GBO Project 2008
URBAN
D 5.3.1: Code of Practice for Geographic Surveillance and 3D City Modelling

IBBT vzw, Interdisciplinair Intstituut voor Breedbandtechnologie
Gaston Crommenlaan 8 (bus 102), 9050 Gent, Belgium ● E info@ibbt.be ● T +32 9 331 48 00 ● F + 32 9 331 48 05 ● www.ibbt.be
RPR Gent VAT BE 0866.386.380



This document is strictly confidential

Document History

Title Deliverable	D5.3.1.: Code of practice for geographic surveillance and 3D city modelling
Version number	1.0
Author	Christophe Geuens

Document History (only main versions)

Document version	Date	Remarks
0.1	01.01.2009	First draft. Submitted for comments
1.0	26.02.2009	Final version

TABLE OF CONTENTS

I. INTRODUCTION 5
I.1. Work package 5
I.2. Content of Deliverable 5
II. IMPLICATIONS OF LEGISLATION ON PERSONAL DATA 7
II.1. A concept of privacy 7
II.2. Principles of personal data protection 8
II.3. In practice: Google Street View 10
I.3.1. Overview 10
I.3.2. Compliance with data protection rules 10
I.3.3. What is different for URBAN? 11
III. CONDITIONS FOR PERSONAL DATA PROTECTION 12
III.1. Directive 95/46/EC 12
III.1.1. Scope 12
III.1.1.a. General 12
III.1.1.b. Applicable on URBAN? 14
III.1.2. Legitimacy of processing 15
III.1.3. Conditions for processing 17
III.1.4. Rights of Data Subject 19
III.1.5. Impact on URBAN 21
III.2. 2002/58/EC and 2006/24/EC 21
III.2.1. Scope 21
III.2.1.a General 21
III.2.1.b. Applicable on URBAN? 22
III.3. Personal Data Protection Act 8 December 1992 (WVP) 22
III.3.1. Scope 22
III.3.1.a. General 22
III.3.1.b. Applicable on URBAN? 22
III.3.2. Criteria for processing 23
III.3.3. Conditions imposed upon processor 25
III.3.4. Rights of Data Subject 28
III.3.6. Implementation on URBAN 30
IV. IMPLICATIONS OF INTELLECTUAL PROPERTY RIGHTS 33
IV.1. Relationship IPR and URBAN 33
IV.2. Copyright 33
IV.2.1. Legal Framework 33
IV.2.2. Scope 33
IV.2.3. Conditions for application 34
IV.2.4. Exceptions/ Exemptions 35
IV.2.5. Implications for URBAN 36
IV.3. Trademark 37
IV.3.1. Legal Framework 37
IV.3.2. Scope 37
IV.3.3. Conditions for application and the scope of protection 37
IV.3.4. Exceptions/ Exemptions 39
IV.3.5. Implications for URBAN 39

IV.4 Conclusion Intellectual property rights 39
V. INSPIRE DIRECTIVE 2007/2/EC 40
V.1. Scope 40
V.1.1. General 40
V.2. Aim and means of Directive 41
V.3. Applicable on URBAN? 41
VI. CONCLUSION 42

I. INTRODUCTION

I.1. Work package

This deliverable is part of Work Package 5, which concerns the legal aspects of the project. Although the concept of the project is nothing new, it goes further than anything we have seen before. The idea is to go beyond what we have available today, being images made from cars or vans. Mobile units will also be used to reach places that are publically accessible but inaccessible to cars or vans. This raises certain questions with regard to privacy and processing of personal data.
Furthermore the images acquired will be kept for possible further use on other applications. This also is a reason for concern. The controversy surrounding Google Street View is a good indication of the sensitivities surrounding geographic surveillance.

There are also questions regarding intellectual property rights, since the project will involve constructing 3D models and thus reproducing works of architecture. These works migth be subject to intellectual property rights and this may impede upon certain aspects of URBAN. This might not only be an impediment to certain applications developed under URBAN, but is also a threat to the existence of the project. A rights holder might have the ability to block or slow the project entirely by refusing a necessary permission; if any.

These two themes were put forward in the research proposal and will be examined in this deliverable in order to provide a modus operandi to approach geographic surveillance and 3D city modelling.

I.2. Content of Deliverable

The goal of this deliverable is to present, as indicated by the title, a code of practice. It is destined to be used as a reference by anyone involved in geographic surveillance and 3D city modelling. It must inform them about the course of action to follow and provide solutions to problems that might arise during development and use of applications. Therefore we try to make the document as accessible as possible, but legal accuracy is the first objective of this deliverable.

The first part will elaborate on the implications of legislation on personal data. It will provide a concept of privacy, without any intention of claiming to be the definition of privacy. It is just meant to give an idea of what could fall under the term privacy, provide some insight in what will follow and what are possible problems when dealing with privacy matters of any kind.
The second part will elaborate on the rules governing personal data and will be one of the core parts of this deliverable. Both the European and the Belgian framework will be discussed and the legal obligations explained. In addition we

will try to deduct conclusions that are valid throughout the EU; for as far as this is possible.
The third part will deal with intellectual property rights. This part will focus on the rights governing works of architecture. Are there any rights applicable on works of architecture and under what conditions?
The fourth and final part will focus on the INSPIRE directive of the EU. The goal of this directive is to establish the interoperability of environmental databases or databases that can be used for environmental policy. The question will be here if URBAN or any part of it falls within the scope of the directive and the consequences of the directive in that case. These consequences will be situated on the technical side of the database, since the directive focuses on the technical interoperability of databases.

II. IMPLICATIONS OF LEGISLATION ON PERSONAL DATA

II.1. A concept of privacy

Privacy is a broad concept. To give an accurate positive definition is impossible. It is not even necessary, because the main issue is the protection of personal data. The goal of the research is to determine how the images must be treated in they contain information regarding a natural person. An image of a person is considered personal data, as we will clarify later. Therefore it is protected under the data protection rules[1].

Privacy could be defined as contextual integrity, as done by Helen Nissenbaum[2]. From the start she narrows the field to informational privacy. In order for privacy to be respected, there is a need for contextual integrity, meaning that there is a need for compatibility with reigning norms of information appriopriateness and distribution. There are norms of information flow that govern contextual integrity. She posits two families: norms of appriopratenes and norms of distribution. The norms that govern the informational flow depend on the context. Every context has its own set of norms. Nissenbaum takes a very facutal approach to determining the privacy. Nissenbaum tries the positive approach; she tries to define when something can be qualified as private.
Privacy can also be defined through specific infringements upon privacy[3], as is done in the taxonomy of privacy of David Solove[4]. He does not limit his scope to personal data. He shifts focus from the vague term privacy towards specific activities that pose privacy problems. Solove considers that we first must understand the problems before we start evaluating privacy legislation. He defines four main categories of infringements, all divided in furder subcategories. Some subcategories are similar, yet different according to him. The first group of activities concern information collection. The second group concerns storage, use and manipulation of information. The third group concerns the dissemination of information. The fourth group concerns invasions into people's private affairs. Solove takes a more negative approach[5]; he tries to indicate the cases when privacy is at risk instead of defining what privacy is.
Most subcategories are related to personal data. This is a hot topic in today's privacy discussions because of the increased technological capabilities. Good examples of these are the subcatergories of aggregation and secondary use. Through aggregation we are capable of drawing up a comprehensible profile of a person from fairly meaningless data. The unit is more than the sum of its components. That is a serious threat to privacy, as is also recognised in the

[1] Opinion 4/2007 on the concept of personal data, Art. 29 Working Party, WP 136, Art. 29 website
[2] Nissenbaum, Helen F., "Privacy as contextual integrity", *Washington Law Review*, Vol. 79, No. 1, 2004, Available at SSRN: http://ssrn.com/abstract=534622
[3] Peck vs. UK, ECHR 2003; Von Hannover vs. Germany, ECHR 2004
[4] Solove, Daniel J., "A Taxonomy of Privacy", *University of Pennsylvania Law Review* 2006, vol 154, available at SSRN: http://ssrn.com/abstract=667622
[5] A truly negative approach would be to define privacy by what it is not.

Europe[6]. This also relates to secondary use, which is the use of data for another purpose than that for which it has been collected. Because most data is saved in an electronic format, it is much easier to use and transfer. This also means that the data could end up with people who should not be able to obtain it.

You could make two main distinctions when discussing privacy. One the one hand there is the protection from physical intrusions into the private sphere. In this case it is mainly discussing searches and detention of people. These are all on a sentient level. You are aware of these facts.
On the other hand there is the protection of personal data. Personal data is situated on a subliminal level, almost a surreal level. That makes protecting it complex and sometimes difficult to grasp. Personal data protection is currently the most debated part of privacy protection and is also the topic of the privacy analysis made in this deliverable. It has come to the forefront because of the advance in ICT. But we will return to that further on in the deliverable. Personal data is defined as data relating to an identified or identifiable natural person. The word identifiable is crucial in this definition, for it enlarges the scope considerably. A person is identifiable if he is identifiable by means reasonably expected to be used[7]. To determine reasonably, we must balance the cost of the operation of identifying the person with the value of the information gathered through this identification. This balancing requires a case-by-case approach, depending on the means and capabilities of the processor.
This definition has one major consequence. Information that is not classified as personal data under this definition, will qualify as anonymous information. And anonymous information can be processed and transmitted freely.

Our field of research will thus deal with personal data protection. We will discuss both the European framework as the Belgian frameworkFor this we will examine different research questions in chapter 3 of this deliverable.
The first is whether the images made can be made at all. Can images be qualified as personal data? Is it allowed to drive around in a van and make pictures of people present?
The second one will concern the conditions for processing. When can you process data? What data can be processed? What are the obligations for the controller? What about the storage of the images? These are just some of the questions that can be raised in this regard.
The third question will concern the storage of the images for use at a later stage or for different purposes. Is this possible? What are the conditions? Are there any special requirements?

II.2. Principles of personal data protection

[6] Recital 4, Directive 95/46/EC
[7] Recital 26, Directive 95/46/EC; Peck vs. UK

There are some general principles in Data Protection that we want to point out before actually working on it. Actual references to these principles will be made further in this deliverable where they will be examined further.

The first principle is that personal data cannot be processed without the consent of the data subject. You could state that the data subject has property rights over his personal data. The data subject has the right to decide who gets acces to his personal data and who doesn't. Therefore consent is one of the main items when discussing personal data, since only he has the discretion to decide over the use of his personal data.

