Procedure Data Processor Agreement and joint controllers agreement (datasharing)

Document management				
Version	**Date**	**Distribution**	**Status**	**Main changes**
1.0	28-06-2018	Intranet	Final	Not applicable
1.1	30-07-2018	HR	Final	Mandate regulation Form Planon Desicion tree
1.2	02-08-2018	Intranet	Final	ZZP, metadata Planon
1.3	10-09-2018	Intranet	Final	
1.4	06-12-2018	LA, DPO, intranet	Final	Extension procedure, checklist

Purpose

When personal data are shared with an external party, provisions have to be made in an agreement. This document describes the procedure.

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 data processor agreement or an agreement for joint controllers (data sharing). 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 11.4**.

Procedure Data Processor Agreement

Step	Who	What
1	Process owner	Use the division of roles to determine whether a Data Processor Agreement is necessary. See Appendix I for an aid for this and Appendix II with examples. It is advisable to consult the Data Representative as an expert within the organizational unit.
2	Process owner	Check whether a Processor Agreement has already been concluded with the relevant party on the basis of the overview at https://www.tilburguniversity.edu/nl/intranet/ondersteuning-werk/financien/inkopen/universiteitsbreed/(Dutch Only). This overview contains the contract manager with whom you can contact to ask whether a Processor Agreement has been concluded.

3	Process owner	Determine in cooperation with the Information Manager of the school / division or project manager who is involved on behalf of Tilburg University: • Who is ultimately responsible (usually school/division director or dean) • Who is authorized to sign (power of attorney) • Who is contract manager within school / division (owner agreement). • Who will carry out contract negotiations? Determine who is authorized to sign an agreement on behalf of the counterparty.
4	Information manager division / school	SurfConext is access with the institution account in a web application If a Surfconext link is realized, the SurfConext administrator of Tilburg University must be informed of the presence of the underlying agreement and the attributes agreed in it via surfconext@uvt.nl.

5	Process owner	Use the latest Tilburg University model Data Processor Agreement, available at https://www.tilburguniversity.edu/intranet/support-facilities/legal/legalprotection/privacy/.
		
		If you can't help deviate from this model (for example by using the model of a large supplier, or substantive modifications of Tilburg model):
		• Prepare an analysis of the deviations with the Data Representative and the Information Manager of the school / division.
		Use the checklist in appendix III.
		• Still questions? Then you can ask for advice to the Privacy & Security working group (privacysecurity@tilburguniversity.edu)
		  • All articles with the exception of the following: Legal Affairs
		  • Article 5: IT Security Officer (which possibly further coordinates internally with the Chief Information Security Officer)
		  • Appendix A: Legal Affairs, but first advice is to coordinate with Information Manager
		  • Appendix B first part: Information manager LIS
		  • Appendix B second part (security requirements): IT Security Officer
		
		The process owner must motivate the responsible director why he deviates from the model agreement and inform the Data Protection Officer about this.[1]

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

6	Process owner	As proof of compliance with the OWASP security standard referred to in Article 5.2 and Appendix B, please contact the IT Security Officer via avg-security-testing@uvt.nl
7	Process owner	Fill in the yellow shaded fields in the agreement and appendixes in collaboration with the Processor. The Information Manager can help with completing Appendix A and/or the Data Representative from the School or Division can be consulted. See also https://www.tilburguniversity.edu/intranet/support-facilities/legal/legalprotection/privacy/contact/
8	Process owner	Have the Data Processor Agreement signed by the authorized representatives
9	Process owner	Archive the Data Processor Agreement together with the main agreement and metadata in the central contract database Planon. See https://tiu-prod.planoncloud.com/case/FW/SR_030.

