"Linked Open Apps Ecosystem to open up innovation in smart cities"

Project Number: 297363

Deliverable:	**D3.9 Legal aspects analysis**
Version:	**1.2**
Delivery date:	**19/04/2014**
Dissemination level:	**PU**
Author:	**Martin Potts, Monique Calisti, Frank Van Steenwinkel Monica Palmirani – Michele Martoni – Dino Girardi (CIRSFID – University of Bologna)**

(Based on original written by **Tom Mertens, Céline Rotthier, Matthias Van Oyen)**

Summary

This deliverable discusses the legal aspects that must be taken into account by a European city when "going smart" by "using" the iCity platform. The document identifies the main legal pillars but also provides a potential scenario based on the current deployed iCity platform and consortium partners involved.

This deliverable provides an overview of the core aspects that cities must consider with respect to privacy, data protection, data retention, data transfer and database security, licenses, liability, contract of service and open government data regulation.

D6.7 will describe the regulation among existing partners and for the future partners for being compliant with this D3.9 deliverable.
D7.1 (business model) will discuss the constitution regulation, the national law of each partner in the consortium.

DOCUMENT HISTORY

Version	Date of issue	Status	Content and changes	Modified by
v1.0	12.12.2012	original		
v1.1	18.12.2013	Final draft	First complete version of the document focused on legal aspects	M.Potts and M. Calisti
v1.2	08.04.2014	Additions based on EC review comments	Legal issues for future iCity Platform – deployments - organizational	Frank Van Steenwinkel (FideCity) Monica Palmirani Michele Martoni Dino Giraradi (CIRSFID – University of Bologna)

TABLE OF CONTENTS

1. Introduction

When becoming “smart”, a city should consider - and be aware of - the various legal implications and issues that this action implies, regarding the iCity platform. In particular, the data risks, with protection of citizens’ personal data and the transfer or storage of data as being a crucial issue. IPR (Intellectual Property Rights) and the contractual aspects should also be carefully evaluated. The processing of personal data will happen in different places throughout the world, which means that different legal jurisdiction and regulations will apply.

The IPR issues around the dataset and API are very relevant topics as the licenses are there not only to protect the authors, but also the end-user and the third parties using the platform. Note that the iCity provides a service of Open Data and API through its platform, it is therefore important to define the eCommerce issues and to investigate the open government regulation implications at national level.

In deliverable D3.9 we will provide an overview of the core aspects that cities have to consider with respect to:

- privacy, data protection, data retention, data transfer and database security;
- Limitation to the open data;
- Licenses and IPR issues;
- eCommerce;
- Open government regulation.

The European framework is used as the starting point because the iCity service platform is based in Europe and will be focused on helping build smart cities in Europe, furthermore all the 27 Member States are required to transform the European legislation into national legislations - see Figure 1. In addition to the European legislation, this deliverable will also consider the relations with non-European countries, in particular the U.S. The reason for this is that often European countries have trans-Atlantic transactions requiring data may be stored remotely with database management companies that reside in the U.S.

This paper also discusses the pressure that is being placed on the legal framework and how this can hinder the development process of a smart city with respect to the retention of data generated or processed in connection with the provisioning of publicly available communication services.

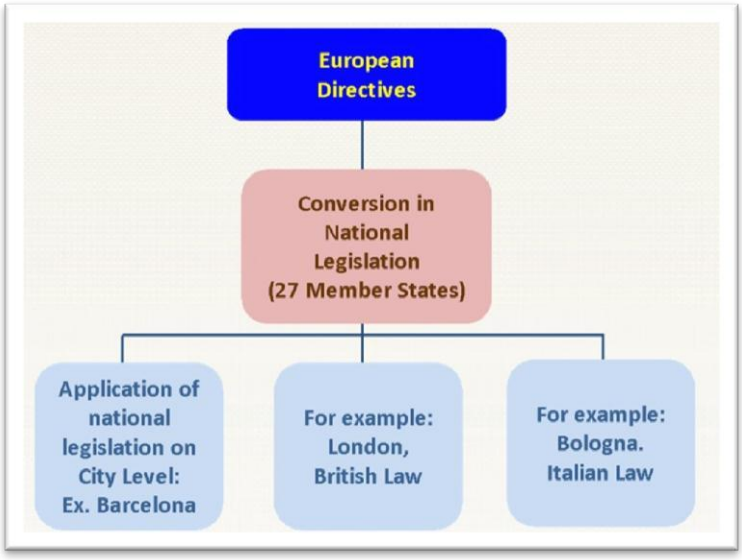


Figure 1: Transform European directives into national legislations

The rest of this document is organized as follows:

- Section 3 present the privacy issues
- Section 4 limitations to the open government data and to the access right
- Section 5 IPR issues
- Section 6 eCommerce
- Section 7 Open government regulation.
- Section 8 iCity analysis
- Section 9 Check list
- Section 10 Conclusions

2. Privacy Issues

2.1 Privacy and data protection

A city comprises individuals (human capital) each of which retain distinctive personal data. If the city wants to become a “smart city”, it is likely that it will have to access and open up certain personal data of its citizens. This data will very likely be processed and used by software developers to develop new on-line applications and services. Obviously, access and use of personal data potentially forms a threat to people’s privacy, therefore processes and code must be incorporated so personal data is fully protected.

Within the scope of iCity, the three relevant privacy issues are:

a) Profiling of the end-user during the access to the iCity platform considering that the developer of API, public officers, end-users will access to the platform with specific access and permissions. Inside of this category we include: web logging, cookies, IP address tracking, and analytics, for improving the quality of the service.
b) Dataset records of behavior of the citizens: social network post, claims, traffic information;
c) API that could track the personal data, in case also detecting the movement of the people with a geolocalization system installed in mobiles, devices, and pc´s.

Figure 1: Privacy Policy

For example a risk on the iCity platform could be against a developer/user where the iCity platform may profile the citizen without their consent – see examples below.

For example on the open dataset: a city can decide to open up its camera infrastructure at a busy intersectionto map the traffic congestion in certain areas.

The raw footage will contain identifiable images of people walking in the street and car number plates.
This is information that should not be allowed to come into open data and in any case they are collected, treated and maintained over time respecting the national privacy regulation.

For example on the API: a city can decide to release an API able to geolocalize the citizens inside of a Wi-Fi network.

Since "Privacy" and "Data Protection" are often used as synonyms and interchangeably, the difference needs to be explained.

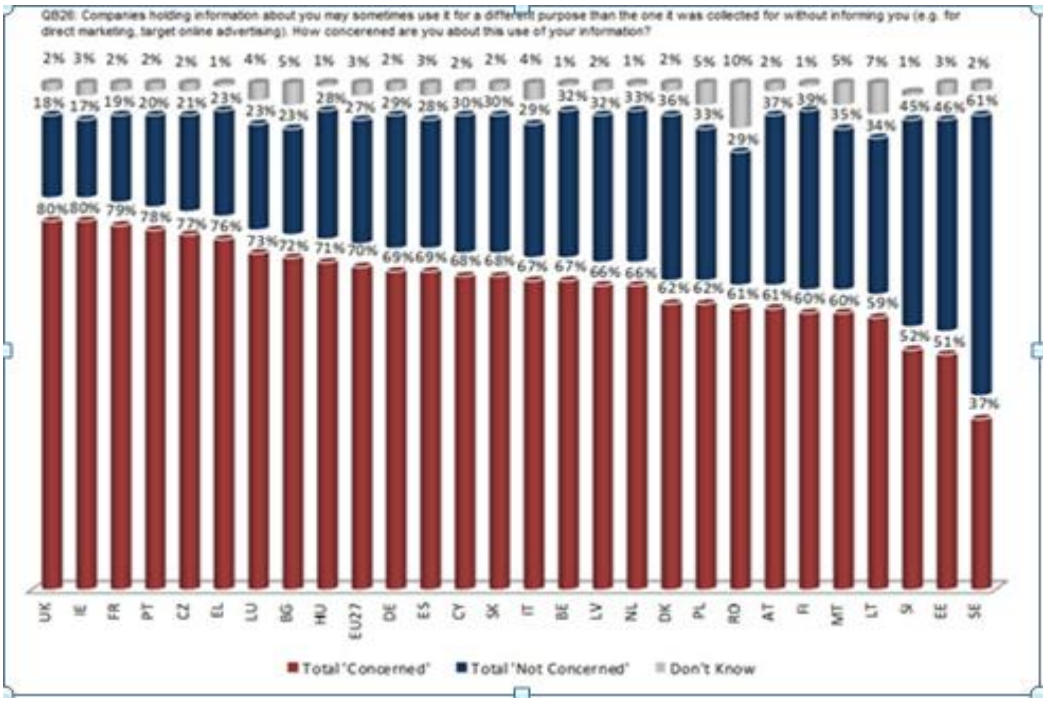


Figure 3: Concern about Privacy issues connected with open data maturity

Privacy not only includes the right to protection of personal data. Privacy is much wider, it's a fundamental right, and it’s an inviolable human right. Privacy is there to protect person’s private life (personal or family).

New technologies through the use of person’s information may result in the violation of privacy. So private information should be protected and it should be mandatory that the individual people have the power to control their own data and the distribution of that data.
This led to the new Right to Data Protection that also includes the right to be forgotten and to be let alone.

