Recommendations to overcome regulatory barriers

28/10/2022

Author:

Steven Soetens (Province of Antwerp)

This project is supported by the Interreg North Sea Programme (Priority 4, Promoting green transport and mobility) of the European Regional Development Fund of the European Union.

Disclaimer:

This paper reflects only the author's view and the Interreg North Sea Region is not responsible for any use that may be made of the information it contains.

Table of content

1. Introduction

Three reports are written to secure and disseminate useful information

1. Written strategy for the continuation of the CycleDataHub (hence CDH),
2. A report with a final set of recommendations to help stakeholders overcome regulatory barriers
3. Literature report about the integration with non-cycling data systems and services.

This report focuses on **recommendations** to help stakeholders overcome **regulatory barriers.**

In the process of the BITS project, the partners of the BITS project started a number of pilots, innovative solutions that contributed to an increase of cyclists, to the safety of cyclists, to the incorporation of cyclists in smart, multimodal solutions. In doing so, a number of barriers were encountered. In this report you can find some recommendations to overcome these barriers.

These barriers can appear on a number of levels, since we have to deal with a large variety of innovative technical systems and services, all of which generate data and information, in a number of languages, countries, regions, formats, legislations.

Moreover, the INTERREG project focuses on the collaboration between public authorities and businesses, environmental organisations and research institutions. This is a very useful collaboration of stakeholders, since we can learn from each other. In terms of barriers, it also means that for a domain focused on cycling, bicycle, and bicycle infrastructure, there are large gaps in knowledge and experience between partners. Most of the policy partners are focused on infrastructural works, and only in the most recent years, measuring cycling traffic, monitoring quality of cycle paths, digital interaction between cyclists and infrastructure, providing a shared bicycle system monitoring air quality, and many other applications are slowly making their way in the realm of bicycle policy.

Barriers can be both on an institutional level and on a level of technical knowledge.

Under institutional regulatory barriers, we will focus on the GDPR of the EU, the protection of personal data. Other regulatory barriers of an institutional nature are more locally defined by the structure and hierarchy of the individual regions, on the simplicity/complexity of tendering procedures, and again the legislation under which the specific project is executed.

To overcome the barrier of technological knowledge, or more specifically the gap in technological knowledge between policy maker and business/research, a data reflex as main principle has been shared amongst partners of the BITS consortium. This data reflex is more relevant for the stakeholders on the policy levels, because most BITS business partners and research institutions have an intrinsic technological nature and the data reflex is often core of their profession. For the partners in policy, the gap in technological knowledge became apparent from the first meetings. To overcome this gap, one can be focused on who needs the data reflex, for what job it is relevant, and at what stage the data-reflex needs to be activated.

2. Institutional Barrier – GDPR

GDPR was prominently present and considered on all levels by the BITS consortium. From the start the university of Oldenburg most adamantly urged to pay attention to and follow strict procedures when dealing with GDPR issues. What is considered personal data, for what legislative purposes can personal data be used and up to what level of aggregation, what are the necessary formal steps to be taken, etc.

For BITS, the main principle is that each partner is responsible for the GDPR regulations on each of their own pilots. Below we will discuss and formulate some recommendations on how we dealt with GDPR when building the CycleDataHub and the bicycle-data.de websites, which both were direct and digital deliverables of the BITS project itself. Next, we will discuss how we dealt with GDPR for one of the pilots with a smart camera, where a potential privacy issue was identified.

Pilot: CycleDataHub / bicycle-data.de

For the Oldenburg University website https://bicycle-data.de/ and the Province of Antwerp CycleDataHub, special attention was given to GDPR regulations. They have processed either data or datalinks of other internal (BITS) and external (non-BITS) projects/pilots/products.

Since both deliverables have a different purpose, there is also a big difference in dealing with GDPR between https://bicycle-data.de/ and CycleDataHub. The Oldenburg University worked on the collected datasets for further data-enrichment, the definition of KPI's, visualisations in graph and on maps, reprocessing to open data. Therefore it actively collected data from the BITS partners (and many German cities) and republished these data as open (**GDPR verified) data** and aggregated KPI's and visualisations.

The Province of Antwerp worked on the creation of the CycleDataHub. The purpose of this datahub is to acquire an overview of cycle data categories, types, formats, and licences per region (as defined by the EU NUTS classification). Since we aimed to guarantee a continuity (see also the report "Continuation of the CycleDataHub"), the GDPR compliancy, but also the dynamism of some datasets, the decision was taken at an early stage of the BITS project that it would not collect datasets by themselves, but **only links to datasets** that have been published online already by the data owner/data producer/data provider. As such, the responsibility of the content of the data behind the links remains the responsibility of the owner of the data, including the GDPR compliance. Moreover, when filling in the survey for entering a datalink to the CycleDataHub, a double disclaimer (both on the use of the personal data of the person that completes the survey and on the use of the data itself) has to be checked before the survey can be continued, completed and validated. A link to the EU GDPR directives is also included as well as a link to the website of the Province of Antwerp for exercising the rights on the use of personal data.

Data disclaimer

The data disclaimer question is formulated as follows and can be used as a template:

"Only anonymized datalinks will be shared through the (**your datacollection**). It is the responsibility of every data provider to share only anonymized and non-personal data. Are your data GDPR compliant? (GDPR directives)". Yes/No

Personal information disclaimer

The personal information disclaimer question is formulated as follows and can also be used as a template:

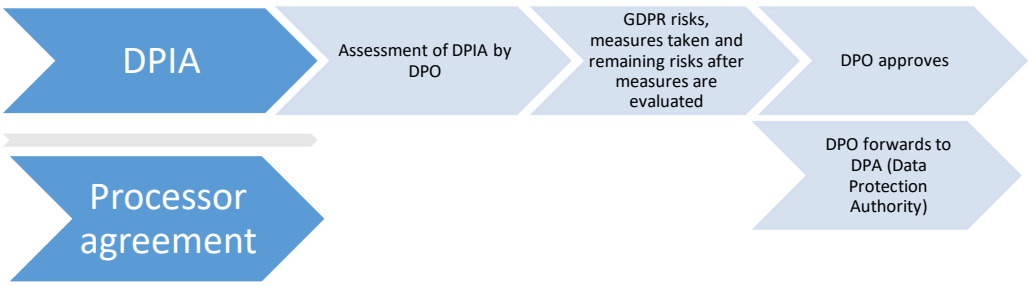
"All data that was provided by you will be processed by the (**your organisation**), with registered office at (**address**) in accordance with the applicable privacy laws. The data will be used exclusively for feedback and clarification on your shared datalinks. Your name and email address will not be shared in the (**your datacollection**) itself. Your personal data will not be transferred to third parties. You have the right to consult, correct or delete your contact details from our contact list. Mail (your **email address**) for these requests. For more information and for exercising your rights go to our **(your weblink on privacy rights**) . Is that okay with you?" Yes/No

Make sure to verify the local legislation since these templates are formulated in accordance with the applicable privacy law for the Province of Antwerp.