Procedure with multiple controllers

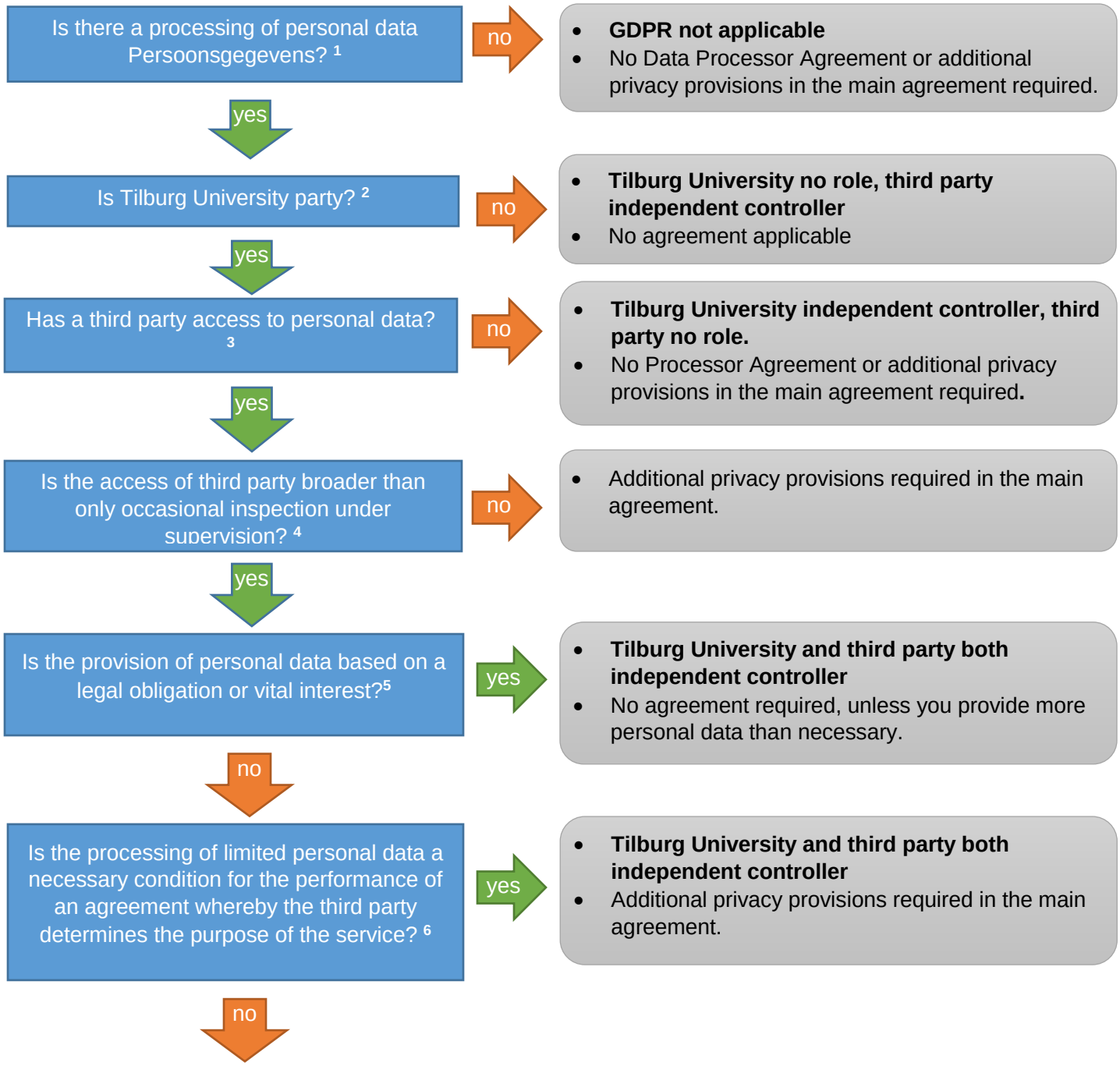
The procedure described above also applies to the situation where there is a data exchange between two controllers. There are two possible situations. For the situation of jointly responsible controllers you may use the available joint controllers agreement (data sharing) or you can make provisions in the main agreement. For the situation of two independent controllers, provisions can be made in the main agreement (e.g. provisions on purpose, content and security of the data exchange).