People are rightly concerned regarding privacy issues. Figure 3 shows a countries report, notice that the culture of the data protection is increasing proportionally to the maturity of the innovation and open data availability. UK where the open government data is one of the best in the world, the consciousness regarding the privacy issues are at the top.

Article 8 of the European Convention on Human Rights (ECHR) indexed "Right to respect for private and family life”; recognized the Right to Privacy.
This article specifies that "Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and it´s necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

The Data Protection Right instead finds some of its origin in the Charter of Fundamental Rights of the European Union (ECFR) (see also Lisbon Treaty) in which we can find the distinction between Privacy and Data Protection.
Next to the right to respect for private and family life in Article 7, Article 8, in facts, grants the

right to the protection of personal data concerning the individual. It also states that the data should be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Every individual has the right of access to his/her data and the right to have it rectified.

The right to privacy and in particular the right to data protection was contained also in the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to Automatic Processing of Personal Data and, included, in European Parliament and Council Directive of 24 October 1995, n. 46, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

2.2 Protection of individuals with regard to the processing of data

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

Cities that are setting up smart city projects will definitely be faced with this Directive [5]. Installing a smart city inevitably means transferring and moving citizens' personal data and therefore adequate protection of their privacy is necessary. The protection of personal data will be one of the biggest challenges for smart cities especially connected with the risk of social control, security, confidentiality, less democracy, discrimination, self-determination (the legal right of people to decide their own destiny).

For example: collecting citizen's personal data to make a database of the subscriptions for public transportation. This data should be protected properly and cannot be seen by just anyone, or used for purposes for which it was not intended.

The Data Protection Directive regulates the processing of personal data within the European Union [6]. It is an essential component of European privacy and human rights law. Article 1 of the Directive literally repeats the fundamental Right to Privacy and in particular the Right to Data Protection: "Every Member State has to protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data". Article 8 of the European Charter of Fundamental Rights is clearly incorporated in the Directive.
Without going into detail, cities should be aware of the scope of the Directive and know what is meant by 'personal data' (Article 2, a) and the 'processing of personal data' (Article 2, b).

Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (art. 4, lett. a), Directive). It can include a person's name, photo, address, credit card number, criminal record, bank statements, posts on social networking websites, ip number, profiling log files, etc.

Essentially, data is personal data when directly or indirectly linked to a person, even if the person holding the data cannot make this link. Any information that relates to an identified or identifiable natural person falls under the definition of the Directive. Obviously, this definition is very broad and it can apply to a vast amount of information.

The processing of data covers any (set of) operation(s) which is performed upon personal data, whether or not by automatic means (Article 3), such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction (art. 4, lett. b) Directive). The concept includes everything from the creation to the destruction of the data.

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.
The Processor, instead, is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
- the processor shall act only on instructions from the controller,
- the obligations set out, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

Every Member State will apply its national law (which is a conversion of the European Directive) when the controller is established within the EU, but also whenever the controller uses equipment to process data situated within the EU. The same conditions apply to controllers established outside the EU but who are in a place where the national data protection law is applicable, due to rules of public international law (Article 4).

2.2.1 Principles

In summary, the main principles of the Directive 95/46/EC are the following [7]:

1) Purpose: data must be processed for specific purposes:
1.1. Data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
1.2. Legitimacy: data must be processed lawfully and fairly;
1.3. Relevance and not Excessive: data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

2) Privacy Notice: Information that the Controller must give to the data subject. The Controller or his representative - in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject - must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as: (c.1) the recipients or categories of recipients of the data; (c.2) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; (c.3) the existence of the right of access to and the right to rectify the data concerning him.

3) Consent: no treatment of data without the information of the point 2) and the consent, with

particular regard to the disclosure to third parties. These treatments are, generally speaking, not possible without the consent of the person concerned (unless there is a legitimate reason to do so, for example for the prevention of a crime or by public lawful reason).

4) Access and correction: people have the right to access or correct incorrect data held about them (unless there is a legitimate reason not to do so, for example for the prevention of a crime).

5) Duration: personal data cannot be kept for longer than is necessary and must be kept up to date. Not exceeding the time of retention unnecessary.

6) Transfer: personal data cannot be sent outside the European Economic Area, unless the person concerned has consented or adequate protection is in place (see *infra*: US-EU Safe Harbor Agreement).

7) Registration: all entities that process personal data must register with the especially established supervisory authority ('controller').
8) Security of processing: the departments holding personal data need to have adequate security measures (both technical as organizational).

It is important for a city to note that European legislation is a Directive, which means that every Member State is bound to achieve the same end result, but it has some freedom in choosing its own means and measures for adopting the rules of the Directive. As a result, its impact is different across the EU and the conversion of this Directive into national law has led to the fragmentation of privacy protection laws in Europe. This fragmentation can cause difficulties in interactions across different countries/ nations.

2.2.2 Jurisdiction and Territorial Scope

It is important to understand when the Controller have the obligation to respect the UE Data Protection Directive and which jurisdiction should be applied.
The criteria for defining the jurisdiction are multiple:
1) The establishment of the Controller in one of the Member states;
2) If the establishment of the Controller is not in EU, if the data or services are concerned to EU people;
3) If the Controller is not established in EU territory, but it uses equipment situated in EU.

The Art. 4 of the EU directive defines the national law applicable and in particular:

1) Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) 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 the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) The Controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) The Controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the

said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2) In the circumstances referred to in paragraph 1 (c), the Controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

It is interesting also to read the art. 3 of the Regulation on the Privacy recently passed at 12 March 2014 in EU Parliament and now under revision of the EU Council[1].

«*1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.*
2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:
(a) The offering of goods or services to such data subjects in the Union; or
(b) The monitoring of their behavior.
3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law».

These means that for each city involved in the iCity consortium we need to verify the privacy issues in details.
Additionally we have also to manage the privacy following the jurisdiction of the country where is installed the server hosting the platform.
In case of mirroring of the iCity platform all the procedure must be repeated for each installation.
In case of cloud computing architecture a special analysis is necessary.

2.2.3 Actors

The privacy directive includes also the definition of the actors and of the action that those actors must perform for guaranteeing a correct application of the above mentioned principles.

There are four main actors;

- **Controller**: 'controller' shall mean 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;
- **Processor**: 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
- **Appointed Subject**: -- national level --
- **Data Subject**: 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

[1] http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

2.2.4 Privacy Notice and Consent

The Controller can process personal data only if Data Subject consents to such processing. Consent must meet different requirements in order to be valid.

First of all, consent must be explicit. Putting consent wording without supplying the necessary information is not sufficient. For example pre-ticked boxes that users have to uncheck are also not a valid method of expressing or obtaining consent.

Secondly, consent must be specific and well-informed.
This mean that Data Subject has to be informed about the processing they agree to, before the processing takes place.

The purposes of the processing must be clear and Data Subject has to understand the features of the processing.

Data Subject has also to understand the consequences of the processing and also about his consent.

Finally, consent must be given freely. This criteria implies that a user has a real choice to consent to processing.

To sum up, consent must be freely given, specific, well-informed and explicit.

UE Directive specify that Member States shall prohibit the processing of 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.

This prohibition doesn't apply if:

(a) The Data Subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) Processing is necessary for the purposes of carrying out the obligations and specific rights of the Controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) Processing is necessary to protect the vital interests of the Data Subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) The processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

Finally Member States may, for reasons of substantial public interest, lay down exemptions.

So personal data may be processed only if the Controller has previously well-informed the Data Subject of the features of the Processing.

The Controller or his representative - in so far as such further information is necessary, having visibility to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject - must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as: (c.1) the recipients or categories of recipients of the data; (c.2) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; (c.3) the existence of the right of access to and the right to rectify the data concerning him.

After this information Personal data may be processed, but only if:
(a) The data subject has unambiguously given his consent; or
(b) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) Processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) Processing is necessary in order to protect the vital interests of the data subject; or
(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).

If the data has not been obtained from the Data Subject, the Controller or his representative, in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the Data Subject, must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:
(a) The identity of the Controller and of his representative, if any;
(b) The purposes of the processing;
(c) Any further information such as:
- The categories of data concerned,
- The recipients or categories of recipients,
- The existence of the right of access to and the right to rectify the data concerning him.

2.2.5 Registration of the user

Every user that enters in the iCity platform with a registration profile needs to accept the privacy notice and to provide the consent using an adequate web form. He also accepts the terms and conditions. The data treatment in iCity includes:

- data management for the authentication;
- data management for statistical purposes;
- data profiling for providing services;
- data concerning the API and dataset used by the developers for tracking permitting the royalty calculation;
- data concerning the usage of the iCity platform.

So the policy note must include detailed information about these activities.

2.2.6 Additional Normative Material

In addition, we should also take into account two extra regulations, which are basically an extension of the data protection rules, but more focused on specific situations:

- *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 [8].*
- *Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters [10].*

The E-Privacy Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on data protection and privacy in the digital age complements the Data Protection Directive. It translates the principles set out in the Data Protection Directive into specific rules for the electronic communications sector. It deals with the regulation of a number of major issues such as the confidentiality of information, treatment of traffic data, spam and cookies. It again shows the importance of privacy when working with electronic data.

