Procedure agreements concerning the processing of personal data

Purpose

When an external party is involved in the processing of personal data, it should be assessed whether provisions need to be made in an (additional) agreement. This document describes the procedure for this assessment.

Introduction

If Tilburg University engages or cooperates with an external organization for the processing of personal data, agreements must be made regarding this processing on the basis of the General Data Protection Regulation (GDPR), in particular with regard to responsibilities and security. These provisions must be laid down in an agreement, for example a processor agreement or a joint controllership agreement. Tilburg University has models available for these agreements, based on SURF models. For more details we refer to the **Privacy & Personal Data Protection Policy - section 11.5**.

Basic procedure

Regardless of the form in which additional provisions are made to process personal data, the two steps below should be completed first. From there, proceed with the applicable procedure.

Step	What
0	Check with the Information Manager and Data Representative whether the following needs to be addressed: • Perform a check on the technical and organizational security requirements. To do so, follow the **Security Check process flow** and accompanying explanation, which can be found on the procedures and models page of Privacy & Security. • Explore whether a connection with SURFconext is possible. SURFconext lets users access a web application with ones Tilburg University account. For more details, see the SURFconext on the procedures and models page of Privacy & Security (only available in Dutch).
1	Based on the division of roles, determine whether and, if so, what type of agreement is necessary. See **Annex I** for a flowchart for this purpose and **Annex II** for examples. It is advisable to consult the Data Representative of your organizational unit. - If a **processor agreement** is required, proceed with the next step set out under ‘Procedure processor agreement’. - If **multiple parties are controllers** and it is preferred to lay down the necessary provisions in a **supplementary agreement**, proceed with the next step set out under ‘Procedure supplementary agreement’. - If **multiple parties are controllers** and it is preferred to lay down the **additional provisions in the main agreement**, proceed with the next step set out under ‘Procedure additional provision in main agreement’. - If no agreement or additional provisions are necessary, the procedure ends here.

Procedure processor agreement

The procedure below describes a step-by-step plan for the process owner to, in collaboration with the Information Manager, conclude a processor agreement.

Step	What
2	Check whether a processor agreement is already concluded with the party concerned. If a processor agreement is already in place, check whether this agreement is up-to-date and whether the new processing activity falls within the scope of the existing agreement. If so, the procedure ends here. If not, proceed with step 3.
3	In collaboration with the Information Manager of the School/Division or Project Manager, determine who is involved on behalf of Tilburg University: • Who is ultimately responsible (usually the divisional director or dean)? • Who is authorized to sign (power of attorney)? • Who is contract manager within the School/Division (agreement owner)? → If necessary, contact Procurement & Contract Management for advice • Who will carry out the contract negotiations? Also determine who is authorized to sign the agreement on behalf of the other party.
4	Use the latest Tilburg University **model for the processor agreement**, which can be found at on the procedures and models page of Privacy & Security. If you can't help but deviate from this model (for example by using the model of a large supplier, or substantive modifications of the Tilburg University model): • Prepare an analysis of the deviations with the Data Representative and the Information Manager of the School/Division. Use the checklist in **Annex III** for this. • Do you still have questions? In that case, the Data Representative can ask the Privacy & Security working group (privacysecurity@tilburguniversity.edu) for advice: • All articles with the exception of the ones listed below: Central Privacy Officer • Article 5: Information Security Team (who may further coordinate internally with the Chief Information Security Officer) • Article 6: Information Security Team (who may further coordinate internally with the Chief Information Security Officer) • Article 10: Legal Affairs and Central Privacy Officer • Annex A: coordinate with Information Manager • Annex B: Information Security Team The process owner should have the responsible director motivate why he deviates from the model agreement and inform the Data Protection Officer in a timely manner about this.[1]
5	Fill in any processing-specific fields in the agreement (in Tilburg University model: the Annexes and the yellow shaded fiels in the agreement) in cooperation with the processor. The Information Manager and/or the Data Representative of the School or Division should be able to help.

[1] In case of a deviation from the model agreement, it is possible that Tilburg University is at risk. It is important that the deviation is done consciously and that the reason for this is recorded in a motivated way so that this is also clear afterwards.

6	Have the processor agreement signed by the authorized representative.
7	Have the Information Manager archive the agreement together with the meta data in Proactis (distribution via email to contractmanagement@uvt.nl).