The processor also has to abide with certain duties and obligations. Those concern the information to the data subject and eventually the governement, as well as the lawfulness and security of the processing. You could make a case for a licensing agreement between the data subject and the processor. The processor is entitled to use something to which the data subject holds the exclusive rights, but he does not obtain the property rights. The property rights remain with the data subject.

For some processings, there is an obligation to notify the national data protection authority before starting the processing. These processings can then be scrutinized by the national Data Protection Authorities. Some processings are not subject to notification, but in some cases Data Protection Authorities can request a notification when they deem it necessary. These notifications are kept in a public registry, accessible to the public[8].

A fourth principle in EU Data protection is that Member States decide on how to implement the EU directives. The Directive lays down the principles of EU personal data protection, the goal if you will; but the Member States are free to choose the means to achieve the goal set forth by the EU. How the data protection is organised practically is part of the policy of the Member State. This is a basic principle of European law that also goes for directives in other domains of EU legislation.

A fifth principle is that anonymous data is free for processing. This also applies to anonymised data; this is personal data that has been stripped of everything that could lead to the identification of the data subject.

Every Member State must establish a national Data Protection Authority (DPA), while on the European level, the Art. 29 Working party[9] is established and a European Data Protection Supervisor.

[8]The site of the Belgian Privacy commission provides on its home page a direct link to the public registry of processings: http://www.privacycommission.be/nl/

[9] named after the article of 95/46/EC by which it has been established.

The working party and the national DPA's issue opinions on matters relating to personal data protection; next to being privacy watchdogs. These opinions are a major help when applying the directive.

There are two key functions when it comes to processing personal data. One is the controller, the other the processor. The controller is the 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[10]. The processor is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller[11]. What immediately shows from these definitions is that the processor is the subordinate of the controller. As we will demonstrate later, he can only act on authority of the controller. As a result of this relation, the controller will be responsible for anything going wrong while processing personal data.

II.3. In practice: Google Street View

I.3.1. Overview

Google Street View is embedded in Google Maps[12]. At certain locations it allows people a street level view of the surroundings. These pictures have been taken using cars with cameras fixed on the roof. It has been also the source of controversy both in the US and in Europe[13]. Google has foreseen an option to tag images that one wants removed, but that does not do away with an infringement upon personal data protection rules[14]. This is similar to the geographic surveillance in URBAN. Therefore it is interesting to see how Data Protection Authorities deal with Street View and what limitations are or are not imposed upon Street View. These will give an indication to limitations applicable on the URBAN project.
Street View is an upgrade of Google Maps, which was also intensely scrutinized when it was first released. For some people Google Maps was already a bridge too far, but resistance has largely faded away and the popularity of the tool increases every day while resistance seems to fade away.

I.3.2. Compliance with data protection rules

The main point of interest is the approval of Google Street View by the UK Information Commissioner's Office (ICO). Google blurred faces of people and

[10] art. 2(d), 95/46/EC
[11] art. 2(e), 95/46/EC
[12] http://maps.google.com/help/maps/streetview/
[13] X., "Google Street View gets go ahead", news.bbc.co.uk, 31/07/2008; Robertsen, S., "Google's Street View could be unlawful in Europe", OUT-LAW News, 5/06/2007
[14] Robertsen, S., *id*; IBLS editorial department., "Google Street View now in Europe, Raising Privacy Concerns", www.IBLS.com, 09/06/2008

license plates of cars to avoid privacy issues[15]. Furthermore the ICO said that altough in some cases identification might still be possible, Google's aim is to capture images of streets and not people. What is interesting about this decision is that it takes the intention of the application into account when determining whether the processing is lawful. The question that rises is whether this position could be followed by other EU National Data Protection Authorities (DPA). It is very well possible this position will be limited to the UK, since it are the Member States who decide how they implement the EU Directives.
In France the blurring is not satisfactory for the French National Data Processing and Liberties Commission (CNIL)[16]. For them it is a step in the right direction, but the technology itself is not perfect. This is demonstrated by the faces of people still being visible in certain areas. Google in turn replied there is still a link available to indicate a picture one wants removed. This does not do away with the fact that the technology is not reliable, which is the case made by CNIL.
We have two European Data protection authorities, both with a different vision. But as we will explain further on, both legislations have the same foundation.

The second point of interest is that Google notified to CNIL prior to gathering the images on city streets. In Belgium there is also a notification system for personal data processing, so we will have to assess whether prior notification is necessary in Belgium as it is in France.

I.3.3. What is different for URBAN?

Where URBAN differs from Street View is that URBAN does not distribute the images gathered as does Google. They might be stored for later use, but they will then only be accessible to a limited number of people with the apriopriate acces permissions. Street View is accessible by all through the internet.
A second difference is that the images are used as a starting point to construct the 3D city models. These city models will be derived from the images using object recognition software that will only take works of architecture into account. This means that personal data contained within the images will be filtered out during the modelling proces, whereas in Street View, the images are distributed as they have been captured. The only change that has been made is the blurring of faces and license plates. For URBAN, anything that is not a construction, e.g. persons and cars, is an imperfection in the model and must thus be eliminated.

[15] X., "Google Street View gets go ahead", news.bbc.co.uk, 31/07/2008; Reardon, M., G"oogle Street View is approved for the U.K.", news.cnet.com, 31/07/2008
[16] Gijzemijter, M., "Google past waasfilter toe op Franse StreetView", webwereld.nl, 4/07/2008; Sayer, P., "Google blurs faces to protect privacy in French StreetView", www.networkworld.com, 03/07/2008

III. CONDITIONS FOR PERSONAL DATA PROTECTION

III.1. Directive 95/46/EC[17]

This Directive is the main legislative body of personal data protection in the EU. In some areas, sector-specific directives have been adopted to deal with specific issues. Their provisions will have priority over conflicting provisions of 95/46/EC.

III.1.1. Scope

III.1.1.a. General

The first part of the scope of the directive can be found in article 3. It is aimed at processing of personal data by automated means or otherwise if it is intended to be part of a filing system. An automated processing always falls within the scope of the directive; it does not matter that it is not intended to be part of a filing system. It is widely acknowledged that technology is a serious threat to personal data, mainly because it allows constructing comprehensive profiles from on itself meaningless data[18]. Processing of personal data in the course of an activity which falls outside the scope of Community or done by a natural person for a purely personal or household activity fall outside the scope of this directive.

Personal data is any information that relates to an identified or identifiable natural person[19]. The art.29 Working Party has issued an opinion regarding the concept of personal data[20]. This opinion was issued as an answer to counter uncertainty and diversity in practice in EU Member States with regard to basic definitions of the directive; especially regarding the concept of personal data. The following will be a summary of the art. 29 Working Party opinion.
The Working Party distills four building blocks from the definition of personal data. These are any information, relating to, identified or identifiable and natural person.
The first is “any information”. This refers to the *nature* of the information. It can be *subjective or objective*. Whatever the tabloids write about a person is considered personal data as is what is written in regular newsmedia. There is no requirement for the information to be true for it to be personal data. It also refers to *content*. Any sort of information regarding a natural person is personal data. What is actually transmitted about a person does not matter, what matters is that something has been transmitted about a person. This also refers to the *format* of the information. Whatever the shape or form of the information it is considered

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281, 23.11.1995, p. 31–50
[18] recital 14 and 26 95/46/EC; D., Solove, *o.c.*, p 505-510
[19] art. 2(a) 95/46/EC
[20] ART. 29 WORKING PARTY, Opinion 4/2007 on the concept of personal data, WP 136, Art. 29 Working Party website

personal information. This is also clearly voiced in the recitals of the Directive[21]; with a specific reference towards image data.
The second building block is “relating to”. Information can relate to natural persons in three ways. The first is *content*. It is information concerning a particular person. In this case the information directly concerns an individual and actually tells you something about that person. The second is *purpose*. The information is likely to be used to evaluate, treat in a certain way or influence status or behaviour of a person. The use of certain information can make the information personal data. A third is *result*. Information can relate to person if it is likely to have an impact on his rights and interests. This impact need not be an major impact. It is sufficient if the person may be treated differently than any other person as the result of the processing of such data. In any of the three cases described information is considered as relating to a person; so they need not be fulfilled at the same time. What this also points out that even if information does not focus on a person, it can still be considered personal data. This is in stark contrast to the decision of the UK DPA when considering Google Street View. They gave the green light, despite faults in the system allowing identification, because the focus was on the streets and not on the persons. But we might see a case of result as a consequence of Google Street View. This judgement may well not be followed elsewhere.
The third building block is the most elaborate and in my view the most important. It is “identified or identifiable”. Identification happens through pieces of information relating to a person, called identifiers. A person is identified within a group of persons if he can be distinguished from others in that group. Identifiable is a person who has not yet been identified, but who could be. A person can be directly or indirectly identifiable. *Direct Identification* mostly refers to identification through the name, the most common identifier, although this will not always be sufficient if for example the surname is quite common. *Indirect identification* comes from a unique combination, small or large, of identifiers; specific to his physical, physiological, mental, cultural or social identity. These identifiers may not even include the name; it is sufficient that the person can be distinguished from others in the same group. The directive says that we must take into account *all means likely reasonably to be used to identify a person* by the controller or a third party. The first thing this statement wants to exclude is the mere hypthetical possibility to single someone out. There must be a real possibility to identify a person. Secondly, the statements compells to take a maximum of factors into account. It is a dynamic test; we must look at the state of the art of technology available to identify the person but also possible evolutions that take place during the processing. So the longer the data are stored, the more a person is likely to be identifiable. We must also look at the purpose of the controller. In some cases a processing only makes sense if the data subject can be identified. In those cases it must be prevented that the legislation is circumvented through declarations that are contrary to the processing. We must look at the actual facts of the processing and disregard the form of the processing. Another factor is the value of the data balanced against the cost of identification. We must also look at

[21] recital 14 95/46/EC

the technical and organizational measures put in place by the controller to prevent identification. If these measures are adequate enough, a data subject may not be identiafiable and the data regarded as anonymous. One of these measures might be the use of pseudonymised data. This means that the real identity of the data subject has been disguised. Pseudonymised data might be data on a subject that might be indirectly identifiable. The effectiveness of pseudonymisation depends on the means and technology that is used in the process. An example of pseudonymised data is key-coded data. In this case pseudonym (a code) is separated from the common identifiers of the data subject. Identification requires a key, which is held separately.
The fourth and final building block is that the information must relate to a "natural person". With this denomination a human being is meant. Legal persons do not fall within the scope of this Directive.
The opinion concludes with a very meaningful sentence. The members of the Working Party, respresentatives of DPA's, are committed to further developing the guidance provided in this opinion. This means that this opinion will determine to some extend the interpretation of national data protection legislation.
Then there is the question what is considered processing. Processing is any operation or set of operations that can be carried out on personal data[22]. So, anything that can be done with personal data is considered processing of personal data.