The Council Framework Decision 2008/977/JHA of 27 November 2008 is intended to ensure that an individual's privacy rights are protected regarding the processing of their personal data in the framework of police and judicial cooperation in criminal matters. Protection is provided when these data are transmitted between Member States or from a Member State to an authority established based on title IV of the Treaty of the European Union.

Last but not least, the Article 29 Working Party constantly monitors the new emerging technology, supports the EU legal framework harmonization, collects all the needs from citizens, SMEs, companies. It usually releases reports that are valuable for understanding the new trends in the privacy domain. Recently it released a report on the personal data breach notification[2] and in the past it released a very relevant report about the risks of the apps, API and web application distribute by mobile[3].

2.3 Profiling CM/REC(2010)13

This recommendation CM/REC(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling is applicable to the iCity environment.

Since profiling generates new data for an individual based on data related to other persons, the data subject a priori cannot suspect the existence of correlation processes that might result in certain characteristics of other individuals being attributed to him or her on the basis of a probability calculation.

[2] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[3] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

Therefore the controller must provide the data subject with easier to understand information when profiling is being used and the right of access must be reinforced, both as regards the fact that his or her data is used in the course of profiling and the fact that the profile is being applied to him or her.

There is therefore a need to inform the developers about their profile and about the analytics capabilities around the API calls.

Also, cities need to be aware that profiling could be done by the development community that get access to the data via the iCity APIs. This development community could do data mining activities. The risk is that what seemed to be initially ´not sensitive´ data, could become very sensitive if data mining activities have been performed.

2.3.1 The characteristics of profiling

Profiling, as understood in the context of this recommendation, takes place in three technically distinct stages:

- A stage during which digitised observations regarding individuals´ behaviour on characteristics are collected and stored on a large scale (data warehousing). The resulting data may be nominative, coded or anonymous.
- A stage during which these data are analysed and “probed” (data mining) permitting the determination of correlations between different behaviours/characteristics and other behaviours or characteristics.
- An inference stage during which, on the basis of certain observable behavioural variables or characteristics specific to a generally identified individual, new past, present or future characteristics or behavioural variables are deducted.

It should be noted that the first two stages (data warehouse and data mining) can be carried out using anonymised or coded data.

As a general rule the third stage concerns an individual who is identified or is identifiable, and is carried out as described above, in a growing variety of fields and by increasing numbers of actors.

2.3.2 Profiling risks

Invisibility in processing and of the data processed

In case of data processing without profiling, the personal data are factually accurate and relate to identified or identifiable individuals. In this context, data subjects are generally aware of, or can guess the nature of the information the data controller holds concerning them. Since profiling generates new data for the individual, he cannot suspect the existence of that data.

Binding application of others people´s data

Individuals are in practice answerable for their own actions and are held socially and legally responsible for them. But what if other data exist about you and you are not aware?

Inevitable uncertainty

Since profiling is based on the use of statistics, the data cannot always be accurate.

What if you get on a blacklist because of this?

Data decontextualisation

The obligation to respect the right of one's privacy implies that data controllers should only process data pertaining to one sphere of the private life of the individual concerned.

2.4 Transfer of personal data abroad

2.4.1 US-EU Safe Harbor Agreement

The Data Protection Directive is applicable whenever personal data is transferred or moved in the European Economic Area. But what happens when data is transferred outside this Area? In a globalized world, the transfer of data to third countries has become an essential factor in daily business life. Future smart cities will definitely encounter this matter because inevitably they will move citizens' personal data abroad, for example to store the data in a cloud or similar data center.

In particular, whilst the US and the EU agree on the importance of the protection of the privacy of their citizens, they have a different approach to privacy. The US focuses more on a mix of legislation, regulation and self-regulation. The EU, on the other hand, relies on comprehensive legislation that requires, for example, the creation of independent government data protection agencies, registration of databases with these agencies and in some instances prior approval of the individual before personal data processing may begin. All these differences have a negative impact on the engagement of US organizations in trans-Atlantic transactions [10].

For example, if personal data is transferred to the US for storage, the American government can access the data based on federal anti-terrorist legislation, without informing the concerned individual. This is a breach of the European privacy principles and therefore the transfer of personal data to a non-EU country is prohibited, unless there is a guarantee that it will receive equivalent and adequate levels of protection.

The solution that has been agreed between the US Department of Commerce in consultation with the European Commission is called the 'Safe Harbor' framework. This was approved by the EU in 2000 and is a streamlined process for US companies to comply with the European Directive on Data Protection. It does not mean that the third country has the same regulations as Europe. It only means that, under the specific circumstances, the country/organization offers sufficient and adequate protection [2]. Examples of Safe Harbor certified companies are Microsoft, Google and Facebook. Adequate or equal protection can either be at a country level (the country's laws offer equal protection) or at an organizational level (where a multinational organization produces and documents its internal controls on personal data) [12].

Organizations can enter the agreement voluntary, as long as they respect the principles outlined in the Directive. If they meet the European Union's requirements, they can obtain a certificate which they have to register. Being part of the agreement helps US organizations avoid interruptions in their business with the EU and prevents them being prosecuted by an EU Member State authority under privacy laws [10].

Principles:

The Safe Harbor Agreement contains 7 privacy principles with which organizations must comply [10].

1. Notice: individuals must be informed about the purpose of collection and use of their personal data.
2. Choice: individuals have the right to opt out of the collection and forward the transfer of data to third parties.
3. Onward transfer: transfer of data to third parties is only possible if the other organizations follow adequate data protection principles.
4. Access: individuals have the right to access their information and correct, amend or delete it, if it is inaccurate.
5. Security: reasonable efforts need to be made to prevent loss, misuse and unauthorized access, disclosure, alteration and destruction of the collected data.
6. Data integrity: the data has to be relevant and reliable for the purpose for which it was collected.
7. Enforcement: there should be effective means to enforce these rules.

Further information on how to join the US-EU "Safe Harbor" agreement, the enforcement and principles, can be found on the website that the US Department of Commerce and the European Commission developed together: http://export.gov/safeharbor/index.asp

2.4.2 Data storage abroad

Outsource or not?

As mentioned in the previous sub-section, personal data can be stored abroad (in the US) under the Safe Harbor Agreement. Another aspect that is associated with storage abroad is the issue of licensing. Most cities will use Open Source software and open standards to limit license contracts and fees, but as smart cities grow and more people get involved, they will have to make use of companies specialized in database management to store the data they collected. An example of such a company is the Oracle Corporation in the US. Whether the city decides to outsource the management to such a company or to store the data itself, is an import consideration it has to make.

When a city stores the data itself, there are certain benefits: complete control over where the data resides, how the data is stored and who has access to the data.

Unfortunately, storing data on its own servers is a very expensive business for cities. To store the data of an entire city, the server will have to be able to store hundreds of Terabytes and the city will have to find the space to install it, the resources to manage it, and pay the energy costs to operate it and cool it. For these reasons, smaller cities in particular will choose to outsource the storage to companies specialized in database management or cloud based services.

Security issues

Although a city probably saves a lot of money by outsourcing the data management, it still has to keep certain security issues in mind. First and foremost are the legal issues concerning data residency. Depending on where the data is physically stored, different regulations apply.

Another point of attention is the transfer of data.

Fortunately, there are some solutions for cities to circumvent these issues.

Solution 1:

One solution is for European cities to outsource the database management to a company located in Europe. The city should make sure that the company is completely located in Europe and should get a guarantee that the company is not using geographically removed data centers. In this case, the Data Protection Directive is applicable and the protection of the data is secured. Also, the distance the data needs to cover while being transferred, is a lot shorter which can reduce security issues. If the company still wants to work with a company outside the European Economic Area, we refer back to the Safe Harbor Agreement regarding privacy protection. If it is not possible to work with a European company but the city chooses to work with for example the Oracle Corporation (US), the city could try to stipulate in the license contract to have the server located in one of Oracle's European branches.

Solution 2:

Another solution is to encrypt data that is stored and transferred. This is a viable security tool for maintaining privacy if the city keeps the methods to decrypt and access to data under its control.

Solution 3:

The city could anonymize the data by using some type of token-based referencing system. Personal data is stored, but only as reference values. Like in the previous option, the city has to keep control over the de-referencing. Once the data is de-referenced, it will never be stored, but only used in secure transactional systems [13].

2.5 Retention of data

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.

Smart cities should take the Data Retention Directive [15] into account because it obliges them, as a provider of publicly available electronic communications services, or of public communications networks, to retain certain telecommunications data, which is generated or processed by them, for a certain period in time. The data has to be retained by cities to ensure that they are available for the purpose of investigation, detection and prosecution of serious crime, as defined by each Member State in its national law (Article 1 of the Data Retention Directive).

2.5.1 Scope of the directive in a city environment

The Directive applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user (Article 2). It does not apply to the content of electronic communications (including information consulted using an electronic communications network).

The main reason for cities to retain data is traffic analysis and mass surveillance. Analyzing the retained data makes it possible to identify the location of an individual at a certain time. This data can be useful for police and security departments to find out more about criminal incidents or to check correspondence to prevent certain criminal activities. Again, privacy

issues occur, especially because certain governments want to use data retention in the war against terrorism.