Pilot: Camera Analysis

When a project involves a camera or cameras collecting information in the public domain, privacy may be an issue. This means a GDPR audit needs to be done. At the province this was prepared by the project manager of the pilot and evaluated/verified by the Data Protection Officer (hence DPO) (and if necessary with legal assistant). On the occasion of this pilot we held a number of meetings with the DPO of the province of Antwerp to learn what steps needed to be taken. The guidelines below are formulated on the basis of the notes of these meetings.

Summarized: Below you can find a process flow with the steps that were followed, followed by a detailed description of these steps.



1. *DPIA (Data Protection Impact Assessment)*

The project manager can start with the data protection impact assessment and the processor agreement (if the pilot/project is outsourced). This is an evaluation document that the project leader must prepare. The template DPIA is added as annex 1 at the end (in Dutch) in which you can find in detail how the GDPR compliancy is verified and guaranteed. In brief the compliance to GDPR for this research involved the investigation of the compliancy to the privacy regulations of an innovative camera technique. In this case, the camera footage is processed directly in the camera. Since the technique was built on a principle of "privacy by design", the actual footage is deleted once the traffic data are extracted. However, we made the exceptional request of extracting footage of the near conflicts on a crossroad, for communication and explanatory reasons. Once detected by the automated data process, 10 seconds before and after a near conflict anonymized footage (in low resolution, in stick figures and in negative) were saved. All other footage is deleted within seconds.

The DPO functions as an independent evaluator who decides whether all risks are covered, whether sufficient measures are being taken, whether the remaining risks are acceptable or not.

2. *Evaluation by DPO*

This document is then evaluated by the DPO. The DPO functions as an independent evaluator who decides whether all risks are covered, whether sufficient measures are being taken, whether the remaining risks are acceptable or not.

If compliant, a processor agreement must be prepared between client (here the Province) and the company to define the mutual responsibility of legality on privacy (GDPR). The DPO may also decide that not all risks are covered, in which case the DPO can forward the DPIA to the DPA (the Data Protection Authority). This is a national organization for the independent evaluation of GDPR. They may still authorize or decline the compliancy, they may make further inquiries and they have the authority to start legal procedures when GDPR regulations were not followed.

3. *Processor's agreement*

Parallel with the DPIA, if the project manager is confident of a positive outcome of the DPO's evaluation, he/she/they can prepare the processor's agreement. This is an agreement between the project manager and an outsourced company that executes the study. If this is done by subcontracting, the subsequent companies must (for their own legal coverage) also prepare a subsequent processor's agreement between companies. The processor's agreement of the camera pilot is added as is in annex 2 at the end of this document.

4. *Inform citizens*

Once you have a positive evaluation of the DPO and the processor's agreements are finalised, the pilot can start. If this involves cameras, it is advised to inform passing citizens with a sign saying that camera-research is being performed. With low resolution (i.e. when persons cannot be recognised), there is no possibility for processing personal data and the GDPR is not applicable, but local legislation may differ on the obligation of informing citizens. For the province of Antwerp there is a

website to which we can refer: https://www.gegevensbeschermingsautoriteit.be/burger/thema-s/camera-s-en-uw-privacy/ander-cameragebruik

For the pilot project of the camera research in Bornem, the province of Antwerp placed these signs at the intersection informing citizens of the research that was being done in the public domain, the GDPR compliancy of this research, and where they can get further information on their rights.

Below you can find how they were placed and how we formulated the information on the sign for passing citizens (in Dutch).

Fietsostrade Sint-Niklaas - Mechelen

F 18

Verkeersveiligheidsonderzoek met camera - Bornem 20-24 september 2021

De Provincie Antwerpen voert op dit kruispunt in het kader van het Europees project BITS (NorthseaRegion Interreg) een cameraonderzoek uit van 20 tot 24 september 2021. We doen dit om het gedrag van de verschillende soorten weggebruikers in beeld te krijgen met als doel de veiligheid te monitoren en de aanleg van het kruispunt te herevalueren. De toegepaste cameratechniek maakt dat alle gegevens en beelden automatisch worden geanonimiseerd. Mocht je toch nog vragen hebben omtrent de bescherming van jouw privacy bij dit onderzoek, kan je volgende website raadplegen:

www.provincieantwerpen.be

Privacy

Indien je geïnteresseerd bent in het project zelf, kan je hier meer details vinden:

www.provincieantwerpen.be

BITS

Provincie Antwerpen

Interreg North Sea Region BITS

BITS Bicycles and Intelligent Transport Systems

BITS Bicycles and Intelligent Transport Systems

Interreg North Sea Region BITS EUROPEAN UNION

3. Knowledge Barrier – Data Reflex

In the paragraphs below, you will find the recommendations that were shared amongst the BITS partners, but also to other colleagues in the Mobility and Spatial Planning dept of the province of Antwerp. This was considered a logical step of knowledge sharing, since we realised quite early on that there are many initially undetected gaps in technological knowledge amongst a variety of specialists. It was also our experience from the data-processing end (the GIS experts) that a data-reflex as anticipation on projects where data were involved greatly increased the efficiency in working with the data afterwards. As such, the data-team is now involved from the start of any project that uses, or produces data. By doing this, we can anticipate efficient reuse of data (is the produced data in the format that we can work with?), who owns the data, what data are ordered exactly, in what format?

This not only results in a much more efficient use of resources, it also enhances the awareness of the importance and relevance of data in a low tech mode of mobility, such as the bicycle.