The second part of the scope of the directive can be found in art. 4 of the Directive. This article states when national law should be applicable. National law is applicable if the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. When he is established in several Member States he must comply with obligations laid down in the national regulations of each the Member States where he has an establishment. It also applies when the establishment is not situated in the Member State's territory, but in a place where its national law applies by virtue of international public law.
A third situation is where the controller is not established on Community territory, but makes use of equipment for the processing of personal data, automated or otherwise, situated on the territory of the said Member State. This does however not apply if the equipment is only used for the purposes of transit through the territory of the Community. When the equipment is used for anything more than transit through the territory of the Community; the controller must conform to the principles of the Directive. In this case he must also designate a representative established in the territory of that Member Sate. This does not prejudice any legal action that could be initiated against the controller himself.

III.1.1.b. Applicable on URBAN?

The directive is applicable on URBAN since a collection of personal data is also considered as processing of personal data. It doesn't matter in what shape or

[22] art. 2(b), 95/46/EC

form the data is collected. This means that the principles laid down in this directive must be upheld by the data controller for URBAN. How the rules must be upheld in practice will depend on the regulations drawn up by the Member States. They are responsible for implementing the principles into national legislation and as such decide how they implement the legislation.

III.1.2. Legitimacy of processing

In this part we will elaborate when you can process data and what data can be processed. This has been extensively regulated in the directive although there is still room left for policy by the Member States. At first we will discuss what data can be processed. Secondly we will discuss when this processing can take place.

Data protection rules make a distinction between two kinds of personal data: personal data and sensitive personal data. Sensitive personal data is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life[23]. Data that does not fall within either of these categories is considered personal data. Sensitive personal data is personal data, but not all personal data is sensitive personal data. This difference is important because only personal data can be processed. The processing of sensitive personal data is prohibited[24].

The next part will deal with the legitimacy of processing. Here again we must distinguish between the legitimacy of processing of personal data and sensitive personal data.

We will commence with the processing of personal data[25].

1. Unambigious consent given by the data subject.
2. Performance of a contract to which the data subject is party.
3. Compliance with a legal obligation to which the controller is subjected.
4. Processing in order to protect the vital interests of the data subjects.
5. Necessity to process data for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller or in a third party to whom the data are disclosed
6. Processing necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under article 1(1) of the Directive.

For any of the cited goals the processing of personal data is legitimate. If the processing is done for another goal, the processing is illegitimate. The law can

[23] art. 8, 95/46/EC
[24] art. 8.1, 95/46/EC
[25] art. 7, 95/46/EC

impose a processing of personal data, but this processing must have a precise goal[26]. The main importance of this primary goal is to establish whether any secondary processings of the same data are compatible with the primary goal.
The legitimate goals of personal data do not apply to sensitive personal data.
For sensitive data, the Member States have the power to decide on allowing consent as a legitimate ground for processing sensitive data[27]. The position of the Directive is that consent does legitimate processing of sensitive personal data.
Processing is also allowed when they are needed for obligations and rights the data controller has in the scope of employment law. It is limited to what is allowed by national law providing for adequate safeguards.
When the data subject legally or physically cannot give his consent, processing is allowed when it is needed to protect the vital interests of the data subject or another person.
The data can be processed when it has manifestly been made public or is necessary for the establishment, exercise or defense of legal claims.
Member States may lay down extra exemptions for reasons of substantial public interest. These exemptions can be given by national law or in a decision of the national supervisory authority. This exemption allows Member States room for a policy in line with their need and privacy culture. In the UK, for example, privacy protection is less strict than in France as we have seen when discussing Google Street View.
The prohibition of the processing of sensitive data shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.
There is also a specific section concerning criminal records and the processing of data regarding administrative recourses. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of an official authority.

[26] Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 36/2008 van 26 november 2008, Advies inzake het ontwerp van decreet betreffende het Centraal Referentieadressenbestand (hierna het CRAB) (A/2008/042); Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 32/2008 van 24 september 2008, Advies inzake het voorontwerp van decreet betreffende de Geografische Data-Infrastructuur Vlaanderen (A/2008/032)
[27] art. 8, 95/46/EC; only 8(d) has been left out because it is out of scope since we are not dealing with foundations, associations or any other non-profit-seeking body.

Art. 9 of the directive tries to preserve the freedom of speech. Member States are allowed to provide exemptions or derogations from Chapters II, IV and VI[28] of the directive for processings of data carried out solely for journalistic purposes or the purpose of artistic expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression. It is important to note in this article that it is the prerogative of the Member States to decide when such a balancing of rules is needed and how they implement it.

III.1.3. Conditions for processing

The EU has imposed strict conditions on the processing of personal data. Some of these have already been pointed out when outlining the principles of personal data protection.

First of all, the controller, or his representative[29], has a duty of information towards the data subject. This duty of information depends on the source of the personal data. If the data is gathered directly from the data subject, the controller must provide him with the identity of the controller and, if any, his respresentative, purpose of the processing and further information[30]. This further information relates to the recipients or category of recipients of the data; whether replies to the questions are voluntary or obligatory and the consequences of the failure to reply; the existence of a right of acces to and the right to rectify his data. This further information must be given if it is necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the data are collected. If the data subject already has this data available, he does not need to provide it again. The data might not be obtained from the data subject[31]. In this case the processor or his representative must provide the data subject with the identity of the controller and of his representative, if any, the purpose of the processing and further information. This further information relates to the categories of data concerned, the recipients or category of recipients and the right of acces to and the right to rectify the data concerning him. This further information must only be provided if necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the data are processed. It is important to note that Member States are allowed to restrict the scope of the rights and obligations of information in some cases[32].

The controller must watch over the confidentiality and the security of the processing of personal data. Confidentiality is in essence protecting against leaks of information by persons having acces to the information. Security is in essence protecting against outside threats. Data can only be processed on authority of the

[28] This means art.5-21, art.25-26 and art.28-30.
[29] art. 4.2., 95/46/EC
[30] art. 10, 95/46/EC
[31] art. 11.1, 95/46/EC; art. 11.2 is out of scope for URBAN
[32] art. 13, 95/46/EC

controller or when required to do so by law[33]. This goes for any person acting on the authority of the processor or the controller, including the processor, who has acces to personal data. The controller must implement appropriate technical and organizational measures to protect the integrity of personal data[34]. This means that data must be protected from accidental or unlawful destruction or accidental loss… This is however not an absolute requirement. The measures must ensure an appropriate level of security compared to the risks represented by the processing and the nature of the data to be protected; having regard to the state of the art and the cost of the implementation of the security measures.
If the controller has a processor to do the processing on his behalf, he must choose a processor that provides sufficient guarantees with respect to the security of the processing[35]. There must be a contract between processor and controller concerning the processing, which must state that the processor can only act on authority of the controller and that the processor must also oblige with the security provisions in the national data protection legislation of the Member States where it is established[36]. The parts of the contract or the legal act relating to data protection and the requirements relating to the technical and organizational measures must be in writing or any other equivalent form[37].

Thirdly there is a duty of notification to the supervisory authority. Prior to carrying out a wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes, the controller or his representative must notify the supervisory authority of the Member State of establishment[38].
Processings can benefit from an exemption of notification or simplification of notification in two cases, ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations[39].
The first case are the categories of processing operations which are unlikely to adversely affect the rights and feedoms of data subjects, taking into account the data to be processed. In this case they must specify the purposes of the processing, the data or categories of data undergoing processing, the category or gategories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored.
The second case is where the controller appoints a personal data protection official, in compliance with the national law which governs him. This official must be responsible for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive and for keeping the register of the processing operations carried out by the controller, containing specific information regarding to the processing[40].

[33] art. 16, 95/46/EC
[34] art.17, 95/46/EC
[35] art. 17.2, 95/46/EC
[36] art. 17.3, 95/46/EC
[37] art. 17.4, 95/46/EC; for the purposes of proof
[38] the geographic scope of the directive has been mentioned previously
[39] art. 18.2, 95/46/EC
[40] this information is contained in art. 19.1 (a)-(e)

The notification must include at least the name and adress of the controller and of his representative, the purpose or purposes of the processing, a description of the category or categories of data subject and of the data or categories of data relating to them, the recipients or categories of recipients to whom the data might be disclosed, proposed transfers to third countries and a general description allowing a preliminary assessment to be made of the appriopratenes of the measures to ensure security of the processing. If any of these data is changed after the notification, these changes must also be notified.

III.1.4. Rights of Data Subject

The data subject does not waiver his rights to control over his personal data by consenting to the processing or transfer of his personal data. He still retains a certain amount of control over the content and the use of his data.
The data subject has a right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed[41]. Ensuing he has the right to be informed in an intelligible form of the data undergoing processing and of any available information as to their source[42]. He is also entitled to know the logic involved in any automatic processing of data concerning him. Especially for automated decisions which produce legally affect him or significantly affect him and which decisions are based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness and reliability[43].
The data subject is also entitled to rectification, erasure or blocking of data which is not processed in compliance with the directive, in particular because of the incomplete or inaccurate nature of the data[44]. This right is also established in the case law of the European Court of Human Rights. In the case Rotaru vs. Romania it was decided that the data held by the Romanian Intelligence Service had to be erased and that it was not enough the data had been acknowledged by the court as not relating to mister Rotaru. The case was seen as an infringement upon art. 8 ECPHR[45]. Romania acknowledged that they infringed upon this article but in defense claimed this infringement to be justified[46]. The Court, however, was of the opinion that the legal grounds cited by the Romanian governement did not provide adequate safeguards needed to comply with art. 8 ECPHR[47]. Information affecting national security may be gathered, recorded and archived in secret files. There are however no safeguards in national law to

[41] art. 12 (a), 95/46/EC
[42] idem
[43] idem juncto art. 15, 95/46/EC
[44] art. 12(b), 95/46/EC; Rotaru vs. Romania, ECHR 4 may 2000
[45] referred to in recital 10, 95/46/EC
[46] Rotaru vs. Romania, ECHR 4 may 2000, nr. 47
[47] idem, nr. 61

impose any limits on the exercise of those powers[48]. Therefore, the Court deemed the measure disproportionate and as a result the infringement on art. 8 ECPHR was deemed illegitimate.
The data controller has the duty to notify third parties to whom data have been disclosed of any erasure, rectification or blocking carried out on request of the data subject. He is exempted from this obligation if this notification proves to be impossible or involves a disproportionate effort.