Data retention can also be necessary for commercial reasons. The data retained will then consist of transactions done on the web and websites visited [16].

For example if a city opens up its WIFI-network for citizens, it has to store certain data like the e-mails that were sent and received, the websites that were visited and certain location data.

Also, if a city provides a telephone network, it has to retain the telephone calls made and received by its citizens, so that police or security departments are able to keep track of who had contact with whom via e-mail, phone or SMS. The content however remains confidential.

2.5.2 Principles

To summarize the main principles of this Directive:

1. Access: only given to qualified national authorities after following a procedure recorded by national law.
2. Categories: different categories of data have to be retained (Article 5)
3. Retention period: at least 6 months to a maximum of 2 years from the date of the communication.
4. Data protection:

- the retained data shall be of the same quality and subject to the same security and protection as data on the network;
- the data shall be subject to appropriate technical and organizational measures to protect it against accidental or unlawful destruction, accidental loss or alteration, or unauthorized or unlawful storage, processing, access or disclosure;
- the data shall be subject to appropriate technical and organizational measures to ensure that they can be accessed by specially authorized personnel only;
- the data, except that which has been accessed and preserved, shall be destroyed at the end of the period of retention.

5. Supervision: a supervisory authority should be established to control the compliance of the rules in the Directive.

Mirroring and Cloud Computing Platform

In case of the iCity platform being mirrored across different server equipment or hosted in a cloud computing environment, the analysis and protection regards privacy issues will have to be replicated for every country involved.

3. Limitation to publishing open government data

Because the cities are public administrations, the majority of the national law about privacy doesn't permit to the public entities to manage, distribute or transmit personal data without a legal purposes or a specific national act. For this reason it is important to conduct an analysis of each dataset provided by the public administrations and also the API provided by the (infrastructure owners) in each city.

Italian case:

In Italy for example is not possible to publish open data that could have some side effect on the building market or that could have a relevant impact on the financial market. It is just an example because the art. 24 of the act 241/90 defines all the limitations to the open data and the art. 4 of the recent legislative decree 33/2013 lists the limitations to the transparency.
For this reason some dataset are not admitted for free publication.
It is not a problem of privacy only, but a problem of national security, internal order, national secret, general market disruption, statistical secret, administrative secret, human rights protection (e.g. refugees).

1. Environmental data

Another example is about environment data that in Europe is regulated by the directive 2003/4/CE. The scope of this directive is defined in the art. 1:

"To guarantee the right of access to environmental information held by or for public authorities and to set out the basic terms and conditions of, and practical arrangements
for, its exercise"

The art. 4 provide also limitation to the access of the environmental data provided by the public administration. Among the other the point (b) and (d) of the paragraph 2 is particular interesting:

"(b) international relations, public security or national defence;"

"(d) the confidentiality of commercial or industrial information where such confidentiality is provided for by national or Community law to protect a legitimate economic interest, including the public interest in maintaining statistical confidentiality and tax secrecy;"

This means that in case the open government data affects a specific economic interest of some private subject (e.g. building price) it could be prudent to not release those dataset in a very precise way but in a more aggregated manner.

2. Geographic data

Another important European directive[4] is about the spatial data in digital format Directive 2007/2/EC:
"'spatial data' means any data with a direct or indirect reference to a specific location or geographical area;"

[4] http://inspire.ec.europa.eu/

Also in this directive the Art. 13 defines the limit of the public access of some spatial data:
“The confidentiality of the proceedings of public authorities, where such confidentiality is provided for by law;

(b) International relations, public security or national defence;

(c) The course of justice, the ability of any person to receive a fair trial or the ability of a public authority to conduct an enquiry of a criminal or disciplinary nature;

(d) The confidentiality of commercial or industrial information, where such confidentiality is provided for by national or Community law to protect a legitimate economic interest, including the public interest in maintaining statistical confidentiality and tax secrecy;

(e) Intellectual property rights;

(f) The confidentiality of personal data and/or files relating to a natural person where that person has not consented to the disclosure of the information to the public, where such confidentiality is provided for by national or Community law;

(g) The interests or protection of any person who supplied the information requested on a voluntary basis without being under, or capable of being put under, a legal obligation to do so, unless that person has consented to the release of the information concerned;

(h) The protection of the environment to which such information relates, such as the location of rare species.”

3. National level limitation to the public access of data

Each country has these implemented limits to the public access of data by national legal framework, for this reason it is important to check carefully the dataset before releasing it in the iCity platform.

4. IPR Issues

4.1 Legal protection of databases of profiling and accounting

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

As mentioned above, smart cities will have to collect and store personal data about their citizens. To keep an overview of all these data, cities will have to create databases which they can keep themselves or transfer to a database management company. In any case, the city keeps the ownership over the databases. Both the form as the content of these databases should be protected against unauthorized use or abuse. Therefore, the Database Directive was defined [16]. Its provisions apply to both analogue and digital databases.

4.2 Licensing for the developers

When a city decides to store its data with a database management company, it pays the company for its service and from then on, the city can access the collected data at all times. It can also buy licenses to give access to the data to certain users. This is a static model in which the city buys a limited amount of licenses. The entire situation becomes much more complex when the city wants to open up this data to the public, or to 3rd party developers. The city will inevitably have to buy many more licenses to give access to the data to several users at the same time.

For example if a city allows 3rd party developers to develop an application based on data from an Oracle API, it has to get a license from Oracle to be able to let the developers make the application (direct access to data). Afterwards, the city will also need licenses to let its citizens access the data via the application (indirect access to data).

Buying a large amount of licenses requires a very large investment from the city. Furthermore, it cannot predict how many citizens will use the app, which could lead to the purchase of too many or too few licenses. A more dynamic licensing model is needed, in which a city agrees to buy a certain amount of licenses for every app, and has the option to buy more if needed. Oracle, for example, provides this in its 'Pay-as-you-grow' licensing model [14].

4.3 Copyright

The *Directive 96/9/EC* offers copyright protection for those databases that are sufficiently creative. For the copyright law to be applicable, a database should be 'a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means' (Article 1 of the Database Directive). The protection only applies to the specific structure, arrangement or form of the content ('original database') (Article 3, part 3). The copyright protection does not extend to the content of the database [17]. The city is protected against the temporary or permanent reproduction of the database; the translation, adaptation, arrangement and any other

alteration; any form of distribution to the public or of copies (subject to the exhaustion of rights); any communication, display or performance to the public; any reproduction, distribution, communication, display to the public of a translation, adaptation, etc. (Article 5).

4.3.1 Sui generis right

The *Directive 96/9/EC* also offers a new form of protection for other databases, the so called *sui generis* right. It is a specific property right for databases that is unrelated to other forms of protection such as copyright. This right protects the content of the database and the substantial investment of time, money and effort the city made. This is irrespective of whether the database is innovative in itself ('non-original' databases). The *sui generis* right provides the city with the right to prohibit the extraction and/or re-utilization of the whole or of a substantial part of the content, evaluated qualitatively or quantitatively (Article 7). The *sui generis* protection is valid for 15 years (Article 10) [17].

4.4 Liability

For guaranteeing a robust and sustainable business model, a crucial issue is the definition of the liability of the cities regarding the dataset or the API use. The cities will release datasets with a proper license where they discharge any liability respect the improper, illegal use of the dataset. License cc-by v.4.0 includes this part:

"Section 5 – Disclaimer of Warranties and Limitation of Liability.
Unless otherwise separately undertaken by the Licensor, to the extent possible, the Licensor offers the Licensed Material as-is and as-available, and makes no representations or warranties of any kind concerning the Licensed Material, whether express, implied, statutory, or other. This includes, without limitation, warranties of title, merchantability, fitness for a particular purpose, non-infringement, absence of latent or other defects, accuracy, or the presence or absence of errors, whether or not known or discoverable. Where disclaimers of warranties are not allowed in full or in part, this disclaimer may not apply to you.
To the extent possible, in no event will the Licensor be liable to You on any legal theory (including, without limitation, negligence) or otherwise for any direct, special, indirect, incidental, consequential, punitive, exemplary, or other losses, costs, expenses, or damages arising out of this Public License or use of the Licensed Material, even if the Licensor has been advised of the possibility of such losses, costs, expenses, or damages. Where a limitation of liability is not allowed in full or in part, this limitation may not apply to you."

Otherwise for the API the cities approve the request from the developers (aka proposal for apps) and on the base of the detailed description of the proposal apps, they can provide the assent or the rejection. Also in this case the assent doesn't mean that the city is liable respect any damage produced by the apps to third parties. This clause will be included in the service contract that any developers should accept on line.

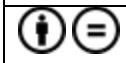
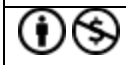
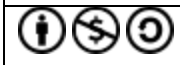
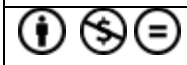
Important is also the identification of the digital identity of the developer in case of infringement of the service contract or for any other legal issue. So the consortium of iCity have to ask a strong authentication to the developers if they intend to use API and submit proposal for apps.