Procedure supplementary agreement

The procedure below applies to the situation in which there is a processing of personal data where multiple parties are controllers and the provisions are going to be laid down in a separate, supplementary agreement. There are two situations possible. For the situation of joint controllership, the available model agreement can be used (joint controllership agreement). For the situation where two or more parties are independent controllers, a data sharing, data transfer or research data agreement can be concluded.

Step	What
2	Check whether the necessary supplementary agreement is already concluded with the party(ies) concerned. If an agreement is already in place, check whether this agreement is up-to-date and whether the new processing activity falls within the scope of the existing agreement. If so, the procedure ends here. If not, proceed with step 3.
3	In collaboration with the Information Manager of the School/Division or Project Manager, determine who is involved on behalf of Tilburg University: • Who is ultimately responsible (usually the divisional director or dean)? • Who is authorized to sign (power of attorney)? • Who is contract manager within the School/Division (agreement owner)? → If necessary, contact Procurement & Contract Management for advice • Who will carry out the contract negotiations? Also determine who is authorized to sign the agreement on behalf of the other party(ies).
4	Use the latest Tilburg University model for the necessary agreement. The **model for the joint controllership agreement** can be found on the procedures and models page of Privacy & Security. **Models of research agreements** can be found on the Research Support Portal. If a model is available, but you can't help but deviate from this model (for example by using the model of a large supplier, or substantive modifications of the Tilburg University model): • Prepare an analysis of the deviations with the Data Representative and the Information Manager of the School/Division. Use the checklist in **Annex IV** for this. • Do you still have questions? In that case, the Data Representative can ask the Privacy & Security working group (privacysecurity@tilburguniversity.edu) for advice.

	The process owner should have the responsible director motivate why he deviates from the model agreement and inform the Data Protection Officer in a timely manner about this.[2]
5	Fill in any processing-specific fields in the agreement in cooperation with the other party(ies). The Information Manager and/or the Data Representative of the School or Division should be able to help.
6	Have the processor agreement signed by the authorized representative.
7	Have the Information Manager archive the agreement together with the meta data in Proactis (distribution via email to contractmanagement@uvt.nl).

Procedure additional provision in main agreement

The procedure below applies to the situation in which there is a processing of personal data where multiple parties are controllers (individually or jointly) and the parties wish to include the additional provisions in the main agreement. This will mainly be the case when the processing of personal data plays a very limited role in the performance of the agreement and only a few main points need to be agreed upon in this regard.

Step	What
2	Check whether the necessary supplementary agreement is already concluded with the party(ies) concerned. If an agreement is already in place, check whether this agreement is up-to-date, whether the new processing activity falls within the scope of the existing agreement, whether the agreement contains provisions regarding the processing of personal data and, finally, whether these provisions are adequate. If so, the procedure ends here. If not, proceed with step 3.
3	In collaboration with the Information Manager of the School/Division or Project Manager, determine who is involved on behalf of Tilburg University: • Who is ultimately responsible (usually the divisional director or dean)? • Who is authorized to sign (power of attorney)? • Who is contract manager within the School/Division (agreement owner)? → If necessary, contact Procurement & Contract Management for advice • Who will carry out the contract negotiations? Also determine who is authorized to sign the agreement on behalf of the other party(ies).
4	In collaboration with the Data Representative, determine what issues require additional provisions in the main agreement. Consider: • Statement to work in accordance with the GDPR and other relevant legislation; • Agreements on purpose limitation (personal data may in principle only be used for predetermined purposes); • Provision of information to the data subjects; • Responsibility for handling requests regarding the rights of data subjects; • Data transfer to third countries; • Taking appropriate security measures;

[2] In case of a deviation from the model agreement, it is possible that Tilburg University is at risk. It is important that the deviation is done consciously and that the reason for this is recorded in a motivated way so that this is also clear afterwards.