The data subject als has the right to object to the processing of his personal data in two cases.
The data subject can object at any time against the processing in accordance with art. 7 (e) and (f)[49] of his personal data on compelling legitimate grounds relating to his particular situation, provided that national legislation does not contain contrary provisions[50]. When this objection is justified, the controller can no longer process the involved data.
Secondly the data subject also has the right to object to the processing of personal data which the controller anticipates being processed for the purposes of direct marketing[51]. Member States must take the necessary measures to inform people about this right of objection.
Thirdly the data subject has the right to be informed before personal data are disclosed for the first time to a third party or used on their behalf for direct marketing and to be expressly offered the right to object free of charge of such disclosure or uses[52].

The data subject also has the right to compensation for damage suffered due to an illegitimate processing of personal data or any act incompatible with the national legislation pursuant to this directive[53]. The data subject is also entitled to judicial remedies for any breach of the rights guaranteed to him by national law applicable to the processing in question[54]. These articles are very important for the data subject. . For this we must relate to the Francovitch case of the European Court of Justice[55]. In this case Italy was held liable because it did not

[48] idem, nr. 57
[49] Article 7
Member States shall provide that personal data may be processed only if:
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).
[50] art. 14(a), 95/46/EC
[51] art. 14(b), 95/46/EC
[52] idem
[53] art. 23, 95/46/EC
[54] art. 22, 95/46/EC
[55] Andrea Francovich and Danila Bonifaci and others vs. Italian Republic, ECJ 19 November 1991, *ECR* 1991, I-05357

implement a directive in national law. This liability, however, is conditional. The directive must be precise enough to ascertain who is entitled to the protection and it is clear which rights are granted to that person. If these two conditions are not met, the Member State cannot be held liable for the lack of or improper implementation of the directive. The legal grounds for this liability are found in the EU Treaty, which states the obligations of the Member States towards the EU.
If these rights are not or not adequately implemented in the national law of the Member State, the person suffering damages can hold the Member State liable for his damages. The subject of the rights is clear, the data subject, as well as the scope of the rights, damages and judicial remedies against illegitimate processing.

III.1.5. Impact on URBAN

The actual impact of this directive may surprise most people. It has little to no direct impact on URBAN. The Directive only sets out the principles the EU wants to see implemented with regard to the protection of personal data. The EU also decides upon the definitions used. How this protection is realised in practice; is subject to the Member States discretion. However, interpretation of national law will have to be done in accordance with the Directive. So the actual data protection is set up by the Member States[56]. This allows policy room for the Member States to take the measures that best suit their national situation. This also implies that there will be differences in the implementation of the Directive. Therefore it is necessary to assess the situation in every Member State separately, as is indicated in the directive[57]. This makes EU data protection law so complex; no two Member States share the same rules.

III.2. 2002/58/EC[58] and 2006/24/EC[59]

III.2.1. Scope

III.2.1.a General

The scope of both Directives is electronic communications. 2002 is oriented at creating a sector-specific data protection framework in addition to directive

[56] e.g.: art. 18.1, art. 20.1, art. 21.1 95/46/EC. All articles state that the Member States shall detemine this, take measures to ensure that,… It states what Member States must do, but not how it should be done.
[57] art.15.2(b), art. 4.1(a)-(b), 95/46/EC
[58] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ* L 201 , 31/07/2002, p.37-47
[59] DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *O.J.* L 105, 31/07/2002, p. 54-63

95/46/EC. 2006 is the data retention directive and is a harmonisation directive aimed at clarifying certain provisions of the 2002 directive.

III.2.1.b. Applicable on URBAN?

Neither of these directives is applicable on URBAN since URBAN doesn't qualify as electronic communications. Therefore these two directives will no longer be taken into account for this deliverable. This also expands to the Belgian National legislation that is derived from both of these directives[60].

III.3. Personal Data Protection Act 8 December 1992[61] (WVP)

III.3.1. Scope

III.3.1.a. General

The WVP defines its material scope as follows: it applies to every partly or fully automated processing of personal data or any non-automated processing of personal data that are filed or destined to be filed[62]. It does not apply on processings done by a natural person for strictly personal or domestic purposes.
As far as the definition of personal data is concerned[63]; this definition is a literal translation of the definition found in the directive. The same goes for the definition of processing.

The geographical scope is defined as follows[64]: it applies to establishments, concerned with processing, of the controller on the Belgian territory or any location where Belgian law is applicable by virtue of international private law. It also applies for processings by a controller without an establishment on the territory of the EU if he uses means, automated or not, on Belgian territory; unless these are only used for the *transfer* of personal data through the Belgian territory. In this case he must also appoint a representative in Belgium. This does not impede legal action against the controller. It is important to know that the law will apply even in cases where non-automated means are used for the processing, this contrary to the material scope of the WVP. In the material scope non-automated processings are only concerned when they are part of a file or destined to be part of a file.

III.3.1.b. Applicable on URBAN?

[60] Wet 13 maart 2005 betreffende de elektronische communicatie, *B.S.* 20/06/2005, p. 28070
[61] Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 18 maart 1993 aangevuld door K.B. 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 13 March 2001, p7908-7919
[62] art. 3 §1 WVP
[63] art. 1§1 WVP
[64] art. 3bis WVP

Is URBAN a processing of personal data as defined by the WVP? Yes, because also images are considered to be personal data[65]. They allow an individual natural person to be singled out within a group for whatever purpose. This makes that URBAN falls within the material scope of the WVP.
The second question is whether URBAN falls within the geographical scope of the WVP. This is also the case since the equipment used to collect the data will be situated on the Belgian territory, but also because it is done by a company with a permanent establishment on the Belgian territory[66].

III.3.2. Criteria for processing

The law clearly defines when processing of personal data is legitimate; but distinction is made between four categories of personal data. We will discuss them in the order as they can be found in the WVP.

The first category is personal data[67]. Processing is legitimate in case the data subject has unmistakably given his consent to the processing. Processing is also allowed when it is needed for the execution of a contract to between the data subject and one or more other parties. The third situation is when there is a legal obligation to process personal data. Personal data can be processed when they are needed to preserve a vital interest of the person concerned. Sometimes a processing has to be done on authority of the governement for matters of public interest; in these cases processing of personal data is also allowed. The last ground for legitimate processing is the necessity to preserve a justified interest of the controller or a third person to whom the data will be transferred, on condition that the rights and freedoms of the data subject do not outweight this justified interest. In this case there is a balancing of interest needed, requiring a case by case approach. Housenumbers can be personal data in as far as they can be linked to a natural person[68]. This is in the Belgian framework fairly easy given the data that is already available in places such as kadaster. Nevertheless, the Privacy Commission does not consider the implementation of the Centraal Referentieadressenbestand in the Geografische Data-infrastructuur Vlaanderen to have any meaningful impact on the private life despite the fact that some data will be publicly accessible[69]:

> De Commissie stelt vast dat enkel de volgende gegevens publiek toegankelijk worden gemaakt: straat, huisnummer, huisnummerlabel, gemeente, postcode, NIS. Zoals reeds

[65] ART. 29 WORKING PARTY Opinion 4/2007 on the concept of personal data, WP 136, p 7
[66] see project proposal, and more precisely list of participating companies and research groups
[67] art. 5 WVP, comparable to art.8 95/46/EC
[68] Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 32/2008 van 24 september 2008, Advies inzake het voorontwerp van decreet betreffende de Geografische Data-Infrastructuur Vlaanderen (A/2008/032)
[69] Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 36/2008 van 26 november 2008, Advies inzake het ontwerp van decreet betreffende het Centraal Referentieadressenbestand (hierna het CRAB) (A/2008/042), nr. 35

> aangehaald (cf. randnummer 15), is de Commissie van oordeel dat door de openbaarmaking van deze gegevens de mogelijke gevolgen voor de persoonlijke levenssfeer eerder beperkt zijn. Zij ziet dan ook geen bezwaren tegen de publieke toegankelijkheid van deze informatie.

Whether this would change for a 3D-City model is unclear, but given the fact that in that case there is no personal data as long as it is not linked to a natural person, it seems to add little to the situation with regard to CRAB.
To obtain this name directly from the CRAB what is not made public, one has to pass by a committee that will have a crucial role[70].

Then we have three special categories of personal data: Sensitive personal data, medical data and litigation data.
It is prohibited to process sensitive personal data. Sensitive data refer to a person's religious or political beliefs, membership of a union, sexual life and racial and ethnic origin. This definition is a bit narrower than that found in the directive[71]. Important to note with regard to these data are only qualified as sensitive when the goal of the processing is the processing of these personal data[72]. Furthermore, one needs to be able to establish for certain or with an almost certain probability that these data are true[73]. There are exceptions to this prohibition[74]. The first exception is a written document from the data subject expressing his consent to the processing. Prior to obtaining this consent the processor must inform the data subject of the reasons for the processing and provide him with the list of the *categorie*s of persons who have acces to these personal data[75]. The consent is not valid if the controller is the current or future employer of the data subject or if the subject is dependant on the controller which prevents him from consenting freely[76]; unless the processing grants him a benefit. The controller is allowed to process data when he is obliged or entitled to by labour law provisions providing for sufficient safeguards. Processing is also allowed to protect a vital interest of the data subject or another person if the data subject is not able, legally or physically, to give his consent. Processing is also allowed when the data have been clearly made public by the data subject. 'Clearly made public' must be interpreted strictly. The data subject must have taken the initiative to make the data public. Processing is also allowed for another reason of considerable public interest, allowed by a law[77]. Member states can decide autonomously over these reasons, in accordance with the rules in European law regarding the qualification of 'law'.