The data reflex[1], which is considered a central concept in the BITS project was demonstrated at several other occasions in the project, but emerged from a technological barrier. The most common data source in cycling is targeted collection. We count to know how many cyclists cross a point, park their bicycles. However, these and other types of ITS can lead to valuable insights, we may want to join them to other services, other datasets, and work in an innovative way on enriched data. These opportunities have to be visible, we must be aware of them, before we can use them. We developed a 4-step approach for this:

1. *Available*

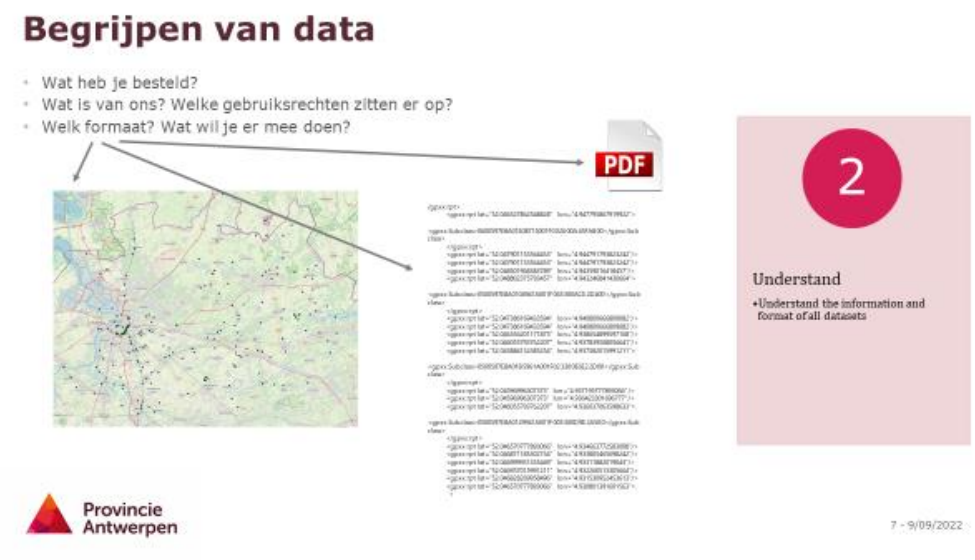
   The data-reflex starts with seeing opportunities and ensuring that data become available. This means arranging from the start that data is collected, and that you will have access to it. This availability goes both ways. What data is needed as input for your project? Is it freely available or must it be produced first? Who is responsible for collection of the input data? And what data results from a project? Or is it a tool?

2. *Understand*

   You have to understand the data, both in terms of information value and how it is technically constructed: what can you do with it and what can't you do with it?

   More practically, this involves knowing what you ordered. What data did you order? And in what format? What are your plans with these data? Maybe these data can be reused by others? And also, who owns the data? What are the user rights on these data?

[1] Also work package 3: Report with user requirements/functional design to inform codesign of ITS solutions and support procurement



3. Process

Data must be processed correctly. How do you convert the data into valuable information? And how do you ensure that the data can be used by others without sacrificing privacy?

Processing data already involves quite some knowledge in data and its qualities. When dealing with data, issues like privacy are at hand, data standards become relevant when you want to ensure a good exchange of data or the integration of data in public services.

Also, practically, processing data can also involve the transfer of data, and agreements on how this should be done. Data can be downloaded, it can be accessed by a webservice or an API.

User's agreements, rights and obligations can be attached to these data exchange procedures.

4. Publish

The final step consists of sharing and inspiring. By sharing data and techniques we offer each other the opportunity to learn and develop new ideas.

The use of data can offer a substantial added value when others can reuse these data. We may not yet realise in which domain our data may be useful to others. However, if the availability, the understanding or the processing potentials of our data were not considered in advance, we may be faced with data or information that is impossible or difficult to integrate or apply in other studies, applications, innovations. As a matter of fact, this is what 'smart' solutions is all about.

Fixing the data as an afterthought often needs much more time, effort, money and it risks in getting ignored.

A major challenge we experienced in this is that getting access to the right data requires good agreements in the beginning. The difficulty is that authorities in this phase focus on the functional requirements and might forget to pay attention to the low hanging fruit in terms of data that the solution offers. In addition, it is not always clear yet what these opportunities will be as the solution might not be clear yet either. Part of a data reflex is therefore training yourself to spot the right opportunities early on in the process when they appear.

Data reflex in BITS

The data reflex is a central concept in the BITS project, as East Riding of Yorkshire Council also shows. East Riding is a municipality with virtually no bicycle facilities and bicycle use. The municipality wants to break through this by, among other things, introducing a bicycle library. Residents can borrow a bicycle that suits their needs: from 'regular' bicycles and e-bikes to all kinds of adapted bicycles. Bicycle coaches then literally help them on their way. By using different sensors in the bicycles to collect data on their use, local authorities gain insight into user behaviour and can invest more specifically in bicycle facilities. Their use is also analysed on a personal level and the bicycle coaches use this to improve their approach. If someone suddenly stops using the bicycle, they can plan a conversation to determine what may have changed and if/how they can help.

Data is often a 'by-product' of ITS applications, as shown in multiple other examples in our project. Dynamic bicycle path lighting turns on when a cyclist is detected and turns off again after they've passed. It's a great application to save energy and reduce light pollution. However, every time a lamp goes on, a cyclist can be counted as well. An app that sets a traffic light for cyclists to green can, in combination with the control phasing of the traffic light, also provide insight into the number of red-light negations. Traffic experts who purchase ITS solutions for improving cycling conditions in their city should therefore not only look at the primary purpose of the ITS application (bicycle lending, lighting, reduced waiting time), but also at other data that can be collected via the ITS applications. Of course, the right agreements need to be made with the supplier (data format, ownership of the data, frequency of the data, etc.).

This text is a cut-out of an article published earlier on this topic. You can find the article here.

Annex 1

Data Protection Impact Assessment

BITS pilots: traffic research with 3D camera at the intersection Puursesteenweg/F18/railway in Bornem

16/07/2021

Version history

Version	Date	Author	Summary of changes made
1	4/6/2021	Xxxx Xxxxxx	Draft
2	16/7/2021	Xxxx Xxxxxx	Final version

Project Responsible Persons

Name	Position
Xxxx Xxxxxx	GIS expert DMOB
Xxxx Xxxxxx	Head team Bicycle DMOB

Approval/validation (if required)

Name	Position	Signature	Date
Xxxx Xxxxxx	DPO		

1. Management summary

This document contains the recording of a Data Protection Impact Assessment (DPIA) as referred to in the GDPR. This DPIA is an analysis of the intended processing of personal data for *Project EU INTERREG NSR - BITS pilot: traffic analysis with camera of a dangerous intersection in Bornem.*

and includes the general context, information on the processing operations, assessment of the associated risks and concrete measures taken to manage these risks and finally a statement on the need for prior consultation with a DPA.

This research is carried out within the framework of the framework agreement of the province VARIA-2017-00608 and within the framework of the European project BITS (Interreg NSR).