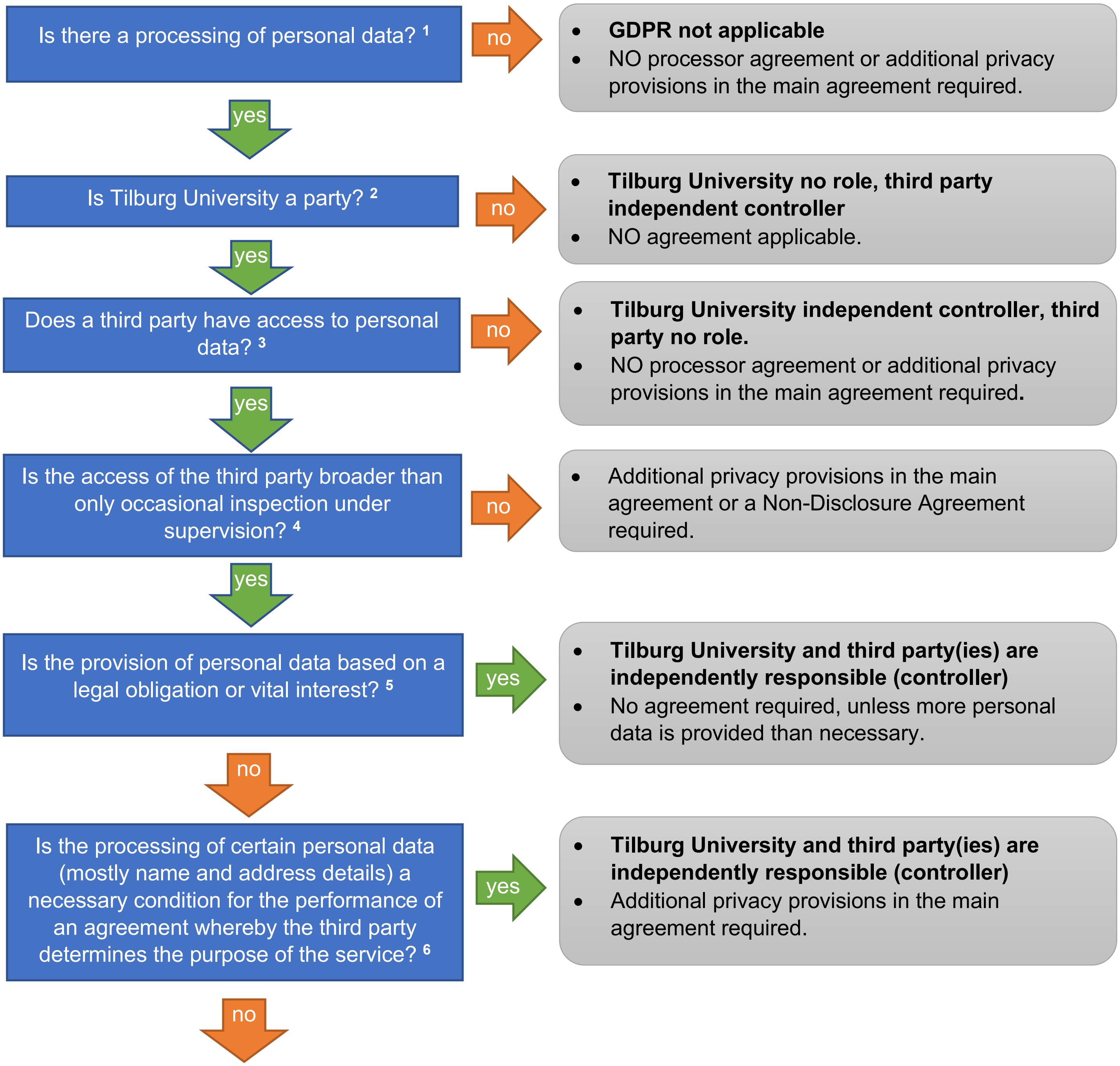
	• Dealing with data breaches Do you still have questions? In that case, the Data Representative can ask the Privacy & Security working group (privacysecurity@tilburguniversity.edu) for advice.
5	Have the agreement signed by the authorized representative.
6	Have the Information Manager archive the agreement together with the meta data in Proactis (distribution via email to contractmanagement@uvt.nl).

Annex I: Determine role division

An external party is a processor if Tilburg University determines the purpose (and means) of the data processing performed by that external party.

It is also possible that Tilburg University is a processor for an external party. In both cases, Tilburg University must conclude a processor agreement. In addition, there is the situation where there is a processing of personal data involving two or more controllers. What type of agreement must be concluded depends on the roles of the parties (processor, jointly or independently responsible).

The flow chart below helps you determine the roles.



Is there a processing of personal data? [1]

no

- **GDPR not applicable**
- NO processor agreement or additional privacy provisions in the main agreement required.

yes

Is Tilburg University a party? [2]

no

- **Tilburg University no role, third party independent controller**
- NO agreement applicable.

yes

Does a third party have access to personal data? [3]

no

- **Tilburg University independent controller, third party no role.**
- NO processor agreement or additional privacy provisions in the main agreement required**.**

yes

Is the access of the third party broader than only occasional inspection under supervision? [4]

no

- Additional privacy provisions in the main agreement or a Non-Disclosure Agreement required.

yes

Is the provision of personal data based on a legal obligation or vital interest? [5]

yes

- **Tilburg University and third party(ies) are independently responsible (controller)**
- No agreement required, unless more personal data is provided than necessary.