4.5 Dataset

The dataset in the European legal framework is a "data base" and so it is protected with the *sui generis right*. There are different licenses for protecting the dataset and in meantime to permit

the circulation of them in the open data community. The next paragraph lists the most important category used in worldwide (creative commons) and also other minor categories used especially in Europe.

4.5.1 Creative Commons

Symbol	Abbreviation	Right	Description
	CC BY	Attribution to the owner of the dataset	It is possible to distribute, modify, and create derivative works, also for commercial purposes with the condition to include the attribution of the owner.
	CC BY-SA	Attribution, with the same license for the derivative works	It is possible to distribute, modify, and create derivative works, also for commercial purposes with the condition to include the attribution of the owner and to distribute with the same viral license.
	CC BY- ND	Attribution and no derivative works allowed.	It is possible to distribute, but not modify nor create derivative works. The use is also for commercial purposes with the condition to include the attribution of the owner.
	CC BY- NC	Attribution to the owner of the dataset and commercial use is not allowed. This license is not open source	It is possible to distribute, modify, create derivative works, but NOT for commercial purposes and with the condition to include the attribution of the owner.
	CC BY- NC- SA	Attribution to the owner of the dataset, commercial use is not allowed, any derivative work must be released with the same license of the owner. This license is not open source	It is possible to distribute, modify, create derivative works, but NOT for commercial purposes and with the same license of the owner.
	CC BY- NC- ND	Attribution to the owner of the dataset, commercial use is not allowed as well as the derivative work. This license is not open source	It is possible to distribute, but not modify nor create derivative works. The use is for noncommercial purposes with the condition to include the attribution of the owner.

Inside of the creative common community there are different release, in particular the v 4.0 includes the sui generis right in order to adapt the creative commons licenses also to the open data:

There are also different releases over time with different characteristics.

Version CC0 1.0	**Version 2.0**	**Version 3.0**	**Version 4.0**
The author waives to the owner right.	Deprecated because they didn't include attribution.	This version includes national and local translation legally binding in each country where it was translated.	Sui generis right included. International license in English.

4.5.2 Other Open Data Licenses

There are several other licenses used in the world

Open Government License – 2.0	UK, National Archive		Compatible with cc-by or ODC-by
OGL-Canada-2.0	Canada		Compatible with cc-by or ODC-by
ODBL	Several countries		Compatible with cc-by-sa
ODC-BY	Several countries		Compatible with cc-by
PDDL	Several countries		Dedicate to the Public Domain (all rights waived)
Free Art License			Compatible with cc-by-sa
IODL	Italy		
IO	France		Compatible with OGL and cc-by
Datenlizenz Deutschland Namensnennung (3052)	Germany		
NLOD	Norway		OGL cc-by ODbL
Common Documentation	Spain		

License	http://datos.gob.es/content/publicar-datos-reutilizables		
European Union Public License - EUPL	http://ec.europa.eu/idabc/en/document/7774.html		
European Commission Re-use legal notice	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:330:0039:0042:EN:PDF		

4.6 API

The regime of protection of API is controversial. The European Court of Justice decided in May 2012 in the case-law SAS Institute Inc. v. World Programming Ltd that the API is not eligible for copyright protection.

http://curia.europa.eu/juris/document/document.jsf?text=&docid=122362&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=972439

In the same period, May 2012, also another decision from the District Court of the North Carolina reinforced this orientation: in the case-law Oracle v. Google, Google won the battle to use the API of Android developed by Oracle, without any infringement of copyright.

So it seems that the API is not copyrightable following the recent jurisprudence and case-law, however it is better in iCity to impose a legal policy on this topic to avoid having problems, simply due to new appeal decisions by the courts.

4.6.2 Open source license

The Open source license includes several types of licenses, figure 4 below shows the relationship amongst this constellation.

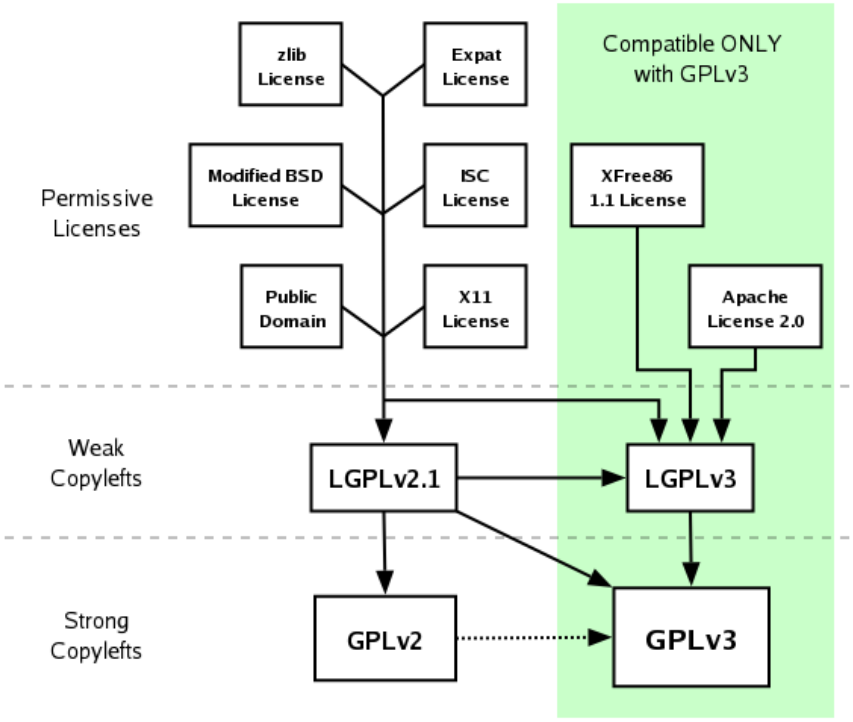


Figure 4: GNU graphic about the open source license

4.7 Problem of compatibility of the licenses

One of the frequent problems arising in second generation Open Data is the compatibility of the licenses among the dataset. Especially when the developer needs to mix together data coming from private and public sector it is difficult to understand firstly if the licenses are compatible, secondly which license is possible to apply to the new enriched dataset. For this reason in the iCity platform it will be fundamental to store the licenses for each dataset and API and then to provide a software module to help the developer to select and check the licenses compatibility. The legal reasoning and logic rule modelling, combined with the compliance verification would be a useful instrument for implementing future iCity platform tools.

5. eCommerce Issues

5.1 Premise

The iCity platform could be used also to sell dataset and APIs developed by the community. More information about this function could be found in the business model.

This activity could be included in the definition of electronic commerce (e-commerce).

It's important to underline that also an NPO (Non-Profit Organization) is subject to e-commerce legal rules.

The Electronic Commerce Directive 2000/31/EC of the European Parliament and of the Council of June 8th 2000, sets up an Internal Market framework for electronic commerce.

Its aim is to provide legal certainty for business and consumers. It establishes harmonised rules on issues such as the transparency and information requirements for online service providers, commercial communications, electronic contracts and limitations of liability of intermediary service providers.

This Directive shall not apply to: (a) the field of taxation; (b) questions relating to information society services covered by Directives 95/46/EC and 97/66/EC; (c) questions relating to agreements or practices governed by cartel law; (d) the following activities of information society services: the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority; the representation of a client and defence of his interests before the courts; gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.

5.2 Definitions

For the purpose of this Directive, the following terms shall bear the following meanings:

(a) information society services: services within the meaning of Article 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC;

(b) service provider: any natural or legal person providing an information society service;

(c) established service provider: a service provider who effectively pursues an economic activity using a fixed establishment for an indefinite period. The presence and use of the technical means and technologies required to provide the service do not, in themselves, constitute an establishment of the provider;

(d) recipient of the service: any natural or legal person who, for professional ends or otherwise, uses an information society service, in particular for the purposes of seeking information or making it accessible;

(e) consumer: any natural person who is acting for purposes which are outside his or her trade, business or profession.

The Information Society Services are defined from Directive 1998/34 as any Information Society service, that is to say, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

For the purposes of this definition:

- at a distance: means that the service is provided without the parties being simultaneously present;

- by electronic means: means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;

- at the individual request of a recipient of services: means that the service is provided through the transmission of data on individual request.

5.3 Obligations

The first obligation of the service provider is to inform the user.

In addition to other information requirements established by Community law, Member States shall ensure that the service provider shall render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information (art. 5):

(a) the name of the service provider;

(b) the geographic address at which the service provider is established;

(c) the details of the service provider, including his electronic mail address, which allow him to be contacted rapidly and communicated with in a direct and effective manner;

(d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register;

(e) where the activity is subject to an authorization scheme, the particulars of the relevant supervisory authority;

(f) as concerns the regulated professions: any professional body or similar institution with which the service provider is registered, the professional title and the Member State where it has been granted, a reference to the applicable professional rules in the Member State of establishment and the means to access them;

(g) where the service provider undertakes an activity that is subject to VAT, the identification number referred to in Article 22 of the sixth Council Directive 77/388/EEC of 17 May 1977 on the harmonization of the laws of the Member States relating to turnover taxes - Common system of value added tax: uniform basis of assessment;

(h) where information society services refer to prices, these are to be indicated clearly and unambiguously and, in particular, must indicate whether they are inclusive of tax and delivery costs;

In addition to other information requirements established by Community law, Member States shall ensure, except when otherwise agreed by parties who are not consumers, that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:

(a) the different technical steps to follow to conclude the contract;

(b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible;

(c) the technical means for identifying and correcting input errors prior to the placing of the order;

(d) the languages offered for the conclusion of the contract.