The province of Antwerp is a partner in this European project and has had a pilot study carried out with 3D cameras at the intersection of the Puursesteenweg in Bornem with the railway line Bornem - Puurs and the bicycle highway F18.

Anonymised footage of the near conflicts is provided for this, as well as data aggregated from the footage in a privacy by design process. The anonymised video footage is converted into data such as types of road users (cars, trucks, bicycles and pedestrians), times of passage, their speed, their trajectory over the intersection, origin and destination within the analysed area (the intersection) and automatically detected (near) conflicts.

The anonymised images of the (near) accidents will be transferred to the province and used as added value to illustrate behaviour at the relevant intersection in policy decisions between province and municipality, as illustrative media in conferences and online clarification of specific traffic situations. The images will also be kept as illustration and material for the European BITS consortium, traffic conferences, congresses and can be requested for academic research.

2. Framework

2.1 Context organisation

Companies involved

Company	**Role**
Province of Antwerp	*Client*
XXXX	*Contractor to the framework contract of the Province of Antwerp VARIA-2017-00608 (Bicycle counters and traffic research)*
YYYY	*Subcontractor to XXXX, executor of the project*
BITS	*EU consortium within which this project is being carried out as a pilot (INTERREG NSR)*

2.2 Context processing

Within the framework of the European BITS project (Interreg NSR), the Province of Antwerp is a partner and is carrying out a pilot study with 3D cameras at the intersection of the Puursesteenweg in Bornem with the Bornem - Puurs railway line and the F18 cycle route.

The standard procedure here assumes an analysis with privacy by design, whereby de facto no video images are stored, but whereby the images are immediately converted into data.
The data contains types of road users (cars, trucks, bicycles and pedestrians), numbers aggregated per time interval (hour/day), in speeds and speed classes, heatmaps with trajectories over the intersection, origin and destination within the analysed area (the intersection) and automatically detected (near) conflicts (Fig 1 below, left and centre).

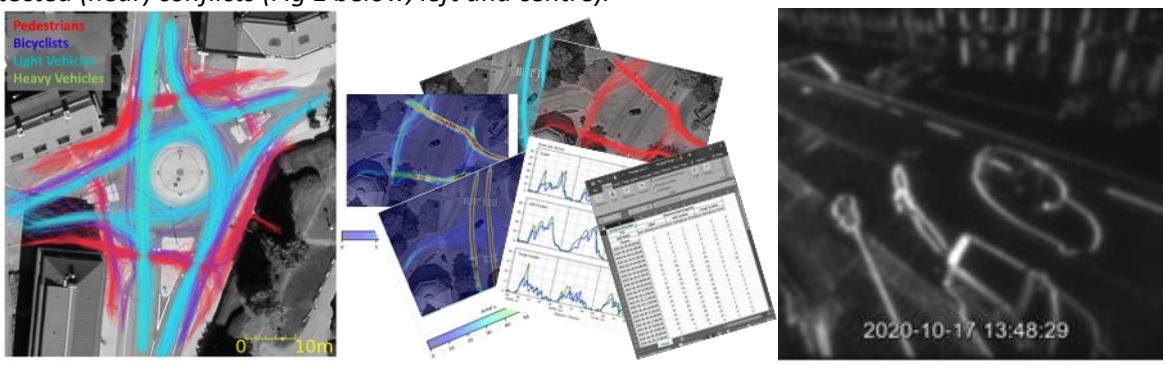


Figure 1. (left) anonymous movement patterns of different types of road users. (middle) anonymous data after processing from the movement patterns: heat maps, graphs and tabular data. (right) anonymised video, generated immediately (in real time) in the sensor. Only this anonymous video footage is kept, the original footage is deleted within 20 milliseconds.
Anonymised footage of the near conflicts is also ordered, as they offer added value as visual support in specific problematic/dangerous traffic situations. All camera images are immediately anonymised in the camera (as a negative image, in low resolution and persons are distorted into stick figures). (Fig.1 above: right)
In post processing of these anonymous images, the footage from 10 seconds before to 10 seconds after the (near) conflict is extracted. These short films of 20 seconds each are delivered to the province. All other footage is destroyed, leaving only the anonymised footage and data. The remaining footage is then used to support traffic policies, presentations, as media for the EU BITS project, online. Media that we make public will also be checked by the provincial staff on recognizability and if necessary or requested will be removed/destroyed.

3. Data Protection Impact Assessment Project

3.1 General Information

1. Scope

This DPIA aims to perform a risk analysis of the privacy and data protection related risks related to the operation of the analysis and processing of camera detection images, taking into account the following personal data processing operations:

- Processing of video images of (possibly underage) citizens and vehicles.

2. Actors involved

Name	Role
DMOB, Province of Antwerp	*client*
BITS consortium	*EU INTERREG NSR project, of which this research is a pilot*
XXXX	*Contractor of the Province, subscribed to framework agreement VARIA-2017-00608*
YYYYY	*Subcontractor, data processor for XXXXXX*
Traffic experts, citizens	*Anonymised images can be used as material in presentations, on the provincial website, in publications, for the European BITS project*

3. Project planning

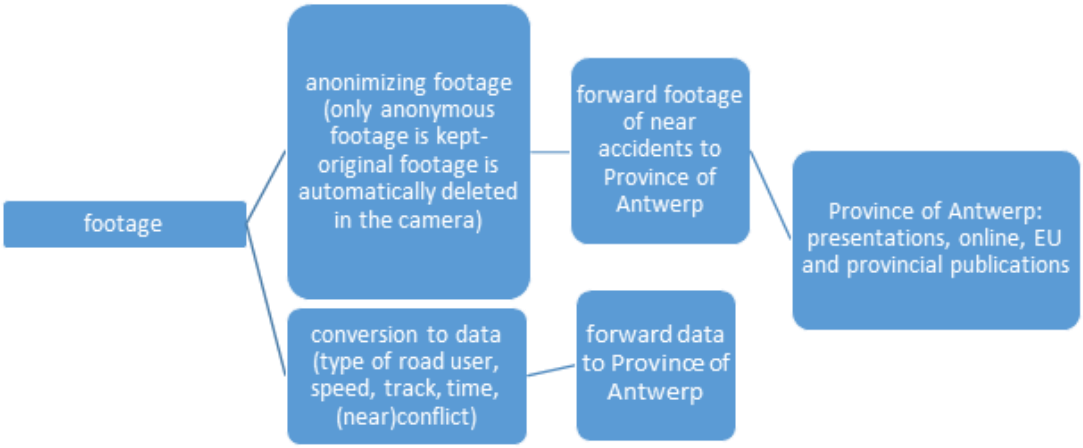
If the DPIA is part of an ongoing project, describe the general planning and deadlines.
The specific 3D camera survey is a continuation of a previous project (23-27 September 2019) where only data was collected. The project presented here will take place from 20 to 24 September 2021. The data and media are expected in autumn 2021.