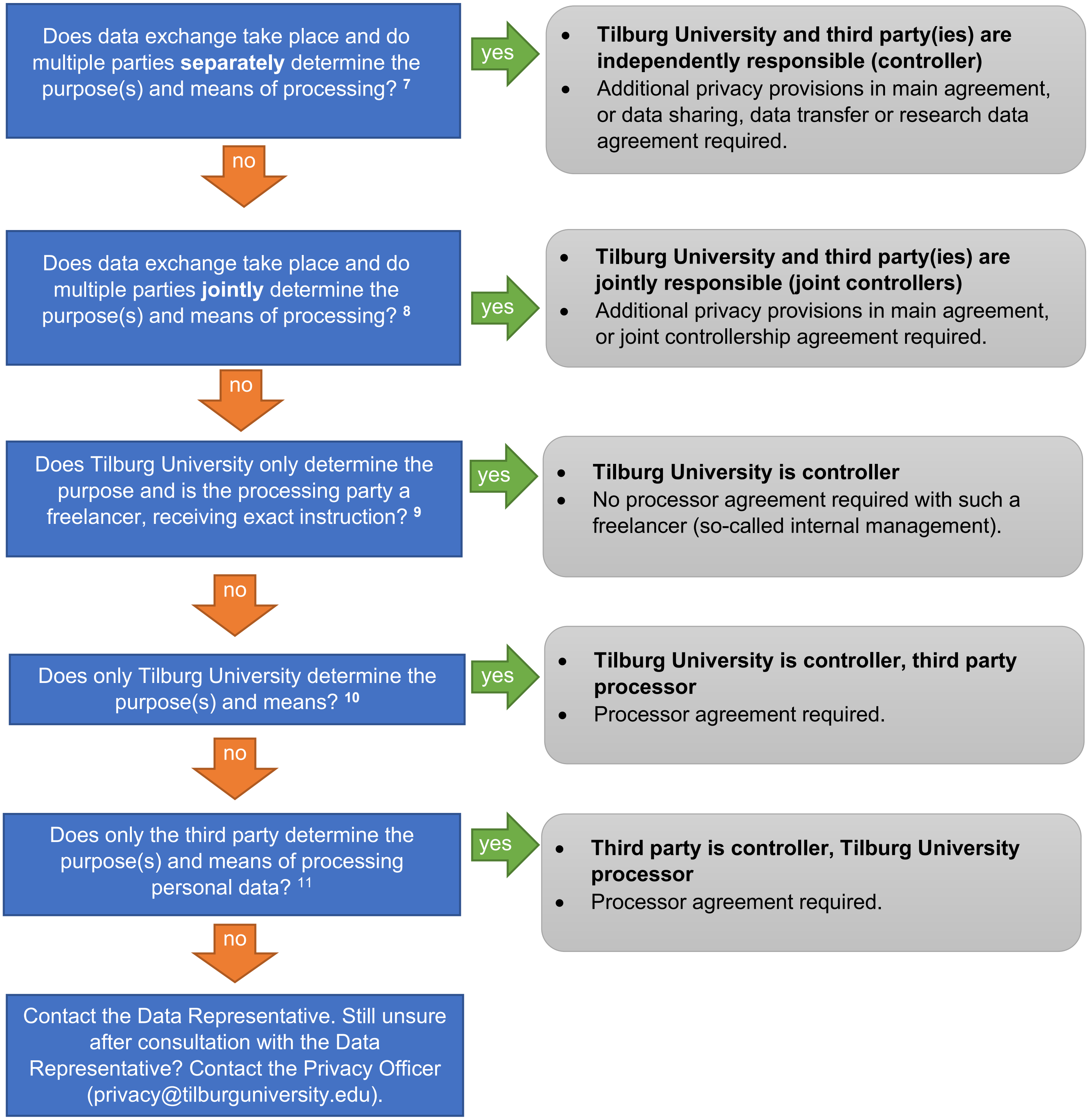
no

Is the processing of certain personal data (mostly name and address details) a necessary condition for the performance of an agreement whereby the third party determines the purpose of the service? [6]

yes

- **Tilburg University and third party(ies) are independently responsible (controller)**
- Additional privacy provisions in the main agreement required.

no



Does data exchange take place and do multiple parties **separately** determine the purpose(s) and means of processing? [7]

- **Tilburg University and third party(ies) are independently responsible (controller)**
- Additional privacy provisions in main agreement, or data sharing, data transfer or research data agreement required.

