Version	Date	Content	Drawn up by	Validated	Adopted
1.0	May 2018	First version based on the GDPR	Working group	Goverance Risk Compliance Officer Data Protection Officer Legal Affairs	Executive Board (8-5-2018) University Council (8-6-2018)
1.1	January 2022	Minor change	Working group	Goverance Risk & Compliance Officer Central Privacy Officer	Data Protection Officer
1.2	March 2023	Modified RASCI Addition of DTIA, Privacy statement Reorganised chapters and minor changes	Data Protection Officer	Goverance Risk & Compliance Officer Central Privacy Officer	Executive Board (14-03-2023)

APPENDIX

APPENDIX 1: DEFINITIONS

Concept	Definition	Chapter
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.	11.5
Data Breach (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.	11.6
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.	11.4
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.	11.2

Data subject	An identified or identifiable natural person to whom personal data relates	
Data Transfer Impact Assessment (DTIA)	A risk assessment when transferring personal data to third countries that looks at service provision, technical, organisational and contractual measures, and the laws in the recipient country.	11.3
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 TiU, employees and students can also identify themselves with a driving license and the TiU 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
Policy	This Policy with regard to the processing of Personal Data at TiU, i.e., the TiU Privacy & Personal Data Protection Policy	11.7
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.	11.5
Processor agreement	The agreement between a controller and processor in which arrangements are made regarding the processing of Personal Data aiming to safeguard the data protection of the data subject (Article 28, Section 3 GDPR).	11.5
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 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 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 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	10.6

	also clear to recipients of the Personal Data. If the restriction is lifted again, the data subject must be informed accordingly (Article 18 GDPR).	
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	4.5 11.5

APPENDIX 2: PRINCIPLES PROTECTION PERSONAL DATA

This Appendix contains the basic principles for the protection of Personal Data.

LAWFULNESS
(Article 6 GDPR)
TiU shall only process Personal Data if this is lawful.
	• TiU lawfully processes Personal Data if
	  ○ the Data subject has given permission for the Processing of the Personal Data for one or more specific purposes, or
	  ○ processing is necessary for the performance of an agreement to which the Data subject is a party or for the purpose of concluding an agreement, or
	  ○ processing is necessary to comply with a legal obligation applicable to TiU, or
	  ○ processing is necessary to protect the vital interests of the Data Subject or other individual, or
	  ○ processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority assigned to TiU, or
	  ○ processing is necessary for the representation of the legitimate interests of TiU or of a third party, except where the interests or fundamental rights or freedoms of the persons whose personal data are processed outweigh those interests, particularly when the Data Subject is a child.
	• TiU will not process any Special Personal Data unless there is an exception as referred to in the GDPR (Article 9).
	• In principle, TiU will not pass on Personal Data to third countries or international organizations unless there is an adequate level of protection (Chapter V of the GDPR).

PURPOSE LIMITATION **(Article5(1) (b) GDPR)** **TiU will only process Personal Data if there is a legitimate purpose.**	• TiU will only process Personal Data if: ○ TiU it is clear about why and how Personal Data is processed: there is a specific, explicitly stated, and legitimate purpose. • TiU guarantees that if Personal Data are used for a purpose other than that for which they were collected, this new Processing also meets the requirements. In doing so, TiU will take into account that further Processing with a view to scientific research will not be considered incompatible with the original objective.

DATA MINIMIZATION **(Article 5(1) (c) GDPR)** **TiU guarantees that Personal Data are adequate, relevant, and not excessive in relation to the purpose(s) for which they were collected.**	• TiU does not process more Personal Data than is necessary in relation to the purpose (data minimization). • TiU guarantees that it processes the minimum necessary Personal Data to realize a correct picture of the Data Subject. • If possible, TiU will Anonymize or Pseudonymize the Personal Data. • TiU does not store Personal Data for longer than is necessary for the purpose for which it was processed or for which there is a statutory storage period.
ACCURACCY **(Article 5(1) (cd GDPR)** **TiU guarantees on the basis of reasonableness that the Personal Data are accurate.**	• TiU will take all reasonable steps to guarantee that the Personal Data is accurate and will update/erase these if necessary.
SECURITY **(Article 32 GDPR)** **TiU shall take appropriate technical and organizational measures against unauthorized and unlawful processing of Personal Data and against the accidental loss, erasure, or damage of Personal Data.**	• TiU has set up the organization of information security in such a way that it is suitable for the Personal Data that is being processed. It shall mainly take the risks into account, in particular those resulting from accidental or unlawful destruction of, loss of, alteration of, unauthorized disclosure of, or access to the data processed. • TiU guarantees the foregoing with adequate procedures and guidelines and well-trained personnel. • TiU has clearly laid down who is responsible for information security. • TiU has set up a system that ensures that information security incidents are followed up quickly and effectively.