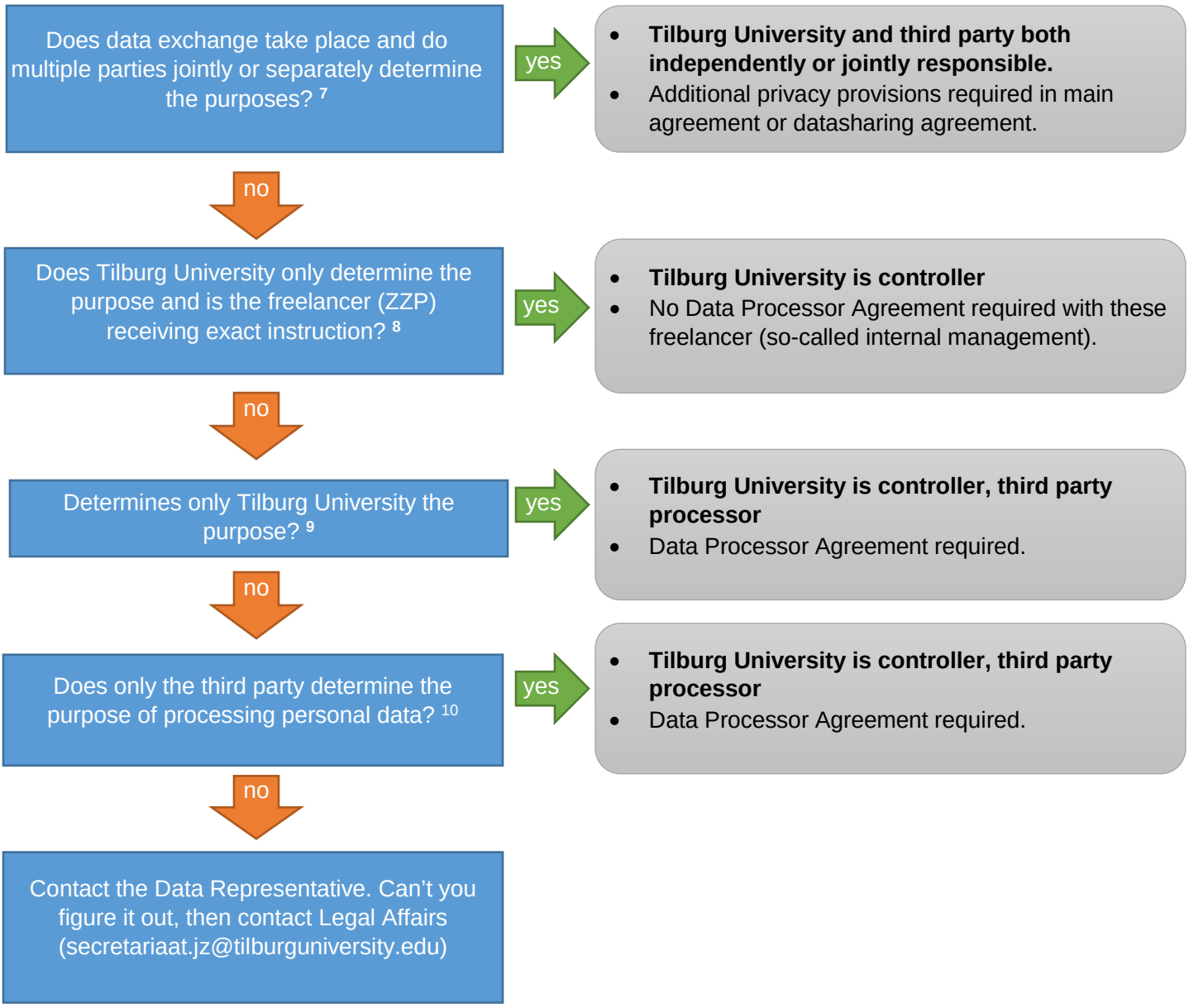
Annex I: Determine role division

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 Data Processor Agreement. In addition, there is the situation where there is a data exchange between two 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.




Does data exchange take place and do multiple parties jointly or separately determine the purposes? [7]
yes
Tilburg University and third party both independently or jointly responsible.
Additional privacy provisions required in main agreement or datasharing agreement.
no
Does Tilburg University only determine the purpose and is the freelancer (ZZP) receiving exact instruction? [8]
yes
Tilburg University is controller
No Data Processor Agreement required with these freelancer (so-called internal management).
no
Determines only Tilburg University the purpose? [9]
yes
Tilburg University is controller, third party processor
Data Processor Agreement required.
no
Does only the third party determine the purpose of processing personal data? [10]
yes
Tilburg University is controller, third party processor
Data Processor Agreement required.
no
Contact the Data Representative. Can't you figure it out, then contact Legal Affairs (secretariaat.jz@tilburguniversity.edu)

1	This should be interpreted broadly: Tilburg University provides personal data, the person involved (e.g. student, employee, respondent) creates its own login account, the person involved / 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) there is processing of personal data.
2	This is the case if an underlying agreement, or if Tilburg University prescribes the application / service or does not provide advice without any obligation ('binding advice'). Non-binding advice: reference to an online survey of a third party. Binding advice: as a student / employee you can use this application to set up surveys or to process datasets where the setting of the surveys or the processing of datasets is part of an assignment, paper, thesis or research.
3	Example: Tilburg University hosts the application itself and the third party does not provide incidental or structural management where they have access to non-anonymised 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, an agreement will always be based on it (for example an agreement that relates to the delivery of an application). Agreements 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 Civil Procedure), IND, DUO, Tax Authorities, NVAO (WHW accreditation). Example Vital interest is providing medical data victim to ambulance service.
6	Example is to provide the name and address of employees to third parties for the delivery of goods (florist, deliverer Christmas packages) or a self-employed (freelancer, ZZP) without receiving instructions and where the primary order does not concern the processing of personal data.
7	For example in joint research projects.
8	Tilburg University allows the processing of personal data by a self-employed (freelancer, ZZP) that works under the instruction of Tilburg University with feedback of enriched personal data.
9	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 Data Processor agreement. For example the outsourcing of the payroll administration, the hosting of applications or the primary processing of personal data.
10	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 role division, contact your Data Representative. Can't you figure it out, then contact Legal Affairs (secretariaat.jz@tilburguniversity.edu).