Does data exchange take place and do multiple parties **jointly** determine the purpose(s) and means of processing? [8]

- **Tilburg University and third party(ies) are jointly responsible (joint controllers)**
- Additional privacy provisions in main agreement, or joint controllership agreement required.

Does Tilburg University only determine the purpose and is the processing party a freelancer, receiving exact instruction? [9]

- **Tilburg University is controller**
- No processor agreement required with such a freelancer (so-called internal management).

Does only Tilburg University determine the purpose(s) and means? [10]

- **Tilburg University is controller, third party processor**
- Processor agreement required.

Does only the third party determine the purpose(s) and means of processing personal data? [11]

- **Third party is controller, Tilburg University processor**
- Processor agreement required.

Contact the Data Representative. Still unsure after consultation with the Data Representative? Contact the Privacy Officer (privacy@tilburguniversity.edu).

1 This should be interpreted broadly: Tilburg University provides personal data, the data subject (e.g. student, employee, research respondent) creates their own login account, the data subject or third party enriches the data collection.
If only a general authorization is passed on via a Tilburg University authentication method

(e.g. SSO / AD / SurfConext), there is no processing of personal data with the third party. At the moment more attributes are passed on (e.g. user name, email address), it is considered to be processing of personal data.

2 This is the case if there is an underlying agreement, or if Tilburg University prescribes the application/service. This may also include the situation in which the use of an application is promoted, for example, in the situation that it is said that a certain application can be used to conduct surveys or process data sets whereby conducting the surveys or processing data sets is part of an assignment, paper, thesis or research.

3 Example: if Tilburg University hosts the application itself and the third party **does not** provide incidental or structural management where they have access to non-anonymized data, then the third party does not have access to personal data.

4 If a third party performs incidental management in a database/application under the supervision of Tilburg University and (possibly) has access to personal data, there should be an agreement serving as a legal basis for this service (for example an agreement that relates to the delivery of an application). Provisions on the processing of personal data (including incidental inspection) should then have been made in that agreement.

5 Legal obligations are explicitly described in legislation. Examples are claims of the Public Prosecutor (126nd paragraph 1 of the Dutch Code of Criminal Procedure), IND, DUO, Tax Authorities, NVAO (WHW accreditation). An example of “vital interest” is providing medical data about a victim to ambulance service.

6 Example is to provide the name and address of employees to third parties for the delivery of goods (florist, provider of Christmas gifts, etc.) or a self-employed worker (freelancer or in Dutch: “ZZP’er”) who receives no instructions and where the primary assignment does not concern the processing of personal data.

7 Data exchange does take place, but parties do not work together towards a specific goal. For example: data exchange with another university as part of a research project without the research project being a joint effort.

8 For example in joint research projects.

9 Tilburg University allows the processing of personal data by a self-employed worker (freelancer or in Dutch: “ZZP’er”) that works under the instruction of Tilburg University with feedback of enriched personal data.

10 Tilburg University outsources the processing of personal data to a third party and the third party may only process the personal data on behalf of Tilburg University. They may not use the personal data for purposes not agreed in the processor agreement. For example the outsourcing of the payroll administration, the hosting of applications or the primary processing of personal data.

11 Tilburg University takes care of the processing of personal data for another organization, for example hosting of third-party applications, providing network facilities, account management for affiliated institutions such as TIAS.

If you have questions about the role division, contact your Data Representative. Should you have any doubts about your assessment, the Data Representative can contact the Privacy Officer (privacy@tilburguniversity.edu).