RIGHTS OF THE DATA SUBJECT
(Chapter III of the GDPR)
TiU guarantees that action will be taken in line with the rights of the individual whose Personal Data TiU processes.
	• TiU informs the Data Subject about the Processing and provides the information in accordance with Article 13 or 14 of the GDPR.
	• TiU will provide access to the Personal Data at the Data Subject's request.
	• TiU will rectify incorrect Personal Data at the Data Subject's request.
	• TiU will erase Personal Data at the Data Subject's request if this is permitted by law.
	• TiU guarantees the Data Subject's right to data portability.
	• TiU will deal with objections by the Data Subject as referred to in Article 21 of the GDPR (if the Processing is based on "task of public interest" or "necessary for the representation of legitimate interest" or in the case of direct marketing) in accordance with Article 21 of the GDPR.
	• TiU will comply with the obligations of the Telecommunications Act, which means that in the case of direct marketing:
	  ○ Only persons who have given specific permission will be approached;
	  ○ It is guaranteed that persons who have not given their consent or who have withdrawn it are not or no longer approached.

ACCOUNTABILITY
TiU can demonstrate that it meets the above obligations.
	• TiU keeps a register of all processing activities, and it documents all additional information in accordance with the documentation requirement.
	• TiU protects data by privacy by design and privacy by default.
	• TiU carries out a Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (PIA) in specific situations.
	• TiU shall take appropriate technical and organizational security measures. This could include the pseudonymization and encryption of Personal Data, the use of a good password policy and the setting up of authorizations but also the establishment of a procedure for the regular testing, assessment, and evaluation of the effectiveness of the security measures taken.
	• Data Leaks are reported to the DPA and, in some cases, to those involved, in accordance with the DPA guidelines.
	  • TiU has appointed a Data Protection Officer.
	  • TiU subscribes to sector-specific codes of conduct.

APPENDIX 3: PURPOSES FOR PROCESSING

Category	Purposes of processing
Students, Prospective students (prospects), Contract students, Participants	1. The enrollment for education; 2. the organization or provision of education, guidance (in education or careers), or the provision of study advice; 3. disclosure or provision of information and communication with the Data Subjects about the institution's products and services; 4. disclosure of 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 payments 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 statutory provisions; 9. the granting of electoral rights in the context of participation; 10. immigration purposes (contributing to or making it possible for (future) students to travel to the Netherlands).
Former students (alumni)	1. Maintaining contacts with former students, including former members of alumni associations; 2. disclosure or provision of information and communication with data subjects about the institution's products and services; 3. disclosure of the activities of the institution or its partners; 4. keeping a record of the information transmitted; 5. calculating, recording, and collecting contributions and gifts.
Staff members Temporary workers Contracted personnel	1. The treatment of human resources; 2. personnel and payroll administration; 3. managing the activities of the Data Subject; 4. the implementation of terms and conditions of employment; 5. the determination and payment of salary entitlements, allowances and other sums and remuneration in kind to or for the benefit of the Data Subject;

	6. calculating, recording, and paying taxes and premiums on behalf of the Data Subject; 7. arranging claims to benefits in connection with the termination of employment; 8. the occupational medical care for the Data Subject; 9. staff welfare; 10. the election of the members of a representative body regulated by law; 11. internal control and operational security; 12. the drawing up of a list of dates of the birthdays of the Data Subject and other celebrations and events; 13. the granting of discharge; 14. the administration of the employee association and of the association of former employees; 15. maintaining contact with the employer of the Data Subject; 16. dealing with disputes and arranging for audits to be carried out; 17. the collection of claims, including the collection of those claims from third parties 18. training of the Data Subject; 19. the transfer of the Data Subject or his/her temporary assignment to another part of the group, as referred to in Section 2:24b of the Dutch Civil Code to which the responsible party is subject; 20. the implementation or application of statutory provisions; 21. records management; 22. performing scientific, statistical, or historical research.
Former employees	1. Maintaining contacts with Data Subject; 2. dealing with disputes and arranging for audits to be carried out; 3. implementing or applying statutory provisions.
Applicants	1. The assessment of the suitability of the Data Subject for a post that is or may become vacant; 2. the settlement of the expenses incurred by the applicant; 3. internal control and operational security; 4. the implementation or application of statutory provisions.
PhD candidates (not being employees)	1. Obtaining a PhD; 2. providing guidance in the context of obtaining a PhD;