[70] Advies 36/3008, nr. 37
[71] art. 8, 95/46/EC
[72] B.,DOCQUIR, "le droit a la vie privée", de boeck Larcier, Brussels, 2008, nr. 490
[73] idem, nr. 486
[74] art. 6 §2 WVP; only those relevant to URBAN will be treated
[75] art. 26 K.B. 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 13 March 2001, p7908-7919
[76] art. 27 K.B. 13 februari 2001
[77] Law, ordonnance or decrete, depending on which governement has the authority under Belgian institutional law.

The two other kinds of sensitive data are medical data and data relating to court or administrative proceedings[78]. Medical data relate to a person's health status. Data that only allow deducting a person's health status are not covered by this protection, such as photographs of a person in his wheelchair[79]. Medical and litigation data will not be discussed because they are out of scope for URBAN.

III.3.3. Conditions imposed upon processor

First there are five general conditions for the processing of personal data[80]. The controller is responsible for enforcing these conditions. The conditions are:

1. Personal data must be processed fairly and legitimately.
2. The data must be obtained for a specified, clearly defined en justified goal and cannot be processed in a way incompatible with this goal. The goal is defined by the controller[81].
3. The data must be relevant and proportionate with regard to the goal for which they were obtained or processed.
4. The data must be accurate. Alle reasonable means must be used to correct or erase inaccurate data.
5. They should not be kept longer than necessary for the realisation of the goal; at least not in a form which allows for the identification of the data subject. This means that the data must be either erased or anonymised

If the controller entrusts a processor with the processing of personal data the controller, or his representative in Belgium, must choose a processor who offers sufficient technical and orginazational security measures for the processing to be done[82]. The controller must enforce these measures, notably by fixing them in contractual clauses[83]. The contract must also establish the liability of the processor towards the controller[84]. The contract must also state that the processor can only act when ordered by the controller unless the processing is ordered by law[85]. He must also determine the elements of the agreement regarding the protection of the data in writing or on an electronic medium[86].

The controller should also limit acces permission and processing means of persons working on his behalf to what is strictly necessary[87]. He must also inform these persons of the relevant legislation and of the instructions for the protection

[78] art. 7-8 WVP
[79] idem, nr. 504-506
[80] art. 4 §1 WVP
[81] art. 1 §4 WVP
[82] art. 16 §1 1° WVP
[83] art. 16 §1 2° WVP
[84] art. 16 §1 3° WVP
[85] art. 16 §1 4° juncto art. 16 §3 WVP
[86] art. 16 §1 5° WVP
[87] art. 16 §2 2° WVP

of personal data during processing[88]. The controller or his representative in Belgium must monitor closely that inaccurate, incomplete, illegitimate and irrelevant data are updated or erased[89]. The controller must also ascertain that the programs used for the automated processing are in accordance with the prior notification done to the Belgian Privacy Commissoin[90].

Then there are requirements regarding the confidentiality and the security of the processing[91]. The controller also has the duty to warrant the security of personal data[92]. He or his representative in Belgium must take all appropriate technical and organizational means necessary to prevent destruction, loss, alteration, access or any other illegitimate processing of personal data. The appropriateness will be judged taking into account the technical state of the art and the cost of implementation of these means on the one hand and the nature of the data and the potential risks on the other hand. The Privacy Commission has elaborated a number of reference measures which we will briefly discuss[93].
Every institution processing personal data should draft a written document, the security policy, containing the detailed strategies and measures for data protection. This policy must be approved by the highest hierarchy of the company and the different responsibles and must be distributed within the company. For the execution of this security policy, the institution must appoint a security consultant. This consultant must hold the necessary competences and training and cannot hold any functions or competences incompatible with the role of safety consultant. His primary role is supervising data processing and protecting security responsibles from pressure. The institution must clearly describe the responsibilities and the management process regarding protection of personal data and integrate it in a fitting manner in the general organisational structure and operations. Disciplinary measures or an obligation of secrecy could be used for enforcement of this policy. The policy should also contain a plan of action for security incidents and continuity. This plan must contain the course of action when a security incident is discovered and who is responsible for dealing with the incident and restoring the situation to normal. The institution must guarantee the physical protection of the personal data. This can be done by placing the infrastructure in a secured location with access limited to authorised persons and the period they exercise their function, this is their working hours. If the continuity of the service must be guaranteed, which would be the case in a road tolling infrastructure, equipment must be installed to prevent, trace and combat physical threats. This equipment must be checked regularly. The institution must also ascertain that the networks to which the equipment is connected guarantee the confidentiality and the integrity of the data. Illegitimate access must be prevented. The institution must also install logging and tracing mechanisms. This

[88] art. 16 §2 3° WVP
[89] art. 16 §2 1° WVP
[90] art. 16 §2 4° WVP
[91] Chapter IV, WVP
[92] art. 16 §4 WVP; this obligation is a good illustration of how wide the scope is.
[93] Referentiemaatregelen, website CBPL:
http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf

must allow for the tracking of every person that has had access to the data or any processing of the data. These mechanisms are a processing of personal data themselves and must therefore encompass appropriate specific measures.

Before commencing any partly or fully automated processing, the controller must notify the Belgian Privacy Commission[94]. Exemptions are possible, but none apply to URBAN[95].
The content of the notification is clearly described in the law.

1. The date of the notification and the legal norm by which the processing is established.
2. The name, first name and full adress or the name and seat of the controller and his representative, if any.
3. The name of the automated processing. Every processing gets a specific name, as you would name a company.
4. The goal or the associated goals of automated processing.
5. The categories of personal data with an *explicit* description of sensitive personal data.
6. The categories of recipients to whom the data might be unveiled.
7. The guarantees that must be attached to the unveiling of data to third parties.
8. The way data subjects are notified, the service where the right to supervision can be exercised and the measures taken to simplify execution of that right.
9. The duration of storage, after which the data can no longer be kept, processed or spread.
10. A general description to assess in advance whether the means taken for security and confidentiality of the processing are sufficient.
11. The reasons of the controller for the exemptions to processing for processing for journalistic, literary or artistic purposes.

The Belgian Privacy Commission has the right to request other information in accordance with the right of control and research[96]. This information could concern the chosen means of automation, the origin of the personal data and the security measures foreseen. If the data are meant to be passed on to a third country, even if only occasionally, then the notification must also contain the categories of personal data to be transferred and for each category the country of destination[97].
The termination of an automated processing or the modification of any element of the standard notification must also be notified.
All automated processings are held in a register by the Belgian Privacy Commission[98]. This register is accessible by anyone either directly using

[94] art. 17 WVP
[95] art. 51-62 K.B. 13 februari 2001
[96] art. 17 §4 WVP; refers to the duties in art. 31-32 WVP
[97] art. 17 §6 WVP
[98] art. 18 WVP combined with art. 63-68 of K.B. 13 februari 2001

telecommunications[99] or in the rooms of the Commission destined for that purpose. Indirect access is possible by directing a request for an excerpt to the Commission; this excerpt can be requested by anyone. The consultation of the register is free and there is no obligation to give a reason for the consultation.

The controller is held liable for damage that results from any action incompatible with rules from the WVP or by virtue of the WVP; unless he can prove he cannot be held responsible for the fact causing the damage[100].

III.3.4. Rights of Data Subject

The data subject has certain rights with regards to his personal data but also with regard to the processing.

The data subject has a right to information from the controller or his representative if the data are collected from him[101]. This information must at the latest be provided at the moment the data are collected from the data subject, unless the data subject already has this information. This information contains the name of the controller or his representative, the goal of the processing, the existance of a right to object free of charge to the processing for purposes of direct marketing of his personal data and additional information. This additional information concerns the recipients or categories of recipients of the data, the possible mandatory character of the processing and the consequences of not responding and the right of correction, unless this right is not necessary to guarantee a fair processing. If the data are collected as ordered by or under authority of a law, decree or ordonnance, the data controller is releived from his information duty[102]. The Belgian Privacy Commission recommends to provide information through the appropriate channels, especially regarding the goal of the data storage, the users of the data, the data controller where the right to acces, correction and removal can be executed[103].

The data subject also has a right when the personal data is not collected of him but from an indirect source[104]. Information must be given at the moment of registration of the data or when the transfer of data to a third party is considered. The information to be given is the same as that when the data is collected from the data subject with a difference concerning the right to object processing for direct marketing. In that case the data subject must be informed prior to the first transfer of the data to a third party for direct marketing purposes or prior to the processing on behalf of a third party for direct marketing purposes. The controller

[99] Link to Belgian public register
[100] The dutch text speaks of “toerekenbaar”, which is a specific legal term meaning that the fact leading to damages can be traced back to him.
[101] art. 9 §1 WVP
[102] art. 9, §2, 2nd section b) WVP; Advies 36/2008, nr. 27
[103] Advies 36/2008, nr. 29
[104] art. 9 §2 WVP

must also ask in writing whether the data subject wishes to object to this processing.
The controller is exempt from the duty to inform the data subject when informing the data subject is impossible or would require a disproportionate effort[105]. The controller provides the information when he first enters into contact with the data subject instead of prior to the registration of the data or considering the transfer. If the data has been transferred to a third party, the third party issues this information.

The data subject who can prove his identity has a right to obtain different sorts of information from the controller[106]. He has the right to know if processings of data concerning him exist and to be informed at least of the goals of this processing, the categories of data concerned and the categories of recipients to whom the data are unveiled. The data subject must be supplied with the data, in an understandable form, that will be processed as well as any available information on the origin of this data. He must be informed of the possibility of summary judgement or the right to rectification or objecting processing[107].
The data subject has a right to have inaccurate data rectified free of charge[108]. He also has the right to object to processing of his data for ponderous and justified reasons relating to his particular situation unless these data are processed in the execution of a contrat or is mandated by law. If the objection is justified, the controller can no longer process this data. He can also apply for a ban on the processing of personal data or deletion of personal data which is irrelevant or inaccurate with regards to the goal of the processing. He can demand removal of personal data or a ban on the processing of personal data which are prohibited from registration, publication or storage or for which the storage period has expired.
When the personal data are processed for direct marketing purposes, the data subject has the right to object to his processing free of charge and without expressing a reason. If the data are collected in writing, the controller asks the data subject on the document used for the collection whether the data subject objects to processing for direct marketing[109]. If the data is not collected in writing, the controller must ask the data subject. This can be done by supplying a document at the latest two months after collecting the data or by technical means that can prove that the data subject has been asked whether he wants to object[110].