Annex II: Examples controller/processor

Cloud solution where Tilburg University is the controller and the third party is the processor. • Tilburg University uses the SAP application for the salary administration of its staff. An external organization takes care of hosting (cloud), application management and content processing (functional management). • Tilburg University uses Office365 and provides a technical interface for authentication (eg Active Directory, Single Sign On, SurfConext). It is very likely that this environment will be used by students / staff to place files containing personal data. Microsoft monitors the integrity of the files through an automated process and will attempt to repair defective files.	**Cloud solution/service where Tilburg University and the third party are both independent controllers.** • Tilburg University uses an online application and provides a technical interface for authentication (eg Active Directory, Single Sign On, SurfConext). The application only receives the authorization and does not process personal data in the application. • Tilburg University outsources the ordering and shipment of Christmas gifts to an external organization and provides a list of names and addresses. The external organization determines its own purpose and means with its services, the contact details are necessary for the shipment.
On premise solution where Tilburg University is the controller and the third party is the processor. • Tilburg University hosts an application on the campus where personal data are processed, the external organization has structural access to this application as they provide the application management.	**On premise solution where Tilburg University is the controller and the third party is not a processor.** • Tilburg University hosts an application on the campus in which personal data are processed, the external organization does not have access to this application, but does implement application management in a test environment with fictitious or anonymized data. • Tilburg University hosts an application on the campus where personal data are processed, the external organization has occasional access when, under the supervision of our own IT department, it solves or advises on problems in organizational issues.

Annex III: Checklist processor agreement third party

Which requirements should a processor agreement meet?
On the basis of Article 28, paragraph 3 of the GDPR, the processor agreement should at least specify the subject and duration of the processing, the nature and purpose of the processing, the type of personal data processed, the categories of data subjects and the rights and obligations of the controller. In addition, Tilburg University has identified several other topics that warrant contractual provisions.

Below you'll find an overview of the areas of concern.

CHECKLIST

1. **General**

☐ All usual contract information is included and completed. In particular, check:
  - Name and business address of the parties;
  - Clear distinction which party is controller and which party is processor;
  - Name of the authorized representatives;
  - Contact persons;
  - Conclusion, duration, amendment and termination of the agreement;
  - Of which country the law is declared applicable (preferably the Netherlands/Dutch law) and where disputes are settled (preferably before the competent court where the controller is located).

2. **Relation with main agreement**

☐ The document shows that it is a processor agreement and it is in addition to a main agreement.
☐ The processor agreement refers to the main agreement (f.e. a contract for services).
☐ The duration of the processor agreement matches the duration of the main agreement.
☐ The (processor) agreement shows that in case of conflict between the processor agreement on the one hand and the main agreement and/or any terms of conditions on the other, the provisions of the processor agreement shall prevail with respect to the processing of personal data.

3. **Relation between controller and processor**

☐ The processor agreement explicitly states that the controller has control over the purpose and means of the processing of personal data.
☐ It is established which categories of personal data will be exchanged.
☐ It is established that the processor processes the personal data exclusively on the basis of the written instructions of the controller.
☐ It is established that the processor must immediately inform the controller if, in its opinion, an instruction violates the GDPR or any other applicable legislation.
☐ It is established that the persons authorized to process the personal data have a (contractual or legal) duty of confidentiality.
☐ It is established that the processor does not process data for purposes other than those specified in this agreement or may provide data to third parties without permission.
☐ It is established that the processor, if it is legally obligated to provide data, reports this to the controller beforehand, unless legislation prohibits this notification.
☐ It is established that the processor supports the controller with the fulfilment of its legal obligations (including supporting the exercise of data subject rights, security, data breaches, notifications, data protection impact assessments).
☐ It is established (if a system or application is involved) that the processor ensures that it is possible for the controller to safeguard the rights of data subjects through the system or application.
☐ It is established that the processor provides all information to necessary to demonstrate compliance with the obligations laid down in Art. 28 GDPR and enable and contribute to audits, including inspections, by the controller or a verifying party authorized by the controller.

☐ It is established that the processor may not process the data outside the EEA, either by itself or by a third party (sub-processor), unless:
  - An adequacy decision in accordance with Art. 45, paragraph 3 GDPR was taken with regard to the third country or international organization concerned, or
  - Appropriate safeguards in accordance with Art. 46 GDPR are made, including rules as referred to in Art. 47 GDPR, with regard to the third country or the international organization concerned, or
  - One of the specific situations set out in Art. 49, paragraph 1 GDPR applies.

4. Processor – sub-processors

☐ It is established that the processor does not engage third parties/sub-processors for processing unless the controller has agreed to this in writing.[3]

☐ It is established that when the controller agrees with the use of third parties, the processor will enter or has entered into a written agreement with these sub-processors, that incorporates at a minimum the provisions of the processor agreement in place between the controller and processor.

☐ Preferably (not compulsory) it is established that if sub-processors do not fulfill their obligations, the processor remains fully liable for any resulting damage.