4. Processors involved and contractual agreements

Processor	Role	agreement signed?	data export?
XXXXX	*Contractor*	*In preparation*	*NVT*
YYYYY	*Subcontractor to XXXX*		*Autumn 2021*

4.1 Description data life cycle / data flows in detail

Presentation of the data flows by means of diagrams or textual description from the receipt or creation of the data to its final destruction, archiving or transmission. (See also 2.2 for the description of the process).



4.2 Review of basic principles of personal data processing

1. Transparency, lawfulness

How is legally required information provided to each data subject?

A sign will be placed at all access roads to the intersection on which the period of video recordings, the purpose of the investigation and a reference to the privacy regulation of the province will be shared with the passers-by.
What is the legal basis for processing personal data?
Public interest, specifically research into the behaviour of different types of traffic at a dangerous intersection to improve traffic safety.

2. Purpose limitation

The purposes for the intended processing are:

- *Measuring the effect of a modified intersection design on the behaviour of road users.*
- *Testing 3D camera research in function of traffic safety.*

This concerns more specifically the detection of the behaviour of road users just before, during and just after a (near) conflict, with a mode of transport (two-wheeler, passenger car, truck, pedestrian), speed, and movement over the intersection, in order to learn lessons with regard to intersection design and human behaviour.

3. Minimal data processing

Considering the purpose mentioned in 4.2.2, which data is absolutely necessary for this?

Data field	***Reason for processing***
Classification (mode) of travel (vehicle)	*Specific behaviour of passer-by in the different modes*
Speed	*Speed of passer-by, necessary to determine risk of near collision*
Track/location	*Movement across the intersection is needed to extract near conflicts*
Detection of (near) conflicts based on speed, proximity and approach angle	*Analysis of (near) conflicts to improve traffic safety at the intersection*
Time	*When do we detect which types of conflicts?*

4. Correctness

There are no issues regarding correctness, as only anonymised images remain. The precision of the data and aggregates is limited by the A.I. algorithms used to convert the images into data. For example, we do see two-wheeled vehicles, but the distinction between a cyclist, a speed pedelec and a motorbike is not very reliable.

5. Storage limitation

After anonymisation and extraction of the (near) accidents, the storage period of the camera images is unlimited because they serve as an illustration and substantiation for the investigation of (near) conflicts at intersections. All other media (the anonymised footage) that do not contain (near) conflicts are destroyed as soon as the (near) conflicts have been extracted.

6. Integrity & confidentiality

What technical and organisational measures have been taken to guarantee the security, confidentiality, integrity and availability of the data?

Risk	*description measures taken*	*effect*
Recognition of citizens	*The footage is put in the negative, resolution is greatly reduced and persons are reduced to stick figures*	*Citizens cannot be identified*
Recognition of vehicles	*All vehicles are put in negative. The resolution is very limited. A number plate is illegible, a large logo can still be recognised*	*Most vehicles cannot be identified*

4.3 Rights of the data subject

How is it ensured that the data subjects 1/ know their rights (privacy policy communicated?) and 2/ can exercise their rights?
- Right of inspection
- Withdrawal of consent
- Opposition to further processing
- Right to request deletion of their data
- Right to be forgotten
- Right to rectification
- Right to object to profiling and automated decision making

All passers-by at the intersection are informed of the presence of cameras by signs posted on all access roads. Anonymity is assured, the period of the investigation is also indicated. The province's website (with privacy regulations and GDPR procedures, as listed above) are clearly communicated.

5. Risks

Listing of risks detected without taking additional measures (inherent risk). In other words, we look at how the situation is now based on the data described in the previous sections. What risks or problems do we see with regard to the data we process (e.g. basic principles of personal data processing, security of the data), and in a broader context, what possible impact on individuals whose data is processed (e.g. rights of the individual, reasonable expectations, sensitivity of the data, possible consequences of a data breach).

5.1 Risk Analysis Methodology

The present Risk Analysis is based on a system whereby, on the basis of a questionnaire filled in, to each answer from that list a numerical score is assigned to a) the probability that a risk will occur and b) the impact of the risk on the data subjects if it were to effect. These values are then multiplied to arrive at a risk classification level of 'high' (red colour code), 'medium' (orange colour code) or 'low' (green colour code).

1. Assess the likelihood

The probability of each risk should be rated on a numerical scale from 1 (low) to 5 (high).

Rating	Description	Summary
1	Very unlikely	Has never happened and there is no reason to believe that it would be more likely now
2	Not likely	There is a possibility that it could happen, but it is

		not likely to happen
3	Likely	All things considered, it is more likely that the risk will occur than that it will not
4	Very likely	It would be surprising if the risk does not materialise, either based on past history or current conditions
5	Almost certain	Either it is already happening regularly or there is some reason to believe that it is almost at the about to happen

2. Assess the Impact

The impact of each risk should be rated on a numerical scale from 1 (low) to 5 (high).