To exercise these rights he has to adress a dated and signed request to the controller, his representative or a person authorised or appointed by the

[105] art. 9 §2 2nd subsection WVP
[106] art. 10 §1 WVP
[107] art. 10 §1(d) WVP, juncto art. 12&14 WVP
[108] art. 12 §1 WVP
[109] art. 34 subsection 1 K.B. 13 februari 2001
[110] art. 34 subsection 2 K.B. 13 februari 2001

controller or the processor who transfers this request to one of the aforementioned people[111].

III.3.5 Sanctions and remedies in Personal Data Protection

We can make a division between civil remedies and criminal sanctions.

There is only a case for a criminal sanction if it is mentioned in the law and the sanction is also provided in the law[112]. In the WVP these are the articles 37 through 43. Article 37, for example, contains the sanction for members, employees or experts from the privacy who breach the duty of confidentiality. They are fined between €200 and €10000. And so are defined a number of other infringements upon the WVP. Also very important is art. 42 WVP. The controller or his representative in Belgium encounters civil liability for any processor fined under art. 38 or 39 WVP.

The data subject also has a few civil remedies at his disposition. These are all initiated in civil court, contrary to criminal sanctions that are initiated in criminal court. One of them is a curtailing action, by which he can halt any illicit processing of personal data[113]. In urgent cases the data subject can initiate a summary procedure, to obtain temporary measures while waiting for a comprehensive judgement on the case. The data subject can also claim damages from the controller for any injury he has encountered as a result of illicit processing of personal data. The controller could avoid liability if he can prove he is not accountable for the injury caused to the data subject.

III.3.6. Implementation on URBAN

The focus is on how URBAN, and in particular the aspect of geographic surveillance, should deal with the legislation that has been set out above. The reason is that the images will contain personal data as has been set out above when discussing the scope of the Directive and the WVP. The 3D city modelling aspect does not hold any privacy implications since only the structures are concerned and no natural persons. The city modelling aspect will be discussed in the chapter dealing with copyright.

The first question is whether Belgian law is applicable to geographic surveillance. Belgian law is applicable because the equipment used to collect the personal data is located on the Belgian territory[114].

The second question is whether geographic surveillance qualifies as processing of personal data and thus subject to data protection legislation. The anwser to

[111] art. 12 §2 WVP juncto art. 32 K.B. 13 februari 2001
[112] B., DOCQUIR,"Le droit de la vie privée", de boeck Larcier, Brussels, nr. 828
[113] art. 14 § 1 WVP; D., DOCQUIR, "vie privée., nr. 814
[114] art. 3bis 2° WVP

that is yes, as we have shown when discussing the scope of the legislation. In collecting the geographic information, personal data is also accidentally gathered. In addition to that it is important to note that the Belgian public register holds a notification for a processing called “Mobile Mapping”. It concerns images used for digital cartography[115].

The third question is whether there are legitimate grounds for the processing of personal data. The WVP allows for the processing of personal data if the legitimate interest of the controller excedes the rights and freedoms of the data subject. Furthermore, the collection of personal data is only collateral to the actual goal of the images. These images are destined for the creation of 3D city models, which you can describe as 3D city cartography. The personal data contained in the images will not be subject to any further processing; unless it is deletion or blurring of identifiers visible in the images. In support of this thesis we have off course the the notification Mobile Mapping, which shows that such a processing is allowed.
An exemption to the rules of personal data processing for research purposes is not advisable, since the project is not only focused on research. The research proposal also contains a part on valorisation of the research results. This means that the research results will also be put to commercial use when possible and that is an important shift in the purpose of the processing. This shift in purpose means also a shift in the rules to follow. This shift in rules makes this option not very attractive.

Is there a duty of notification of this processing to the Privacy Commission? The Commission has to be notified since this concerns an automated processing of personal data. The automation is in the use of camera’s to collect the images. Tele Atlas already notified the Privacy Commission for a processing called Mobile Mapping and the notification also covers the scope of URBAN. Therefore it is not necessary to notify again if Tele Atlas would be the controller and anybody else using the images within this project as a processor. If Tele Atlas is not the controller, a controller must be appointed. The controller is he who determines means and goals of the processing. This could be the consortium.
Data subjects should also be notified. But the data does not hold any contact details. As a result, it is impossible or would at least require a disproportionate effort to inform the data subjects[116]. Therefore, information should be given upon the first contact with the data subject and not at the time the information is collected. This is also the course of action found in the Mobile Mapping notification.

Further measures could also be to inform people on the company website about the use of geographic surveillance for the creation of digital cartography and provide a link to the privacy policy regarding the personal data collected

[115] https://www.privacycommission.be/elg/publicRegister.htm?decArchiveId=35021; notified by Tele Atlas
[116] Mobile Mapping notification

collaterally. It might also be a good idea to post a copy of the notification on the same website or provide a link to the public register and provide a keyword to facilitate the search in the register[117]. This is not necessary but shows the good faith of the controller.

Another issue is how long the data will be stored. The answer to this question will depend on whether it is possible to take the personal data out of the images without this being detrimental to the image quality required for the creation of 3D city models. If it is possible, then the personal data should be erased as soon as possible, since it is not necessary to store the data for the purpose of digital cartography. Else the processing will not be in compliance with data protection rules and lead to liability and possibly even criminal prosecution[118]. If this is not possible however, the data can be stored, but adequate safeguards should be provided to comply with the obligation of security and confidentiality of the data.

Transfer to third parties is not relevant for URBAN, since it is possible to establish a relationship controller-processor between the different partners. This facilitates matters, but imposes upon the controller an obligation to monitor the processors. The choice of processor and the contractual relations must be in accordance with the WVP[119]. The WVP states that the controller must choose a processor who can provide the same level of security and confidentiality as is imposed upon the processor. The processor can only act on authority of the controller or under the obligations that are also imposed upon the controller. The latter means that the processor can be commandeered by public authorities to execute a processing on personal data for reasons of considerable public interest.

It is also important to note that the WVP also applies to processing of data by the governement or government institutions. They can be releived from certain duties such as the information duties but not from duties such as the security and confidentiality requirements and the fact that the data must be relevant, accurate and up-to-date. The government also has a certain margin of appreciation regarding the legitimate reasons of data processing. These are however not unlimited as the case-law of the European Court of Human Rights demonstrates.

[117] the name of the processing is the best option since this is probably unique.
[118] art. 36-43 WVP
[119] art. 16 WVP

IV. IMPLICATIONS OF INTELLECTUAL PROPERTY RIGHTS

IV.1. Relationship IPR and URBAN

The relation is not obvious at first. Probably because the buildings are situated in public space and we do not feel as if any limitations apply in public space. But this is not true. A building can be protected by intellectual property rights if it complies with the conditions set forth for protection by intellectual property law. URBAN could infringe on intellectual property rights. The 3D city models are nothing other than a digital reproduction of buildings. And you cannot reproduce, in any shape or form, protected materials without consent from the rights holder.

Therefore, we must take a look at intellectual property rights. We will mainly focus on trademark and copyright, since in these two topics the physical appearance can be protected, whereby in patent law, an invention is protected and appearance is not relevant. Copyright protects works of art. That art can be any kind of art, literature, music, architecture. Trademark mostly refers to the protection of brand names such as Coca-Cola, McDonalds, Triumph and their logos such as the Nike Swoosh or the badges of car brands[120]. As we will demonstrate later, some companys use architecture as part of their trademark. Therefore we must also take a look at trademarks. But when producing accurate city models, trademarks themselves might also be reproduced and we will have to find out what the consequences are for this reproduction.

IV.2. Copyright

IV.2.1. Legal Framework

The core text is the Belgian Copyright Act[121]. This Act defines the protection granted to works of litterature and art.

IV.2.2. Scope

The protection is aimed at works of art and litterature. Art can have different and disparate meanings[122]. Often there is strong debate on whether something should be qualified as art. We must however not confuse the existential debate with the legal debate. We are talking about art as it is approached by the legal world, according to law, jurisprudence and doctrine.
What does the legal world qualify as art then? It doesn't qualify anything as art. It accepts nearly anything. It makes a distinction between art worth protecting and not worth protecting. What is not worth protecting is what does not meet the criteria set forth for protection. This assessment is made in a case-by-case approach, which holds some general guidelines.

[120] examples: http://en.wikipedia.org/wiki/Trademark
[121] Wet 30 juni 1994 betreffende het auteursrecht en de naburige rechten, *B.S.* 27.07.1994
[122] examples: http://en.wikipedia.org/wiki/Art

Most important though is that architecture could also qualify as art. But in order to receive protection under copyright law, the work of architecture must comply with the conditions set forth. Theses conditions determine the qualification of architecture as art in the legal sense and hence provide protection.

The scope is limited in time. Protection is limited to 70 years after the death of the author[123]. If there are joint authors, the protection lasts for 70 years after the last of them has died.

IV.2.3. Conditions for application

Copyright law grants protection to works that are the result of a creative effort carrying the mark of the author[124]. It does not cover methods, ideas and techniques[125].

Two components can be discerned in this definition. The first one is a creative effort. This one is quite easily accepted, especially concerning architecture. Designing a structure requires a lot of time and intellectual effort. Many things have to be calculated. This already qualifies as an intellectual effort, but this is not sufficient for protection[126].