Annex II: Examples

Cloud solution where Tilburg University is the Data Controller and the third party is the Data 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 with additional personal details. 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 part are both independent Data Controller.** 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 sending of Christmas parcels 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 Data Controller and the third party is the Data Processor. Tilburg University itself 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 Data Controller and the third party is not a Data Processor.** Tilburg University itself 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 anonymised data. Tilburg University itself 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 model DPA third party

What must a processor agreement meet?
On the basis of art. 28.3 GDPR the data processor agreement must 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. Below an overview of the checkpoints.

CHECKLIST

1. General

- ☐ All usual contract information is included and completed, in particular check:
  - Name and business address of the parties;
  - Clear distinguishment which party is controller and which party processor;
  - Name of the authorized representatives;
  - Contact persons;
  - Establishment, duration, modification and termination of the agreement.

2. Relationship with main agreement

- ☐ The document shows that it concerns a processing agreement.
- ☐ The processor agreement refers to the main agreement.
- ☐ The duration of the processor contract matches the duration of the agreement.
- ☐ The (processor's) agreement shows that in case of contradictions between the processor's agreement, any general terms and conditions and the agreement, the provisions of the processor's agreement regarding the processing take precedence.

3. Relationship between controller and processor

- ☐ The agreement explicitly states that the controller has control over the purpose and means of processing the personal data.
- ☐ It has been established which categories of personal data are being exchanged.
- ☐ It has been established that the processor processes the personal data exclusively on the basis of written instructions from the controller.
- ☐ It has been established that the processor must immediately inform the controller if, in his opinion, an instruction violates the AVG or other applicable legislation.
- ☐ It has been established that the persons authorized to process the personal data have a (contractual or legal) duty of confidentiality.
- ☐ It has been 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 has been established that the processor, if he is legally obliged to provide data, reports to the controller beforehand, unless this legislation prohibits this notification.
- ☐ It has been established that the processor supports the controller in the implementation of his legal obligations (including rights of the data subject, security, infringements, reports, data protection impact assessment).
- ☐ It has been established that the processor ensures that it is possible for the controller to guarantee the rights of data subjects through the system .
- ☐ It has been established that the processing provides all the information that is necessary to fulfill the requirements set out in art. 28 AVG's obligations and to make audits, including inspections, by the controller or an inspector authorized by the controller and contributing to it.
- ☐ It has been established that the processor may not process the data outside the EEA unless:

- An adequacy decision in accordance with art. 45 paragraph 3 of the GDPR was taken with regard to the third country or international organization concerned, or
- Appropriate guarantees in accordance with art. 46 AVG are made, including regulations as referred to in art. 47 GDPR, with regard to the third country or the international organization concerned, or
- To one of the specific conditions in art. 49 paragraph 1 GDPR is satisfied with regard to the third country or the international organization concerned.

4. Processor-subprocessors

- ☐ It has been established that processor does not engage third parties/subprocessors for processing unless the data controller has agreed to this in writing.[2]
- ☐ It has been established that when the controller is in agreement with the use of third parties, the processor then enters into a subprocessing agreement with these sub- processors, which minimally incorporates the provisions of the processor agreement between the controller and the processor.
- ☐ It is recommended (not compulsory) to record that if subprocessors do not fulfill these obligations, the processor remains fully liable for any resulting damage.

5. Security / data breaches / (security) incidents

- ☐ The data processor agreement and/or annex(es) determine(s) that the processor provides adequate guarantees in accordance with GDPR with regard to the application of appropriate technical measures and organizational measures (security requirements based on an approved risk analysis / connection of 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 has been established that the processor periodically reports about security and points of attention in it, or at least makes all information available to the controller.
- ☐ It has been established that the processor cooperates on checks on these processing operations.
- ☐ It has been established that the processor improves the security on the instructions of the controller.
- ☐ It has been established that the processor is obliged to report security incidents immediately and to comply with retention periods in accordance with applicable laws and specified regulations (including confidentiality, security requirements).
- ☐ It has been 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 has been established that in the event of an incident, the processor immediately informs the contact person of the controller and keeps it informed of developments.
- ☐ It has been established that processor is liable for penalties and damages caused by breach of contract processors, GDPR or other applicable law.
- ☐ It has been established that the processor indemnifies the controller for fines and damages caused by noncompliance with the processor agreement, GDPR or other applicable legislation.

6. Duration of this agreement:

- ☐ It has been 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);

[2] If no specific written permission is requested, but general prior permission is required, it must be stipulated that the processor informs the controller in a timely manner when he engages a third party, that the controller can object to this and that he can give (additional) conditions for this deployment. It is preferable to define 'timely' or to set a deadline.

- ☐ It has been established that the processor is obliged to cooperate in the adequate transfer of work to a subsequent processor.
- ☐ It has been 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) removal or return delivery.