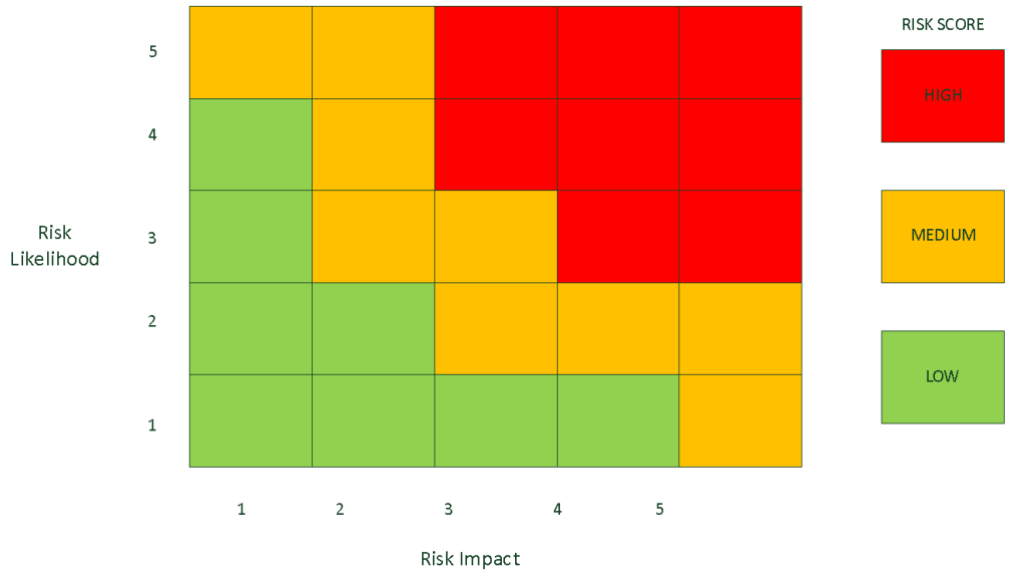
Rating	Description	Impact on customer	Financial Impact	Health and Safety	Image Damage	Legal Impact
1	Negligible	None	None or very little	Very small additional risk	Negligible	No implications
2	Slight	Some localised disruption to normal business operations	Some	Within acceptable limits	Slight	Little risk of non-compliance with the compliance
3	Moderate	Could still deliver the product/ service with some difficulty	Unwelcome but bearable	Increased risk requiring immediate attention	Moderate	Definite risk of acting illegally
4	High	Business is seriously damaged in key areas	Serious effect, on revenue and/or profit	Highly life-threatening	High	Illegal trading in some areas
5	Very high	No longer operational/ no service to members	Seriously damaging; organisation will go bankrupt	Real or strong possibility of death	Very High	Fines and possible imprisonment of staff

3. Risk classification

Based on the assessment of the level of likelihood and impact, a point total is calculated for each risk by multiplying the two figures. The resulting point total is then used to decide on the classification of the risk based on the matrix shown in the table below.

Each risk is assigned a classification based on its point total as follows:

- HIGH (RED) - 12 or more
- MEDIUM (ORANGE) - 5 to 10
- LOW (GREEN) - 1 to 4



5.2 Identified risks

No.	Description	Severity	Chapter
RISK-001	Recognition of citizens	Low	4.3.6
RISK-002	Vehicle recognisability	Low	4.3.6

6. Measures taken

Describe the measures taken to reduce the risks as mentioned in 5.2. This can be done by including a paragraph per risk (e.g. RISK-001) describing the actions taken to reduce the risk.

Risk	Action taken
RISK-001	Anonymisation due to low resolution, negative of original image, stick figures instead of persons
RISK-002	Low resolution, negative, the Province itself determines which images become public and ensures that recognisable large logos on trucks are not made public

7. Residual risks

Analyse here which of the risks identified in chapter 5 are not sufficiently covered by measures from chapter 6. These are the residual risks. Below is an overview of the various risks that cannot be covered by the various measures (or residual risks).

7.1 Overview of residual risks

The identified risks are sufficiently covered by the described measures. Consequently, there are no residual risks.

7.2 Decision on prior consultation DPA

Depending on the residual risks from 6.1, it is determined here whether or not prior consultation will ultimately be carried out. In other words, whether the local data protection authority should be contacted to ask for advice regarding the processing because the residual risks are (possibly) too high.

If relevant, also mention here the approval or reference to a report of a project team, management consultation, etc. where the decision on the prior consultation was discussed.

This is not applicable. It is not necessary to submit the processing to the DPA.

Annex 2

PROCESSOR AGREEMENT

Between
The Province of Antwerp*, on the one hand,** with company number *0123.456.789* and registered office at ***address, represented by *xxxxx, function, acting on behalf of xxxxx, and xxxxx, function*, acting in implementation of the *research agreement nr. of dd/mm/YYYY*, **hereinafter referred to as 'the Processor' or 'the Parties'.**
And
Company XXX* on the other hand,** with company number *XX12345678* and registered office at ***address, represented by *xxxxx*, **hereinafter referred to as 'the Processor' or 'the Parties'.**
It is agreed what follows:

Preliminaries
In accordance with the applicable legislation on privacy, in particular the General Data Protection Regulation[1], in the event that a Processing Owner relies on a Processor for the processing of personal data, an agreement must be drawn up regarding such processing.
The Processing Agent has concluded the framework agreement *xxxxxxxxx* with the Processor for activities relating to traffic research. In this specific case, the Processor calls on *xxxxx*, hereinafter referred to as the 'Subprocessor' as far as camera research is concerned.
The Controller shall exchange personal data directly with the Subprocessor in accordance with the terms and conditions set out in this Agreement.

Article 1 - Definitions
- GDPR: Abbreviation of General Data Protection Regulation (see footnote 1).
- Personal data' are, as stated in Article 4.1 of the GDRP (hereinafter abbreviated as 'the Data'): "any information relating to an identified or identifiable natural person ("the data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular 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".
- The 'Controller' is, as stated in Article 4.7 of the GDPR: "a natural or legal person, public authority, agency or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".
- The 'Processor' is, as stated in Article 4.8 of the GDPR: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller".
- The 'Processing operations' referred to in this Agreement are processing operations within the meaning of Article 4.2 of the GDPR: "an operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data".
- A 'Data breach' as stated in Article 4.12 of the GDPR: "a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, data transmitted, stored or otherwise processed".

Article 2 - Object of the Agreement

2.1. The Processor and the Controller enter into this processor agreement as a legal obligation arising from the following agreement(s):

- *Research Agreement nr*.

Hereinafter abbreviated as "the main agreement(s)".

2.2. This processing agreement is within the framework of the agreements made by the Parties in the above-mentioned main agreement(s) (and any annexes) and is intended to formalise the agreements relating to the protection of the Data in accordance with the applicable legislation on privacy.

Article 3 - Commitments of the Parties

3.1. All Parties expressly and principally undertake to comply with the following (non-exhaustive) legal provisions:

a. the provisions of the GDPR;
b. the minimum security standards required by the Commission for the Protection of Privacy;
c. the provisions of the Act regulating a National Register of Natural Persons of 8 August 1983;
d. other relevant legislation.

3.2. As long as the Act on the Protection of Privacy with regard to the Processing of Personal Data of 8 December 1992 (Privacy Act) remains in force, the Parties undertake to comply with the provisions of that Act.

Article 4 - Obligations of the Processor

4.1. The Processor acts exclusively on the instructions of the Processing Responsible Party and will only access and/or process the Data if and to the extent that this is necessary for the performance of the main agreement(s).

4.2. The Data may only be processed by the Processor for the purposes specified in this Agreement (Annex 1). The Processor undertakes not to act or allow to be acted in a manner contrary to the undertakings set out in this Agreement or any applicable legal provisions.