	3. the implementation or application of statutory provisions; 4. dealing with disputes and arranging for audits to be carried out.
Respondents in the context of scientific research	1. Performing scientific research as referred to in the Dutch Higher Education and Research Act and the Nehterlands Code of Conduct for Academic Practice; 2. the recording of consent to participate in scientific research; 3. the implementation or application of statutory provisions or regulations on the basis of applicable codes of conduct; 4. dealing with disputes and arranging for audits to be carried out.
Subscribers, members (e.g., Library, Sports Centre)	1. Execution of the agreement/subscription; 2. the transmission of information for the benefit of the Data Subject; 3. the calculation, recording, and collection of subscription fees, including the transfer of claims to third parties and other internal management activities; 4. dealing with disputes and arranging for audits to be carried out.
Debtors/creditors	1. Calculating and recording income and expenditure; 2. making payments or collecting claims, including placing them in the hands of third parties; 3. dealing with disputes and arranging for audits to be carried out; 4. maintaining contacts between the responsible party and the debtors and creditors; 5. the implementation or application of statutory provisions.
Suppliers	1. Calculating and recording income and expenditure and making payments; 2. the collection of claims, including the collection of such claims by third parties and other internal management activities; 3. maintaining contacts by the responsible party with the customers or suppliers; 4. dealing with disputes and arranging for audits to be carried out.
Other contacts	1. Maintaining contacts.

APPENDIX 4: RESPONSIBILITIES

Task	Part	Deliverable	Accountable[28]	Responsible[29]	Supportive[30]	Consulted[31]	Informed[32]
Monitoring laws and regulations		Legal Advice	• Legal Affairs	• Legal Affairs • Central Privacy Officer		• Data Protection Officer	• Goverance Risk & Compliance Officer
Definition of Personal Data Protection Strategy		Data Protection Strategy	• Executive Board	• Core team Protection Personal data	• Policy Officer • Communications Officer	• Data Protection Officer	• Directors' meetings • Executive Board and Deans Consultations • Data Representatives • Research Data Office
Definition of Personal Data Protection Policy		Privacy & Personal Data Protection Policy	• Executive Board	• Central Privacy Officer	• Policy Officer • Communications Officer • Core team Protection Personal data	• Data Protection Officer • Goverance Risk Compliance Officer • CISO and ITSO	• Directors' meetings • Executive Board and Deans Consultations • Data Representative • Research Data Office
Definition of thematic, Division, or School Policy		Thematic Policy/ Division policy or School policy	• (vice-) Dean School or Division Director	• Data Representative	• Policy Officer • Communications Officer	• Data Protection Officer • Central Privacy Officer	• In case of essential change • Education Portfolio Holders' meeting

[28] ***Accountable***: The person who is (ultimately) responsible, authorized, and gives approval to the result. When it matters, he must be able to make the final judgement and have the right of veto. There is only one person Accountable.

[29] ***Responsible***: The person responsible for the implementation. He shall be accountable to the accountable person.

[30] ***Supportive****:* This person gives support regarding the result. They may facilitate and be asked for advice (no obligation).

[31] ***Consulted*** This person (partly) gives direction to the result. He is consulted (mandatory) prior to decisions or actions. This is a two-way communication.

[32] ***Informed***. Someone who is informed about the decisions taken, the progress made, the results achieved, etc. This is a one-way communication.

Task	Part	Deliverable	Accountable[28]	Responsible[29]	Supportive[30]	Consulted[31]	Informed[32]
						• Goverance Risk Compliance Officer •	• Research Portfolio Holders' meeting • Participation body
• Carry out DPIA & DTIA	Carry out Pre-DPIA	Pre-DPIA	• Process owner/ system owner	• Process owner/ system owner	• Central privacy Officer	• Data Representative • Data Steward • Data Protection Officer	
	Carry out DPIA	Data Protection Impact Assessment	• Process owner/ system owner	• Process owner/ system owner • Data Representative	• Central privacy Officer • Chief Information Security Officer • Information Security Officer • IT Security Officer	• Data Protection Officer	
	Carry out DTIA	Data Transfer Impact Assessment	• Process owner/ system owner	• Process owner/ system owner • Data Representative	• Central privacy Officer • Chief Information Security Officer • Information Security Officer • IT Security Officer	• Data Protection Officer	
Logging Processing data Personal data		Data Processing Register	• Process owner/ system owner	• Information manager or functional manager		• Data Representative	• Central privacy Officer • Data Protection Officer

Task	Part	Deliverable	Accountable[28]	Responsible[29]	Supportive[30]	Consulted[31]	Informed[32]
Closing Processing Agreement with regard to the protection of personal data	Processing Agreement	Standard model	• Process owner/ system owner[33]	• Information manager or functional manager		• Data Representative	• Central Privacy Officer • Data Protection Officer
		Customised standard model or supplier model	• Process owner/ system owner[34]	• Information manager or functional manager	• Legal Affairs	• Data Representative • Centrale Privacy Officer • Legal Affairs[35] Security standards: • Chief Information Security Officer • Information Security Officer • IT Security Officer	• Data Protection Officer
	Other Agreements	Data exchange agreement, Joint controller Agreement, Standard Contractual Clauses, et cetera	• Process owner/ system owner[36]	• Information manager or functional manager	• Legal Affairs	• Data Representative • Centrale Privacy Officer • Legal Affairs[37] • Security standards: • Chief Information • Security Officer	• Data Protection Officer