Member States shall ensure that, except when otherwise agreed by parties who are not consumers, the service provider indicates any relevant codes of conduct to which he subscribes and information on how those codes can be consulted electronically.

Contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them.

Member States shall ensure, except when otherwise agreed by parties who are not consumers, that in cases where the recipient of the service places his order through technological means, the following principles apply:

- the service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means,

- the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.

Member States shall also ensure that - except when otherwise agreed by parties who are not consumers - the service provider makes available to the recipient of the service appropriate, effective and accessible technical means allowing him to identify and correct input errors, prior to the placing of the order.

The legal analysis will be more detailed in the light of the characteristics of the legal entity that will be defined in the business model.

It must be verified, as well as European law, even the national norms that implement the European Directives.

5.4 Consumer Rights

The legal analysis of the platform implies also the analysis of the so called “consumer law” in particular in connection with e-commerce services.

The platform in fact delivers services, by distance contracts, not only in favour of professional users but also of consumers.

So the owner of the platform has also to respect the consumer law.

The Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 regulates consumer rights.

This Directive amends Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council.

It should further study the legal national rules implementing Community principles.

On the other hand the latter analysis can only be completed once the definition of the business model and the identification of the characteristics of the legal entity that will manage the platform have been defined.

5.5 Obligations

The Directive, in particular, introduces additional information requirements for the consumer's benefit in order to better protect their rights.

Before the consumer is bound by a distance contract, or any corresponding offer, the trader shall provide the consumer with the following information in a clear and comprehensible manner:

(a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;

(b) the identity of the trader, such as his trading name;

(c) the geographical address at which the trader is established and the trader's telephone number, fax number and e-mail address, where available, to enable the consumer to contact the trader quickly and communicate with him efficiently and, where applicable, the geographical address and identity of the trader on whose behalf he is acting;

(d) if different from the address provided in accordance with point (c), the geographical address of the place of business of the trader, and, where applicable, that of the trader on whose behalf he is acting, where the consumer can address any complaints;

(e) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges and any other costs or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable. In the case of a contract of indeterminate duration or a contract containing a subscription, the total price shall include the total costs per billing period. Where such contracts are charged at a fixed rate, the total price shall also mean the total monthly costs. Where the total costs cannot be reasonably calculated in advance, the manner in which the price is to be calculated shall be provided;

(f) the cost of using the means of distance communication for the conclusion of the contract where that cost is calculated other than at the basic rate;

(g) the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services and, where applicable, the trader's complaint handling policy;

(h) where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right in accordance with Article 11;

(i) where applicable, that the consumer will have to bear the cost of returning the goods in case of withdrawal and, for distance contracts, if the goods, by their nature, cannot normally be returned by post, the cost of returning the goods;

(j) that, if the consumer exercises the right of withdrawal after having made a request in accordance with Article 7 or Article 8, the consumer shall be liable to pay the trader reasonable costs in accordance with Article 14;

(k) where a right of withdrawal is not provided for in accordance with Article 16, the information that the consumer will not benefit from a right of withdrawal or, where applicable, the circumstances under which the consumer loses his right of withdrawal;

(l) a reminder of the existence of a legal guarantee of conformity for goods;

(m) where applicable, the existence and the conditions of after sale customer assistance, after-sales services and commercial guarantees;

(n) the existence of relevant codes of conduct, as defined in point (f) of Article 2 of Directive 2005/29/EC, and how copies of them can be obtained, where applicable;

(o) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract;

(p) where applicable, the minimum duration of the consumer's obligations under the contract;

(q) where applicable, the existence and the conditions of deposits or other financial guarantees to be paid or provided by the consumer at the request of the trader;

(r) where applicable, the functionality, including applicable technical protection measures, of digital content;

(s) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of;

(t) where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it.

The Directive secondly prescribes formal requirements for distance contracts and also the way to give the information requested.

Save where the exceptions provided for in Directive, the consumer shall have a period of 14 days to withdraw (art. 9) from a distance contract, without giving any reason, and without incurring any costs other than those provided for in the same Directive (Article 13 and Article 14).

Finally the Directive regulates the exercise of the right of withdrawal, the consequence of the omission of information on the right of withdrawal, the way to exercise of the right of withdrawal, the Effects of withdrawal, the obligations of the trader and of the consumer in the event of withdrawal.

The legal analysis will be will deepen in the light of the characteristics of the business model. It must be verified, as well as European law, even the national norms that implement the European Directives.

6. Open Government Data Regulation

6.1 Open up Public Data Resources for Re-use. The review of the Directive 2003/98/EC on re-use of PSI

The web site of the Digital Agenda for Europe notes that Public Authorities produce large amounts of data that could become the raw material for new, innovative cross-border applications and services[5].

The 12th of December 2011 the European Commission, in order to achieve the aims as indicted in the DAE and to unlock the public data potential across Europe, has launched an "Open Data Strategy for Europe" enacting the so called "Open Data Package".

The decision from the Commission was taken under the Action 3, "Open up public data resources for re-use", of the European Digital Agenda that calls for, by 2012, the review of the Directive on re-Use of Public Sector Information, notably its scope and principles on charging for access and use[6]. The proposal for a revision of the Directive was adopted on 12th December 2011 enacting the above explained Open Data Package. In 2003, the EU adopted the Directive on the re-use of public sector information (PSI Directive)[7]. It has introduced a common legislative framework regulating how public sector bodies should make their information available for re-use in order to remove barriers such as discriminatory practices, monopoly markets and a lack of transparency.

The PSI Directive is into force in the EU and it has been fully implemented by the single Members States since 2008.

According to Art. 1, "Subject matter and scope", the Directive on the re-use of public sector information into force provides a common legislative framework for the European public sector information market: "this Directive establishes a minimum set of rules governing the re-use and the practical means of facilitating reuse of existing documents held by public sector bodies of the Member States".

The Directive 2003/98/EC focuses on the economic aspects of information rather than the access of citizens to information.

It encourages the Member States to make as much information available for re-use as possible. It addresses material held by public sector bodies in the Member States, at national, regional and local levels.

The PSI Directive covers the following issues in respect of PSI:

- Availability;
- Charging;
- Transparency;
- Non-discrimination;

[5] http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-3-open-public-data-resources-re-use

[6] Digital Agenda Action 3: http://ec.europa.eu/digital-agenda/en/pillar-i-digital-single-market/action-3-open-public-data-resources-re-use

[7] DIRECTIVE 2003/98/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of

17 November 2003 on the re-use of public sector information.

http://ec.europa.eu/information_society/policy/psi/rules/eu/index_en.htm

- No exclusive arrangements;
- Licensing;
- Practical tools to facilitate the discovery and re-use of public documents.

The Explanatory Memorandum[8] of the Commission proposal analyses the new general contest that has led to the revision of the Directive 2003/98/EC.

The economic general context has shown and recognized the importance of opening data resources, including public data.

As to the Explanatory Memorandum the general objectives of the EC proposal are:

- "contribute to economic growth and job creation by unlocking the economic potential of government-owned data through improved conditions for the exploitation of PSI";
- strengthen positive effect on the transparency, efficiency and accountability of governments and contribute to citizen empowerment;
- catalyse a change of culture in the public sector, creating a favourable environment for value-added activities resulting from the re-use of public information resources;
- provide the market with an optimal legal framework to stimulate the digital content market for PSI-based products and services, including its cross border dimension;
- prevent distortions of competition on the Union market for the reuse of PSI and ensure specific conditions at different stages of the chain of commercial and non-commercial exploitation of PSI so that access is improved and re-use facilitated;
- made data unlocked, discoverable and effectively available for re-use;
- assure that financial and non-financial transaction costs stays as low as possible;
- ensure that re-users have access to an efficient and effective redress mechanism to be able to enforce their rights;
- reinforce the original Directive in order to overcome the remaining barriers, e.g. lack of information about what data are actually available, restrictive or unclear rules governing access and re-use conditions, discouraging, unclear and inconsistent pricing where the re-use of information is chargeable, and the overall excessive complexity of the process for obtaining permission to re-use PSI, in particular for SMEs;
- eliminate dominant position held by re-users or "hybrid" public bodies in order to avoid discriminatory treatment or unjustified exclusive agreements for the exploitation of PSI;
- remove regulatory and practical borders to re-use across the Union affecting the development of the internal market for PSI re-use;
- ensure the same types of data are available on similar, if not the same, terms and conditions irrespective of their national origin.
- innovate in products based directly on PSI and in complementary products and increase, the combination of different public and private information to produce new goods.

6.2 Analysis of the new Directive 2013/37/UE on PSI.

The following section provides an analysis by articles of the proposed amendments made by the new Directive 2013/37/UE approved the 26 of June 2013.