4.3. The Processor undertakes:

a) ensure that the processing of the Data is carried out under the supervision and responsibility of a dedicated data protection officer, as provided for in Articles 37 to 39 of the GDPR;
b) provide its own up-to-date information security plan/information security policy, in which the various reference measures are given concrete form.

4.4. The Processor is obliged to keep the Data it receives from the Processing Responsible confidential, except insofar as a statutory provision or a court order obliges the Processor to disclose it or if the data provision takes place on the instructions of the Processing Responsible Party. Any mandatory disclosure of the Data to third parties, based on a statutory provision or a court order, must be notified by the Processor to the Processing Responsible Party in advance.

4.5. The Controller authorises the Processor to communicate this Data to all persons, institutions and bodies that participate directly in the execution of the order and are authorised to receive such Data.

4.6. The Processor is permitted to make a copy under this Agreement if this is necessary for the performance of the order or for backup purposes. The use of copies and backups is subject to the same rules as the use of the original Data.

4.7. The Processor guarantees that the persons working in its name and on its behalf only have access to the Data they need to perform their task or assignment under this Agreement. This shall apply to staff, hired or temporary personnel and any third parties directly or indirectly involved in the performance of the processing. The Processor shall prevent, by means of segregation of duties, that a combination of access rights could lead to unauthorised actions and/or access to the Data.

4.8. The Processor undertakes to inform the persons working under its responsibility or authority of the provisions of the applicable legislation and of its implementing decrees. It shall inform the Processing Manager in writing of the precise way in which it will fulfil this undertaking.

4.9. The Processor shall provide, upon reasonable request by the Processing Owner, an updated list of the staff, hired or temporary staff and any third parties (see also Article 6), directly or indirectly involved in the performance of the order and the authorisations they have in relation to the Processed Data.

4.10. The Processor shall provide the Processing Agent, whenever requested, with a copy of the Data processed under this Agreement in a format to be mutually determined, being:

- *Anonymous data from movement patterns, traffic counts and traffic safety indicators (see left and centre in Figure). These data will be made available as graphs, excel sheets and possibly as csv files or other open data formats.*
- *Anonymised video footage as a context for the road safety indicators, (see figure on the right as an illustration. This video will be delivered as normal video files in avi or mpeg format.*

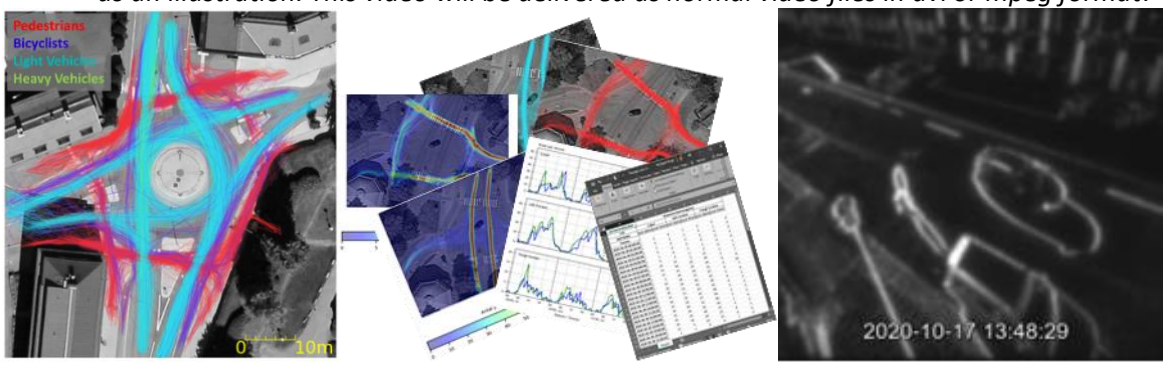


Figure 1 . (left) anonymous movement patterns of different types of road users. (middle) anonymous data after processing from the movement patterns: heat maps, graphs and tabular data. (right) anonymised video generated immediately (in real time) in the sensor. Only this anonymous video footage is saved, the original footage is deleted within 20 milliseconds.

4.11. The Processor undertakes not to store the Data at a location outside the European Economic Area or to transfer them to countries outside the European Economic Area without the prior written consent of the Processor.

4.12. The Processor undertakes to assist the Controller in responding to requests from Data Subjects regarding the exercise of their legal rights (Chapter III of the GDPR).
If a Data Subject makes a direct approach to the Processor to invoke one of the rights granted to them under Chapter III of the GDPR, the Processor shall inform the Controller thereof without delay and shall only comply with the Data Subject's request with the Processor's written consent.

4.13. The Processor shall immediately inform the Processing Owner if, in its opinion, an instruction infringes the GDPR or other provisions of Union or Member State law on data protection.

Article 5 - Responsibilities and safeguards

5.1. The Processor shall ensure that all Data it provides to the Processor under this Agreement can be legally disclosed to the latter in accordance with the applicable legislation.

5.2. The Processor undertakes to acquire, maintain and regularly update the software and equipment, as well as the licences required for their legal use, in order to have a state-of-the-art system to fulfil its obligations under this Processing Agreement.

5.3. The Processor shall ensure that none of the equipment or software it uses under this Processing Agreement infringes the intellectual property right of a third party (such as copyright, patent, sui generis right, trademark, etc.).

5.4. The Processor shall ensure, to the extent technically possible, the integrity, availability and confidentiality of all Data that it processes under this Processing Agreement. The Processor shall do this at least by implementing and using security technologies and techniques, which are consistent with industry best practices. This includes mechanisms to detect and/or identify vulnerabilities and the timely implementation of patches and/or updates. The questionnaire in Annex 3 must be completed in full by the Processor.

5.5. The Processor shall be responsible for the security and proper use of the access codes, user names and passwords, as well as for regularly changing these codes and passwords, for accessing and processing the Data. The Processor undertakes to do its utmost to ensure that all persons having access to the Data preserve the confidentiality of their codes and passwords.

5.6. The Processor undertakes to inform the Controller immediately (within 24 hours at the latest) in writing of the existence of any Data Breach and any other serious attempts at unlawful or unauthorised Processing or access to Personal Data and of the actions it will take to remedy the incidents.
In addition, taking into account the nature of the Processing and the information available to it, the Processor shall assist the Controller in complying with its obligations regarding:

- Reporting of a data breach to the supervisory authority in accordance with Article 33 of the GDPR;
- notifying the person concerned of a data leak in accordance with Article 34 of the GDPR.