[33] Authority to sign in accordance with the mandate regulations
[34] Authority to sign in accordance with the mandate regulations
[35] Only mandatory in case of authorization Executive Board
[36] Authority to sign in accordance with the mandate regulations
[37] Only mandatory in case of authorization Executive Board

Task	Part	Deliverable	Accountable[28]	Responsible[29]	Supportive[30]	Consulted[31]	Informed[32]
						• Information Security Officer • • IT Security Officer	
Advising on the Protection of Personal Data	Executive Board & Supervisory Council	Advice	• Data Protection Officer	• Data Protection Officer	• Central Privacy Officer • Governance Risk & Compliance Officer		• Central Privacy Officer • Governance Risk & Compliance Officer
	School or Division		• Data Representative	• Data Representative	• Central Privacy Officer • Governance Risk & Compliance Officer		• Data Protection Officer
			• Central Privacy Officer	• Central Privacy Officer			• Data Protection Officer
			• Data Protection Officer	• Data Protection Officer			• Central Privacy Officer
Rights Data Subjects	Access Rectification Erasure Restriction Portability	Respons	• Process owner/ system owner	• Process owner/ system owner		• Data Representative	• Central Privacy Officer • Data Protection Officer
	Objection	Decision	• Process owner/ system owner	• Process owner/ system owner	• Legal Affairs	• Data Representative • Central Privacy Officer	• Data Protection Officer

Task	Part	Deliverable	Accountable[28]	Responsible[29]	Supportive[30]	Consulted[31]	Informed[32]
	Complaint	Advice	• Data Protection Officer	• Data Protection Officer			
Reporting data breach	Internally	Internally Reported data breach	• All employees	• All employees		• Central Privacy Officer • Data Protection Officer	
	Analyzing data breach, registering internally, defining improvement measures, advice	Data breach report	• Central Privacy Officer • Data Protection Officer	• Central Privacy Officer • Data Protection Officer	• Data Representative • Governance Risk & Compliance Officer • Chief Information Security Officer • Information Security Officer • IT Security Officer	• Notifier data breach	• Executive Board (high impact) • Directors' meeting (high impact) • Director/Dean/Management (medium impact) • Data Representative • Notifier data breach (case)
	Externally – Data Protection Authority	Report data breach to DPA	• Director School or Division	• Central Privacy Officer • Data Protection Officer			• Executive Board (high impact) • Directors' meetings (high impact) • Director (medium impact)
	Informing Data Subjects	Information letter	• Director School or Division	• Staff member division/school to be appointed	• Data Representative		• Central Privacy Officer • Data Protection Officer
Privacy Statements		Privacy Statement	• Process owner/ system owner	• Process owner/ system owner	• Data Representative	• Central Privacy Officer • Data Protection Officer	

Task	Part	Deliverable	Accountable[28]	Responsible[29]	Supportive[30]	Consulted[31]	Informed[32]
Raising awareness		Awareness – knowledge about Protection of Personal Data	• Executive Board • Director School or Division	• Data Representative • Central Privacy Officer • Data Protection Officer	• Human Resources • Legal Affairs • Marketing & Communication • Goverance Risk & Compliance Officer • Information Security Officer		
Organizing training and education Protection of Personal Data	Data Represen-tatives	Training	• Director US	• Central Privacy Officer	• Goverance Risk & Compliance Officer • Data Protection Officer		
	Other members of staff		• Directors Schools & Divisions	• Director US & Director LIS	• Data Representative • Central Privacy Officer • Information Security Officer	• Data Representative	• Data Protection Officer
Monitoring and checks on compliance with legislation and regulations		Monitoring report	• Data Protection Officer	• Data Protection Officer	• Central Privacy Officer	• Goverance Risk & Compliance Officer	
		Dashboard	• Data Protection Officer	• Data Protection Officer	• Central Privacy Officer	• Goverance Risk & Compliance Officer	• Executive Board • Supervisory Council
		Annual report Annual plan Supervisory agenda	• Data Protection Officer	• Data Protection Officer	• Central Privacy Officer	• Goverance Risk & Compliance Officer	• Executive Board • Supervisory Council • Directors' meeting

Task	Part	Deliverable	Accountable[28]	Responsible[29]	Supportive[30]	Consulted[31]	Informed[32]
							• Computerisation and Automation Steering Group • Data Representative