[8] Proposal for a Directive of the European Parliament and of the Council Amending Directive 2003/98/EC on re-use of public sector information

http://ec.europa.eu/information_society/policy/psi/docs/pdfs/opendata2012/revision_of_PSI_Directive/proposal_directive_EN.pdf

The amendment of Article 3 of the PSI Directive specifically introduce the new general rule that requires Member States to ensure that “existing documents” held by public sector bodies of the Member States shall be “reusable for commercial and non-commercial purposes”, unless covered by the exceptions provided for in the Directive. As to whereas n. 6 of the Amending proposal the Directive 2003/98/EC does not contain an obligation to allow re-use of documents. The decision whether or not to authorise re-use remains with the Member States or the public sector body concerned. At the same time, the Directive builds on national rules on access to documents. Whereas n. 7 of the amending proposal established that “Directive 2003/98/EC should therefore lay down a clear obligation for Member States to make all generally available documents re-usable. The proposed amendment of Article 3 includes therefore under the Directive for the first time libraries, museums and archives. According to whereas n. 10 the scope of application of the Directive is extended to libraries (including university libraries), museums and archives. The Directive does not apply to other cultural institutions, such as operas, ballets or theatres, including the archives that are part of these institutions.

Art. 3, version into force:

General principle

“Member States shall ensure that, where the re-use of documents held by public sector bodies is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.

Where possible, documents shall be made available through electronic mean”.

Art. 3 as to amending proposal will be replaced as follows:

General principle

Subject to paragraph (2) Member States shall ensure that documents referred to in Article 1 shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV. (2) For documents for which libraries (including university libraries), museums and archives have intellectual property rights, Member States shall ensure that, where the re-use of documents is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.

The new Directive update the terminology of previous directive, which referred to “electronic means”, using the expression “machine-readable format” taking therefore into account the advantage of contemporary semantic web technologies (RDF/OWL, Linked data).

As explained in the whereas n. 11 “To facilitate re-use, public sector bodies should make documents available through machine readable formats and together with their metadata where possible and appropriate, in a format that ensures interoperability, e.g. by processing them in a way consistent with the principles governing the compatibility and usability requirements for spatial information under 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)”. According to the new Directive this is the **Article 5** :

Article 5

Available formats

1. Public sector bodies shall make their documents available in any pre-existing format or language, and, where possible and appropriate, in open and machine-readable format together

with their metadata. Both the format and the metadata should, in so far as possible, comply with formal open standards.

2. Paragraph 1 shall not imply an obligation for public sector bodies to create or adapt documents or provide extracts in order to comply with that paragraph where this would involve disproportionate effort, going beyond a simple operation.

3. On the basis of this Directive, public sector bodies cannot be required to continue the production and storage of a certain type of documents with a view to the re-use of such documents by a private or public sector organisation.

As to whereas n. 13 “In relation to any re-use that is made of the document, public sector bodies may, where practicable, impose conditions on the re-user, such as acknowledgment of source. Any licences for the re-use of public sector information should in any case place as few restrictions on re-use as possible. Open licences available online, which grant wider re-use rights without technological, financial or geographical limitations and relying on open data formats, may also play an important role in this respect. Therefore, Member States should encourage the use of open government licences”.

Paragraph 1 of **Art. 8, Licences**, will be replaced by the following:

1. Public sector bodies may allow re-use without conditions or may impose conditions, where appropriate through a licence. These conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.

2. In Member States where licences are used, Member States shall ensure that standard licences for the re-use of public sector documents, which can be adapted to meet particular licence applications, are available in digital format and can be processed electronically. Member States shall encourage all public sector bodies to use the standard licences.

The version into force of **Paragraph 1, Art. 8,** is:

“Public sector bodies may allow re-use without conditions or may impose conditions, such as indication of source, where appropriate through a licence.

These conditions shall not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition.”

Finally Article 9 is replaced by the following:

“Member States shall make practical arrangements facilitating the search for documents available for re-use, such as asset lists of main documents with relevant metadata, accessible where possible and appropriate online and in machine-readable format, and portal sites that are linked to the asset lists. Where possible Member States shall facilitate the cross-linguistic search for documents. ”

The new version of **Art. 6, “Principle governing charging”,** proposes considerable amendments to the charging policy of the Member States establishing that public bodies shall in principle not be allowed to charge more than marginal costs incurred for the reproduction and the dissemination of the public sector document.

Only in exceptional cases higher charges can be made. Accordingly whereas n. 12 of the EC proposal states: “The necessity of not hindering the normal running of public sector bodies

covering a substantial part of the operating cost relating to the performance of their public task from the exploitation of their intellectual property rights should notably be taken into consideration. The burden of proving that charges are cost-oriented and comply with relevant limits should lie with the public sector body charging for the re-use of documents".

Amendments to **Article 6 (Principles governing charging)**

Principles governing charging

1. Where charges are made for the re-use of documents, those charges shall be limited to the marginal costs incurred for their reproduction, provision and dissemination.

2. Paragraph 1 shall not apply to the following:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) by way of exception, documents for which the public sector body concerned is required to generate sufficient revenue to cover a substantial part of the costs relating to their collection, production, reproduction and dissemination. Those requirements shall be defined by law or by other binding rules in the Member State. In the absence of such rules, the requirements shall be defined in accordance with common administrative practice in the Member State;

(c) libraries, including university libraries, museums and archives.

3. In the cases referred to in points (a) and (b) of paragraph 2, the public sector bodies concerned shall calculate the total charges according to objective, transparent and verifiable criteria to be laid down by the Member States. The total income of those bodies from supplying and allowing re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment. Charges shall be calculated in line with the accounting principles applicable to the public sector bodies involved.

4. Where charges are made by the public sector bodies referred to in point (c) of paragraph 2, the total income from supplying and allowing re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, preservation and rights clearance, together with a reasonable return on investment. Charges shall be calculated in line with the accounting principles applicable to the public sector bodies involved.

The version into force of **Art. 6, Principles governing charging,** is:

Principles governing charging

"Where charges are made, the total income from supplying and allowing re-use of documents shall not exceed the cost of collection, production, reproduction and dissemination, together with a reasonable return on investment. Charges should be cost oriented over the appropriate accounting period and calculated in line with the accounting principles applicable to the public sector bodies involved."

6.3 Open Government Data and Personal Data Legislation relationship

Data Protection and the Re-use of Public Sector Information in the European Union is a growing concern after the Commission, on December 12th 2011, adopted the above explained Open Data Package.

The European Data Protection Supervisor (EDPS) has issued an opinion that calls for data protection safeguards before public sector information containing personal data can be re-

used[9]. The opinion provides a detailed analysis covering many important aspects ranging from licensing, anonymization and transfer of data outside of the EU. Peter Hustinx, the EDPS, says: "The re-use of PSI containing personal data may bring significant benefits, but also entails great risks to the protection of personal data, due to the wide variety of data held by public sector bodies. The Commission proposal should therefore more clearly define in what situations and subject to what safeguards information containing personal data may be required to be made available for re-use."[10]

Open Data policies and Data Protection laws have a similar objective: to create a fair environment for the circulation and the processing of data, but from PSI perspective no personal data should enter in the open government data definition and this create some weakness in the coordination among the two topics.

Broad PSI Re-use and Purpose-Bound Personal Data Re-Use: How to Strike the Balance?

The EDPS calls for a Proactive Approach. As to the opinion of EDPS "it is crucial that public sector bodies take a proactive approach when making personal data available for reuse. A proactive approach would make it possible to make the data publicly available with the explicit purpose of reuse, subject to specific conditions and safeguards in compliance with data protection rules".

To ensure data protection compliance EDPS recommends that the Commission develop further guidance on the data protection aspects of PSI re-use taking into account primarily anonymization and licensing. The EDPS suggest the implementation of a template for adequate data protection clauses in licenses.

In particular concluding his opinion EDPS recommends that the EC Proposal of amending PSI Directive should:

- establish more clearly the scope of applicability of the PSI Directive to personal data;
- require that an assessment be carried out by the public sector body concerned before any PSI containing personal data may be made available for reuse;
- where appropriate, require that data be fully or partially anonymized and license conditions specifically prohibit re-identification of individuals and the reuse of personal data for purposes that may individually affect the data subjects;
- - require that the terms of the licence to reuse PSI include a data protection clause, whenever personal data are processed;
- - where necessary considering the risks to the protection of personal data, require applicants to demonstrate (via a data protection impact assessment or otherwise) that any risks to the protection of personal data are adequately addressed and that the applicant will process data in compliance with applicable data protection law[11];

[9] Opinion of the European Data Protection Supervisor on the "Open Data Package"

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-18_Open_data_EN.pdf

[10] PRESS RELEASE EDPS/08/12

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-08_Open_Data_EN.pdf

[11] In this respect see: EVPSI & LAPSI Final Meeting Turin, 9-10/7/2012 Eleonora Bassi University of Turin. In this work are indicated the recommended tools in order to fulfil the EDPS purposes such as: PETs, Privacy by Design, Anonymisation, Privacy Policies, PIA, Codes of Conduct, Guidelines, Anonymisation by Default.