The second component is carrying the mark of the author[127]. This criterion is defining for protection, since there is apparantly a reluctance to award this to works of architecture. The first reason is that in the current day, construction is subject to an elaborate set of technical regulatoins. The variety depends on the kind of structure. And the more something is regulated, the less room there is for creating something personal[128]. Therefore, buildings are by some considered to be ineligible for protection under copyright. This view is too restrictive; although when there is only one form possible, for whatever reason, no protection can be given[129]. Every building must be judged on its own merits. The mark of the author can be found in many different aspects. It can be in the appearance of the building, but also in colors, style features, materials, how certain problems are solved[130]… Buildings have been judged original because of the way they adress technical issues and how different solutions can be combined[131]. As it happens,

---

[123] art. 2 Belgian Copyright Act
[124] Antwerpen (1ste k.) 14 oktober 2002; *A&M* 2003, 4, p 276-278; S., VANLANGENDONCK, *Auteursrecht in de bouwkunst*, Bruylandt, Brussel, 2004, p 71
[125] J., DEENE, "Intellectuele rechten kroniek 2007", *NJW* 2008, 185, nr. 6
[126] S., VANLANGENDONCK, *o.c.*, p 101-102
[127] Antwerpen (1ste k.) 14 oktober 2002; *A&M* 2003, p 276-278
[128] S., VANLANGENDONCK, *o.c.*, p 79
[129] S., VANLANGENDONCK, *o.c.*, p 79
[130] Rb. Antwerpen 5 januari 2007, 03/7248/A, onuitgegeven, quoted in J., DEENE, "Intellectuele rechten kroniek 2007", *NJW* 2008, 185, nr. 22; examples can be found in the works of famous architects such as Frank Lloyd Wright (organic architecture), Le Corbusier (modern architecture), Gustav Eiffel (steel constructions), Victor Horta (Art Nouveau)...
[131] S., VANLANGENDONCK, *o.c.*, p 102

note that novelty is no requirement for protection. Collage is accepted as an art form[132].
The main problem is the fact that determining whether there is a mark of author is always subjective and can differ depending on who is judging[133]. This is reflected in the expression: de gustibus et coloribus non disputandum est. This is the great strenght of this criterion, it is broad, but also its weakness, it is unpredictable.

Copyright protection can be granted to works of architecture, but it will not be granted per se. As with any work of art, architecture has to comply with the criteria set forth in legislation. But for architecture, due to its technical nature, it is more difficult to comply with these criteria since the architect does not get the opportunity to express himself as much as in other forms of art such as litterature and painting.

IV.2.4. Exceptions/ Exemptions

There is one exception that is particularly important when talking about copyright on works of architecture. This is article 22, §1, 2° of the Belgian Copyright Act:

*When the work is lawfully made public, the author cannot oppose the reproduction and communication to the public of a work exhibited in a **publicly accessible place** where the purpose of the reproduction or communication to the public is not the work itself*

To be elegible for this exception, the work must have been lawfully made public. In other words, the author must have used his right to publicise his work. For works of architecture, this is not as troublesome as for others kinds of art due to the magnitude of the work. Furthermore, works of architecture are mostly situated in the public space.
The most important will be to assess what the goal is of the reproduction or communication to the public. This has already been subject of litigation. One case dealth with the opening credits of a show, which showed the surroundings where the show was recorded[134]. In the credits came shots of a sculpture. The claim was these shots were infringing upon the copyright of the sculptor. This claim was rejected on different grounds. First because the director wanted to recreate the atmosphare of the surroundings of the talk show, the sculpture was part and parcel to these surroundings. Secondly the images were brief and part of the kaleidoscopic vision given by the director. In this case it was judged the goal of the reproduction was deemed legitimate, because the goal of the credits was to recreate the surroundings of the show and not the sculpture. Also

[132] Collage: http://en.wikipedia.org/wiki/Collage
[133] Gent (17de k.) 16 april 2002, *A&M* 2002, p 347-349; in first instance the judge found no violation, while there was judged to be infringement in the appeal to the judgement
[134] Bruxelles (9° ch.) 4 septembre 2003, *A&M* 2003, p. 384-385

important to note in this case is that the court found the article to be clear and not needing any interpretation in accordance with case law and doctrine prior to the article. In another case there was judged to be an infringement[135]. The label of a beer bottle showing a sculpture located on a square in Ostend was deemed to infringe upon the copyright of the sculpture. The sculpture[136] was deemed to be the centre of attention of the reproduction instead of an accidental appearance, despite the fact that the scenery was also pictured on the label. This decision was an appeal against the decision in first instance, which said that there was no infringement since the label wished to recreate the atmosphere of Ostend by using one particular square, the one where the sculpture was situated. The second case clearly demonstrates the complexity of the matter. In one case we have two different outcomings although the subject of the litigation is the same. Compare it with the first judgement however and something comes up. In the first case, the reproduction was part of a kaleidoscopic view of the surroundings and there was deemed to be no emphasis on the sculpture. In the second case the sculpture was deemed to be the centre of attention of the label and on that basis the court decided there was an infringement. Hence one of the questions when assessing a reproduction will be what is meant to be emphasised by the reproduction. Whether it is the protected work or something more, of which the work is part[137].

IV.2.5. Implications for URBAN

The implications for URBAN are fairly limited. 3D city models are the goal. These models require the reproduction of structures situated in the public area.
First it is important that not every structure that is reproduced is protected by copyright. As we have said previously, it is not easy for works of architecture to comply with the conditions set forth for protection under copyright law. We could say that only exceptional buildings will enjoy protection. And these are only protected for a period of 70 years after the death of the architect, which means that buildings such as the Eiffel Tower[138] and Tower Bridge[139] are part of the public domain and are no longer subject to copyright. This means that possibly only a small percentage of the structures reproduced are subject to copyright.

The question is then, for the structures protected, if we can claim the exception of art. 22 §1 2°. The goal of URBAN are 3D city models, so the reproduction is aimed at recreating a city, not a particular building. Therefore, referring to the judgements above, we could claim that the goal of the reproduction is not the building itself; the reproduction is accessory to the goal[140].

---

[135] Gent (17de k.) 16 april 2002, *A&M* 2002, p. 347-349; note that only the use of the sculpture was subject of litigation, not the name of the beer.
[136] This sculpture is titled 'The Sea", but is known in Ostend as "Dikke Mathilde", the name of the beer which used it for its label.
[137] S., VANLANGENDONCK, *o.c.*, p 146-147
[138] Gustav Eiffel died in 1923, over 80 years ago
[139] Joint effort of John Wolfe-Barry (died 1918) and Horace Jones (died 1887)
[140] J., DEENE, "Intellectuele rechten kroniek 2007", *NJW* 2008, 185, nr. 44-45

IV.3. Trademark

IV.3.1. Legal Framework

The current legal framework is the Benelux Convention regarding intellectual property[141]. This Convention replaces the former dispersed body of legislation.

IV.3.2. Scope

The scope of trademark law is to protect distinctive signs that are used to differentiate goods or services from identical or similar goods or services. The best examples are brands such as Coca Cola and Pepsi, Mercedes and BMW…
The protection is granted for 10 years, starting from the date of application for protection[142]. After these 10 years the trademark holder must apply for an extension. If he does not apply for an extension, the brand is considered free and can be registered by another person[143].
The fact that a trademark is not registered or that registration has been denied does not mean the trademark can not be used or that it can not be protected in any other way. The protection in this case is however not worth mentioning since it will only be possible in a very limited number of cases under very strict conditions. However, this is beyond the scope of this deliverable.

IV.3.3. Conditions for application and the scope of protection

Trademarks are not given automatically, contrary to copyright. You need to apply for a trademark to acquire a trademark. The competent authorities will then asses the validity of the request and determine whether there is reason to grant the request or not.

The main condition is the distinctive character of the trademark[144]. If the proposed trademark does not allow distinguishing the goods or services it relates to from other goods or services, then the proposed trademark will not be approved. In practice, the distinctive character of the trademark is accepted quite easily. There are three reasons to reject a trademark:

1. A trademark that has no distinctive character whatsoever.
2. Trademarks that are only composed by generic indicators for characteristics of products such as weight, height…

[141] Benelux Bureau voor Intellectuele Eigendom: http://boip.int/nl/generalLegalRegulations.html
[142] art. 2.9.1. BVIE
[143] art. 2.9.4. en art. 2.26.1.a. BVIE
[144] D., KAESMACHER, *Les droits intellectuels*, Larcier, Brussel, 2007, p. 161-165

3. A trademark has become a common identifier for a product such as gin, water, petrol, diesel…[145]

In any of these three cases, a trademark will not be approved. This does not mean however that the trademark can not be used for commercial purposes. The only downside of using it is that it will not be protected in case of abuse.

Secondly the trademark must be lawful. In three cases a trademark is considered unlawful[146]. Only two of them are relevant for URBAN, the third refers to denominations of wines and spirits. A trademark must not conflict with public order and morality. This means it should not be in violation with the law or be offensive. Registering a brand such as “Nigger” or “Raghead” for example is impossible. This does however not apply to the use that is made of the brand. If a brand is for example adopted by neo-nazi groups (Lonsdale), that has no effect on the lawfulness of the trademark. A trademark may neither be deceiving. A trademark is deceiving if it is not thruthful regarding nature, quality or geographical origin of the product. It can be deceithful either by nature or by use. To be considered as deceithful, the trademark must be able to influence the conduct of the consumer.

Thirdly, the trademark must be available[147]. In two cases a trademark is unavailable. Firstly, the unavailability can result from the private right of a third party. This refers to family names[148], social denomination, commercial name… The second reason is that the trademark has been registered by a third party as a trademark. In any of the two above cases, a trademark is unavailable. In any other case, the trademark is available.

Registering a trademark grants protection against abuse of the registered trademark in any of the following cases[149]. A third party cannot use the trademark to offer similar goods or services. Nor can he use a similar trademark that may create confusion. Neither can he use the trademark for any goal if he would benefit from using the trademark. A third party is also prohibited from using a trademark for other purposes than distinguishing goods or services when he has no good reason to use the trademark and when he illicitely profits from the distinctive character or reknown of the trademark or when he violates the trademark.

---

[145] Best known example of the impact is the practice of the Coca Cola company: R., COOTER, T., ULEN,”Law and Economics”, Pearson Addison Wesley, Boston, 2004, p. 136
[146] Art. 2.4.b. BVIE; D., KAESMACHER, *o.c.*, p165-167
[147] Art. 2.4.c-e. BVIE
[148] Art. 2.23 BVIE; In Leuven there is a shop selling household electronics under the name Van Praag, after the owner. This conflicted with the trademark Hugo Van Praag, a chain of household electronics stores. Van Praag in Leuven was granted the right to continue under his own name because it was his family name.
[149] art. 2.20 BVIE

As for the scope of protection, this can be limited to Belgium or more broad such as the Benelux, E.U or even worldwide[150]. This choice has to be made when registering the trademark. The reach of the protection must thus be determined for each registration separately.

IV.3.4. Exceptions/ Exemptions

There are no exceptions or exemptions to trademarks. This would go against the idea of trademark protection, which is to protect commercial interests. The only reason that protection would not apply in a certain case is that the case falls outside the scope of protection.