5. Security/data breaches/(security) incidents

☐ The processor agreement and/or annex(es) determine(s) that, in accordance with GDPR, the processor provides adequate guarantees with regard to the application of appropriate technical measures and organizational measures (security requirements based on an approved risk analysis/connection to the code of conduct/certification), so that the processing complies with the GDPR's requirements and the protection of the rights of the data subject can be guaranteed.

☐ It is established that the processor periodically reports about security and areas of concern therein, or at least makes all information available to the controller (at its request).

☐ It is established that the processor cooperates with checks on these processing activities.

☐ It is established that the processor improves the security at the instructions of the controller.

☐ It is established that the processor is obligated to report security incidents immediately and to comply with retention periods in accordance with applicable laws and specified regulations (including confidentiality, security requirements).

☐ It is established that in the event of an incident, the processor immediately takes adequate measures to end/stop the incident and to limit the consequences of the incident and prevent repetition.

☐ It is established that in the event of an incident, the processor immediately informs the contact person of the controller and keeps this person informed of developments.

☐ It is established that processor is liable for penalties and damages caused by not complying with the processor agreement, the GDPR or other applicable legislation.

6. Liability

☐ It is established that a limitation of liability from any other agreement or arrangement does not apply to:
  - redress actions under Article 82 of the GDPR; and
  - actions for damages arising from the recovery of fines imposed by the Supervisory Authority that are wholly or partly attributable to the other party.

☐ It is stipulated that the parties shall inform each other as soon as possible about possible liability claims or fines imposed by the Supervisory Authority.

☐ It is stipulated that the parties will give each other reasonable support (including in any case the provision of information) for the purpose of conducting a defense against possible claims for liability and fines by the Supervisory Authority, if necessary for a reasonable fee.

[3] If no specific written permission is requested, but general prior permission, it should be stipulated that the processor informs the controller in a timely manner when it engages a third party, that the controller can object to this (in writing) and that it can provide (additional) conditions for this engagement. It is preferable to define 'timely' or to agree on a deadline, for example of one (1) month.

7. Duration of the agreement

☐ It is established that certain obligations will continue to apply after the end of the agreement (this concerns obligations that by their nature are intended to continue to apply even after the expiration of the agreement, such as confidentiality).

☐ It is established that the processor is obligated to cooperate with the adequate transfer of operations to a successive processor.

☐ It is established that the processor must, at the discretion of the controller, delete the personal data (and the existing copies) after the end of the processing services or return them within a certain period, unless they have to be kept on the basis of a statutory provision. It is stipulated that the controller may issue instructions and may impose requirements on the (method of) deletion or return.

☐ Preferably (not compulsory) it is established that for the transfer of personal data an open file format will be used.

Annex IV: Checklist agreement external party in case of joint controllership

Which requirements should a joint controllership agreement meet?
Pursuant to Article 26, paragraphs 1 and 2 of the GDPR, in the case of joint controllership, the controllers must transparently allocate their respective responsibilities for fulfilling the obligations arising from the GDPR. In particular, responsibilities should be assigned with respect to the exercise of data subject rights and the provision of information as referred to in Articles 13 and 14 GDPR (information to the data subject about the processing of personal data). In addition, it is advisable to make agreements about confidentiality, liability and what to do in case of a personal data breach, among other things.

It is **not** mandatory to enter into a separate agreement in the case of joint controllership, as long as the necessary provisions are recorded in any legal act. Thus, it is also possible to include the provisions in another agreement (for example, a covenant agreement for conducting research). In practice, however, parties often prefer to create a document specifically intended for this purpose (such as the joint controllership agreement).

Below you'll find an overview of the areas of concern.

CHECKLIST

1. **General**

□ All usual contract information is included and completed. In particular, check:
  - Name and business address of the parties;
  - Name of the authorized representatives;
  - Contact persons;
  - Conclusion, duration, amendment and termination of the agreement;
  - That certain obligations will continue to apply after the end of the agreement (this concerns obligations that by their nature are intended to continue to apply even after the expiration of the agreement, such as confidentiality).
  - Of which country the law is declared applicable (preferably the Netherlands/Dutch law) and where disputes are settled (preferably before the competent court where the controller is located).

2. **Object of the agreement**

□ It is established to which project/research/collaboration the agreement applies.
□ It is laid down which processing activity/ies of personal data is/are applicable.