However, the Processor is not permitted to report the Data Leak itself to the GBA or to make the notification to the person concerned. This is exclusively the responsibility of the Processing Agent.

5.7. Taking into account the nature of the processing and the information available to it, the Processor undertakes to assist the Controller in enforcing the obligations concerning the data protection impact assessment as set out in Article 35 of the GDPR.

5.8. The Processor shall indemnify the Processing Responsible Party against any complaint lodged by a third party, including the Data Protection Authority, that would result from an act or omission by the Processor in breach of its obligations as set out in this Processing Agreement or in breach of applicable law. In particular, the Processor shall indemnify the Processing Party against the reimbursement of any legal costs (including attorney's fees) and damages that the Processing Party may be ordered to pay as a result of its activities.

Article 6 - Subcontracting

6.1. For the practical implementation of the processing, the Processor may enter into subcontracting agreements with third parties (hereinafter referred to as "Subprocessor(s)"). The Controller generally consents to the sub-processing of the Data by Sub-processors in order to achieve the purposes.

6.2. If the Processor (partially) outsources the processing of the Data on behalf of the Processing Responsible Party, the Processor will always do so by means of a written agreement with the Subprocessor that imposes the same or at least equivalent data protection obligations on the Subprocessors as the obligations imposed on the Processor under this Processing Agreement. If the Subprocessor fails to fulfil its data protection obligation under such a written agreement, the Processor will remain fully liable to the Processing Party for compliance with those obligations.

6.3. The Processor shall keep an up-to-date list (Annex 2) of active subcontracts with Subprocessors and shall provide it to the Processing Responsible Party within a reasonable time. The Processor will inform the Processing Responsible Party on a structural basis if this list changes. The Processor can then object to the acceptance of the proposed Subprocessor.

6.4. The fact that the Processor entrusts all or part of its undertakings to Subprocessors does not relieve it of its responsibility towards the Processing Manager. The latter does not acknowledge any contractual relationship with these Sub-processors.

6.5. All obligations imposed on the Processor shall also be imposed on each of its Sub-processors for the services that concern them. In particular, the Processor shall impose the secrecy obligation on its Subprocessors. It shall keep proof of their compliance with this at the disposal of the Processing Manager.

Article 7 - Control by the Controller

7.1. The Processor is entitled to verify compliance with this Processing Agreement. To this end, it may, by appointment, visit the premises or places where the Processor carries out the data processing or provide the relevant information in connection with this right to inspect. The Processing Responsible Party will inform the Processor in writing at least ten days prior to carrying out the inspection. The Processor will carry out the audits, unless mandatorily required otherwise, only on working days during office hours.

7.2. Upon request by the Processing Party, the Processing Party shall be obliged to provide all information and assistance relevant to the implementation of this Processing Agreement.

7.3. Shortcomings identified in audits shall be addressed by the Processor and converted into a plan. This plan shall be submitted to the Processing Owner for review and approval within a reasonable period of time, which is proportionate to the seriousness and complexity of the shortcoming identified.

7.4. The Processor shall ensure the implementation of the corrective action at its own expense and in accordance with the timing indicated in the proposed plan.

Article 8 - Intellectual property

All intellectual property rights to the Data and to the databases containing this Data shall belong to the Controller, unless contractually agreed otherwise between the Parties.

Article 9 - Duration and end of the agreement - retention of data

9.1. This Agreement shall enter into force upon signature by the Parties and shall continue for as long as the Processor needs to process the Data transferred by the Processing Party and as long as necessary for the performance of the main agreement(s) for the purposes of which this Processing Agreement is entered into.

9.2. Upon termination of this processing agreement, the Processor shall provide the Processing Agent or any person designated by the Processing Agent with a current copy of the database(s) containing the Data processed in a structured, commonly used and machine-readable format free of charge. The Processor shall also provide the Processing Agent with any information or documents required for the subsequent processing of the Data. The Processor shall contribute in good faith to the transfer of all Data and databases to the computer system designated by the Processing Agent.

9.3. If all Data and databases have been transferred, the Processor shall immediately cease any processing of the Data and destroy any copy and back-up of the Data and databases that it may still possess free of charge, unless contractually agreed otherwise between the Parties or the storage of the Personal Data is required by Union or Member State law. The Processor shall provide a signed "Declaration of Destruction" to the Processing Agent after the destruction is carried out.

9.4. Articles 4.4 (duty of confidentiality), 4.8, 5.4 (confidentiality), 4.12, 5.6, 5.7 (assistance), 6 (subcontracting), 7 (checks), 9.2 (end of contract), 11 (applicable law and competent courts) shall remain in force after the transfer or termination of this processing agreement.

9.5. If the Processor does not comply with its obligations under this Processing Agreement, the Processing Owner may, without prejudice to the right to obtain compensation, terminate the Order in whole or in part after giving a written notice of default and stating reasons if the Processor fails to take appropriate measures.

Article 10 - Completeness of the Agreement

If any provision of this processing agreement is destroyed or declared invalid in any other way, the rest of the agreement shall remain in force and the provision in question shall be replaced by a valid provision that reflects as closely as possible the original intention of the Parties.

Article 11 - Applicable law and competent courts

11.1. This processing agreement is subject to Belgian law.

11.2. The Parties shall make every effort to settle any disputes relating to the execution of this processing agreement amicably. If this proves impossible, the courts of the *district of Antwerp* shall have sole jurisdiction.

11.3. This Processing Agreement replaces any previous agreement, declaration or understanding, whether oral or written, relating to the subject matter of this Processing Agreement.

11.4. The Parties confirm that they acted in good faith when negotiating and drafting the present Agreement, and confirm their intention to follow the same principle when implementing it.

11.5. Amendments or supplements to this processing agreement shall be agreed upon in writing between the Parties. Amendments or supplements shall be recorded in an addendum to this processing agreement and shall not be binding until this addendum has been signed by both Parties.

Article 12 - Conclusion

By signing this Processor Agreement, the Processor agrees to respect the above provisions and also to impose them on the employees of its organisation and on anyone it may engage in the context of the execution of this Processor Agreement.
He realises that his organisation can be held responsible for the abuse or negligence of his employees.

Drawn up in *Antwerp on DATE* in two copies of which each Party declares having received one signed copy. The Annexes referred to in this Processing Agreement form an integral part of this Agreement.

On behalf of the Controller

..... *(first name and surname)*
..... *(function)*

On behalf of the Processor

..... *(first name and surname)*
..... *(function)*