IV.3.5. Implications for URBAN

The implications are limited since the primary use of URBAN is to create a 3D city model. There is no offering of similar or comporable goods or services by the makers making use of the same trademark. And that is the core issue. The protection granted to trademarks applies in cases where a third party uses a registered trademark in the cases cited previously. In any other case, the protection of trademarks does not apply.
There is no intention to gain any personal advantage from the use of the trademarks in the 3D city models. The goal is to provide a city model as accurate as possible. This includes signposts, facades and everything that is helpful when people are trying to orient themselves in an URBAN environement. But these are just details, the main point of focus are the buildings.
Commercialization of the city models will take place under a different trademark than the ones reproduced in the city models. So for personal gain, a different trademark will be used. This should also make URBAN fall outside the scope of trademark protection.

IV.4 Conclusion Intellectual property rights

The consequences of intellectual property rights on URBAN overall are limited.
As we have demonstrated, structures can be subject to copyright, although structures are quite often denied protection because of a lack of originality. Furthermore, structures are mostly located in a public area and as a result their protection is subject to exceptions. Reproduction of the protected structure is allowed if the focus of the reproduction is not the structure itself, but for example a view of the city or a skyline.
Trademarks seem of little relevance to URBAN. Mostly they will refer to different goods or services than those resulting from URBAN. Additionally, results of URBAN will be commercialised under a private trademark (Tele Atlas?). Therefore it should not be a problem, contrary to copyright which might create a problem, although unlikely.

[150] Art. 2.2 BVIE

V. INSPIRE DIRECTIVE 2007/2/EC[151]

V.1. Scope

V.1.1. General

In art 1.1 the directive defines its purpose:

> "The purpose of this Directive is to lay down general rules aimed at the establishment of the Infrastructure for Spatial Information in the European Community (hereinafter referred to as INSPIRE), for the purposes of Community environmental policies and policies or activities which may have an impact on the environment."

To establish this infrastructure, INSPIRE relies upon infrastructures owned and operated by the Member States. Art. 4 of the Directive clearly defines what spatial data sets[152] fall within the scope of this directive:

> This Directive shall cover spatial data sets which fulfil the following conditions:
> (a) They relate to an area where a Member State has and/or exercises jurisdictional rights;
> (b) They are in electronic format;
> (c) They are held by or on behalf of any of the following:
> (i) A public authority, having been produced or received by a public authority, or being managed or updated by that authority and falling within the scope of its public tasks;
> (ii) A third party to whom the network has been made available in accordance with Article 12;
> (d) They relate to one or more of the themes listed in Annex I, II or III.

These are cumulative conditions, meaning that all the conditions must be fulfilled in order for the spatial data set to fall within the scope of the directive. Since URBAN is destined to form the GRBV, which is held by a public authority as stated in (c)(i), the question is if it relates to one of the themes listed in either of three annexes. In annex I we find two themes that are held within URBAN: Adresses[153] and Geographical names[154]. In Annex III we find another theme: Buildings[155].

---

[151] DIRECTIVE 2007/2/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), *O.J.* 25.04.2007, L 108

[152] defined in art. 3.3. INSPIRE directive

[153] Location of properties based on address identifiers, usually by road name, house number, postal code.

In case of identical copies of spatial data sets, the directive only applies to the reference version of which the copies have been derived.

V.2. Aim and means of Directive

The aim is to facilitate environmental policy making by linking all relevant databases. At this moment it is very hard to work cross-border since this requires consulting different databases and integrating the data separately[156]. The directive wants to do away with this by removing obstacles that exist today[157]. One of the means is a Community geoportal through which Member States should provide acces to their infrastructure. This portal will make use of metadata about the data that are collected and created by public bodies in their spatial data sets.

V.3. Applicable on URBAN?

It will not apply to the project directly since we have to wait for the adoption of metadata rules and the implementing rules before the entry into force of the Directive. The metadata rules are currently in the formal adoption process while the implementing rules are still in the draft process[158]. Until these rules are accepted, it is hardly possible to determine to what extent URBAN will be affected by these rules. The deadline for the rules is 15 May 2009 and it allows for a two year implementation period after the adoption of metadata rules and implementing rules. This means that the inspire directive will probably not enter into force before 15 May 2011.

---

[154] Names of areas, regions, localities, cities, suburbs, towns or settlements, or any geographical or topographical feature
of public or historical interest
[155] Geographical location of buildings
[156] recital 15 INSPIRE
[157] recital 20-23 INSPIRE
[158] http://inspire.jrc.ec.europa.eu/

VI. CONCLUSION

This Code of Practice should provide guidance for geographic surveillance and 3D city modelling. Privacy and Intellectual property rights have been the main topics of research. INSPIRE has been discussed as a point of interest for the future, but incomplete legislation to date hinders entry into force and further analysis. It is also more of interest to government agencies controlling spatial information databases than for private consortia.

The video-images with recognisable people are the core privacy-issue of geographic surveillance. Different solutions for the problem have been pointed out. These are erasing personal data or blurring faces and other pieces of information that lead to identification. Note that the focus of data protection lies on how a processing is done, rather than on the fact that a processing is done. The law states that a processor must take all measures necessary for security and confidentiality of the processing. This is also reflected by the reference measures for security that have been published by the privacy commission; the focus lies on the means rather than the goal. The processor has the choice of means to fulfill his duty, taking into account the characteristics of the personal data. The courts, in a law-suit and the Privacy Commission, as supervising authority, have the authority to assess these means. There should not be any problems in complying with the law. When one tries to stretch the law, problems could arise and the penalties for infringement are severe. All things considered there should not be a problem when the law is applied properly and measures are reviewed when needed.

As far as Intellectual Property Rights are concerned, copyright could be an issue. Structures could fall within the scope of protection if they comply with the conditions for protection. Any reproduction, e.g. 3D city model, would consequently require consent from the rights holder. However, case-law seems to show that copyright on structures is rarely granted. Furthermore, copyright is limited in time. This means that although some building might be eligible for protection, they could not benefit from protection due to their age. Additionally, copyright legislation also provides certain exemptions from copyright. The most important appears to be the exemption for rights exposed in a public area. Care should be taken because the definition of public area could differ, depending on the case.

Trademark, plenty are present in public areas, was also discussed and did not appear problematic. Trademarks are generally protected against their use for commercial purposes by a person other than the rights holder. Commercial use of URBAN results will probably be done under a different trademark. This should take away the first issue. Nevertheless, trademarks also benefit from protection against any abuse for personal gain. This could relate to their incorporation in 3D city models. However, this should neither be a problem. The incorporated trademarks are a mere feature of the 3D city model. Rights holders might even display interest in this feature. Exceptions or exemptions to trademark protection are non-existent. The only reason trademark does not apply is that the case at hand is out of scope.

Different issues regarding URBAN have been adressed. None seem to be insurmountable at the moment. This on condition that applicable legislation is respected and the measures providing security and confidentiality are reviewed when needed.

TABLE OF AUTHORITIES

Directives

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *OJ* L 201 , 31/07/2002, p.37-47 21
DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. L 105, 31/07/2002, p. 54-63 21
DIRECTIVE 2007/2/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 39
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995 12
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.12

Statutes

Wet 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 18 maart 1993 aangevuld door K.B. 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 13 March 2001, p7908-7919 22
30 juni 1994 betreffende het auteursrecht en de naburige rechten, *B.S.* 27.07.1994 32
K.B. 13 februari 2001 ter uitvoering van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *B.S.* 13 March 2001, p7908-7919 24
Wet 13 maart 2005 betreffende de elektronische communicatie, *B.S.* 20/06/2005, p. 28070 22

Cases

Andrea Francovich and Danila Bonifaci and others vs. Italian Republic, ECJ 19 November 1991, *ECR* 1991, I-05357 22
Antwerpen (1ste k.) 14 oktober 2002; *A&M* 2003, 4, p 276-278.....35
Bruxelles (9° ch.) 4 septembre 2003, *A&M* 2003, p. 384-385.....37
Gent (17de k.) 16 april 2002, *A&M* 2002, p 347-349 36
Peck vs. UK, ECHR 2003 7
Rotaru vs. Romania, ECHR 4 may 2000 20
Von Hannover vs. Germany, ECHR 2004 7

Data Protection Authority Opinions

ART. 29 WORKING PARTY, Opinion 4/2007 on the concept of personal data, WP 136, Art. 29 Working Party website.....12

Opinion 4/2007 on the concept of personal data, Art. 29 Working Party, WP 136, Art. 29 website.....7

Doctrine

B.,DOCQUIR, “le droit a la vie privée”, de boeck Larcier, Brussels, 2008,.....23
D., KAESMACHER, *Les droits intellectuels*, Larcier, Brussel, 2007.....36
R., COOTER, T., ULEN,”Law and Economics”, Pearson Addison Wesley, Boston, 2004.....37
Referentiemaatregelen, website CBPL: http://www.privacycommission.be/nl/static/pdf/referenciemaatregelen-vs-01.pdf 25
S., VANLANGENDONCK, *Auteursrecht in de bouwkunst*, Bruylandt, Brussel, 2004,.....33

Doctrine Articles

J., DEENE, “Intellectuele rechten kroniek 2007”, *NJW* 2008, 185.....33
Nissenbaum, Helen F., “Privacy as contextual integrity”, *Washington Law Review*, Vol. 79, No. 1, 2004, Available at SSRN: http://ssrn.com/abstract=534622.....7
Rb. Antwerpen 5 januari 2007, 03/7248/A, onuitgegeven, quoted in J., DEENE, “Intellectuele rechten kroniek 2007”, *NJW* 2008, 185.....34
Solove, Daniel J., “A Taxonomy of Privacy”, *University of Pennsylvania Law Review* 2006, vol 154, available at SSRN: http://ssrn.com/abstract=667622 7

Press Articles

Gijzemijter, M., “Google past waasfilter toe op Franse StreetView”, webwereld.nl, 4/07/2008 11
Robertsen, S., *id*; IBLS editorial department., “Google Street View now in Europe, Raising Privacy Concerns”, www.IBLS.com, 09/06/2008 10
Sayer, P., “Google blurs faces to protect privacy in French StreetView”, www.networkworld.com, 03/07/2008 11
X., “Google Street View gets go ahead”, news.bbc.co.uk, 31/07/2008.....10

Industry information

Google Street View: http://maps.google.com/help/maps/streetview/ 10
Notification Tele Atlas: https://www.privacycommission.be/elg/publicRegister.htm?decArchiveId=35021.....30