3. **Processing of personal data**

□ The processing of personal data is detailed. In particular, consider:
  - a description of the processing activity;
  - the purpose of the processing activity;
  - what personal data are involved;
  - which category(ies) of data subjects are involved;
  - what the retention periods of the personal data are.

4. **Mutual obligations between parties**

□ The agreement expressly states that the parties will process personal data in accordance with the agreement and applicable laws (e.g., the GDPR).
□ It is stipulated that the parties shall not process data for purposes other than those specified in this agreement, unless it concerns further processing for a purpose compatible with the purpose for

which the personal data was collected. The party carrying out such further processing is independently responsible for this processing activity.

☐ It is stipulated that the parties are each separately responsible for maintaining a record of processing activities.

☐ It is stipulated that the obligations arising from this agreement also apply to those who process personal data under the authority of the parties.

☐ It is stipulated that, if necessary, parties will conduct a data protection impact assessment (DPIA) prior to processing.

☐ A specification of the mutual responsibilities and division of tasks with respect to the rights of data subjects is included in (an appendix to) the agreement.

☐ It is stipulated that each party is independently responsible for taking appropriate technical and organizational measures for processing personal data. A specification of the technical and organizational security measures taken by the parties is included in (an annex to) the agreement.

5. Access to personal data

☐ It is established that access to personal data by the parties is kept to a minimum. Ideally, (an annex to) the agreement defines which (groups of) individuals (preferably based on role or function) have access.

☐ It is stipulated that, if a party outsources (parts of) the (further) processing of the personal data in question to a processor, that party shall ensure that the processor processes the personal data in a proper and careful manner and in accordance with the applicable laws and regulations regarding the processing of personal data and an adequate processor agreement is concluded. This processor agreement may be inspected by all parties, unless otherwise stipulated.

☐ It is stipulated that parties may have personal data processed by other persons or organizations outside the European Economic Area, provided that the applicable laws and regulations governing the processing of personal data are complied with. The transfer mechanism on the basis of which this is possible is also laid down (whether or not in an appendix).

6. Non-disclosure and confidentiality

☐ It is stipulated that those authorized to process personal data have a duty of confidentiality (contractual or legal).

☐ It is established that none of the parties may provide data to third parties without the consent of all other parties.

☐ It is established that if one of the parties is required by law to disclose data, that party shall notify the other parties prior to disclosure, unless the law prohibits such notification.

7. Liability

☐ It is stipulated that the parties are only liable to each other for damage arising from or related to an attributable failure to comply with the provisions of the agreement.

☐ It is stipulated that if one of the parties imputably fails to comply with the provisions of the agreement, that party will indemnify the other parties against third-party claims for any damage arising from or related to such failure.

8. Personal data breach

☐ It is stipulated that if, in the context of the project/research/collaboration, a personal data breach has been discovered by one of the parties, that party will notify the other parties without delay.

☐ In (an appendix to) the agreement there is a specification of the information which parties must provide each other in case of a personal data breach.

☐ It is stipulated who is/are responsible for reporting a personal data breach to the supervisory authority and/or data subjects (e.g. that parties are each independently responsible for reporting a personal data breach, if the breach occurred under its responsibility).

IF SUPPLEMENTARY TO ANOTHER AGREEMENT:

9. Relation to main agreement

☐ The document shows that the agreement is supplementary to a main agreement.
☐ The supplementary agreement refers to the main agreement (e.g. a project agreement).
☐ The duration of the supplementary agreement matches the duration of the main agreement.
☐ The supplementary agreement shows that in the event of a conflict between this agreement on the one hand and the main agreement and/or any general terms and conditions on the other, the provisions of the supplementary agreement shall prevail with respect to the processing of personal data.

Document management

Version	date	distribution	status	Main changes
1.0	28-06-2018	Intranet	Final	n/a
1.1	30-07-2018	HR	Final	Mandate scheme Contractform Planon Decision tree annex I
1.2	02-08-2018	Intranet	Final	freelancer, metadata Planon
1.3	10-09-2018	Intranet	Final	
1.4	07-11-2018	LA, DPO, intranet	Final	Expansion procedure, checklist
1.5	01-04-2019	Intranet	Final	Archive university
1.6	04-11-2021	Internally	Concept	Change in decision tree, alteration in checklist (a.o. due to new version processor agreement)
1.7	08-09-2023	DPO	Concept	Extension document to procedure for agreements concerning personal data
2.0	27-09-2023	Intranet	Final	
2.1	29-04-2024	Intranet	Final	Repaired links, added ‘liability’ to Annex III