- - clarify that reuse can be made contingent upon the purpose for which reuse is made, in derogation from the general rule allowing reuse for any commercial and non-commercial purposes;

In addition, the EDPS suggests:

- - to consider allowing costs of pre-processing (such as digitalization), anonymization and aggregation to be charged to license-holders where appropriate, and
- - that the Commission develops further guidance, focusing on anonymization and licensing and consult the WP29[12] in this regard.

Furthermore Other important aspects concerning the open data are presented in the LAPSI[13] and EVPSI[14] EU research projects. Nevertheless the Open Government Data area of interest as to the definition of OFKN provided in the Open Data Handbook[15] must be analysed considering also the EU' legislation about Privacy Directive 95/46/EC now under revision by the "General Data Protection Regulation" [16] (especially for the Right to be Forgotten), IPR Directive 2004/48/EC, INSPIRE Directive 2007/2/EC and any other directive or regulation that limit the disclosure of confidential information protected in different domain or concerning special human rights (e.g. refugees, victim of violence, witness protection programme).

With this particular regard the topic of anonymization of open data is not a point in the "General Data Protection Regulation" despite the evident risk of revealing the identity of people using data mining or other statistical tools applied to big open data.

[12] Working Party Art. 29 recommended to adopt a case by case approach "in order to strike the balance between the right to privacy and the right to public access" (Opinion 7/2003, wp 83)

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_en.pdf

[13] http://www.lapsi-project.eu/norms

[14] www.evpsi.org/

[15] http://opendatahandbook.org/

Open Government Data is a subset of Public Sector Information, which is broader in scope. Open Government Data is Public Sector Information (Government Data) that has been made available to the public as Open Data.

As explained in the Open Data Handbook: "Open data, especially open government data, is a tremendous resource that is as yet largely untapped. Many individuals and organisations collect a broad range of different types of data in order to perform their tasks.

Government is particularly significant in this respect, both because of the quantity and centrality of the data it collects, but also because most of that government data is public data by law, and therefore could be made open and made available for others to use".

[16] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

7. iCity Key Legal Points

The relevant user scenarios are:

- The Cities provide links to their open data. The open data are stored in the city local system and they are accessible remotely. iCity uses a cache of the data. The Cities must provide ONLY dataset privacy free and without quasi-identifiers. The licenses that the cities should provide of the dataset MUST be open license: preferably cc-by or cc-by-nd 4.0;
- The Cities provide also API(s). The API should be fair, ethic, privacy compliant and released with an open source license (preferably a permissive license);
- The developers pay iCity for accessing the APIs and platform. The developers develop apps using APIs. The application should be fair, ethic, and privacy free;
- iCity is managing profiling for the end users, developers, officers, citizens. So it requires a privacy policy for managing the account database, profiles, cookies, analytics and registration form.
- iCity has to perform identity management with strong authentication in order to resolve potential infringement and liability cases for third parties.
- Developers need to sign a service contract.
- Cities need to sign a special regulation where they declare that the dataset are compliant with privacy, copyright, administrative law and released with Open Data licence. Also the API should be released with Open Source license.

	Open Data Regulation	Privacy	IPR and License	eCommerce	Non-Profit Organization
iCity platform (legal responsible)	Check if all the datasets the platform provides are legal	Process for managing private data in the iCity platform. Geographical location of hardware equipment Provide Privacy Note. Provide consent to the privacy note. Collect consent	Be sure that all the datasets and APIs included in iCity have a proper license open data and open source.	Check the service provider contract and SLA for providing an eCommerce service in line with the law. Provide the obligatory information for eCommerce service. Provide the obligatory information for Consumer	

		to the privacy note. Provide a proper form of online legislation. Check if the datasets crossing together permit de-anonymization. Guarantee to not transfer the personal data outside of EU.		Law service. In case of payment it is necessary also to respect the rules of the online payment. Provide term of service and track the consent by the developers.	
iCity manager or any partner of NOP	Check if all the datasets are admitted by the national public law, especially concerning the limitations defined by each national law.	Check if the dataset is privacy free and respects the privacy legislation.	Check if the dataset and API are regulated with a proper open data and open source license. Make sure that the API doesn't infringe any IPR.		Each partner need to check the national law if it can enter in the NOP. Each iCity manager must check if its national law permits to receive royalties and revenues. Each iCity manager must check the taxation regime in case of royalties and

					revenues.
developers		He/she must release the consent for the privacy note. He/she must release the consent for the term of service. He/she must ask the authorization to each iCity manager in case the proposal project uses APIs and datasets coming from other cities.	Check if you can release a new dataset or API with Open Data and Open Source licences. If releasing a new dataset or a modified dataset it needs to have a license in line with the IPR.	He/she must be compliant with the terms of service and the e-Commerce and Consumer Law framework. He/she must release APPs with the obligatory information requested by the eCommerce and Consumer Law framework.	

Table 1 user scenario - legal

7.1 Architecture – Legal summary

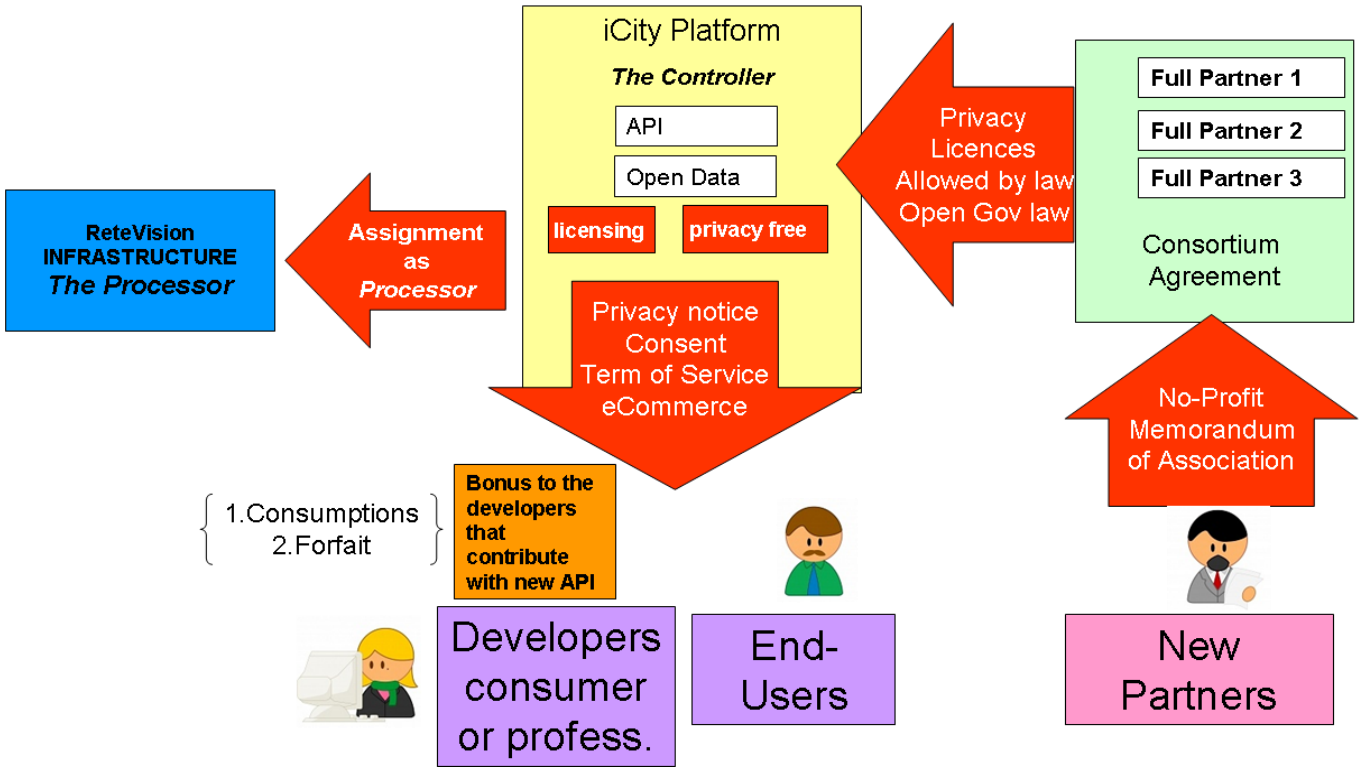


Figure 5: Legal implications of the iCity platform

- The iCity portal functionality is the representation of the relevant information for the different user profiles via the internet. Depending on the user profile, certain services will be made available. Public means that you don't need to authenticate yourself to access the web page; however you do need to authenticate yourself to access the private portal. Via this portal, developers and administrators can get access to the Open Infrastructure, in order to manage it.
  Legal: Recommendation CM/Rec(2010)13 (original convention 108)

- The Web Services Gateway manages the API access and takes care of the authentication and authorization of the API calls.

- The orchestration is the execution engine for business processes and business rules. If existing systems exist in the cities (for example legal approval workflow in the city for a project) then the link can be made here.

- The system management will provide infrastructure and iCity Platform management capabilities.

- The 3rd party applications are the applications made by the cities ecosystem of developers.

None sensitive data could become sensitive due to data mining

- Cities are making their infrastructures available via APIs.

Cities need to their free, specific and informed consent to provide the data

8. Check list for iCity Platform Legal Representative

Privacy	**To check**	**Yes/No**
	Did you identify the jurisdiction of the iCity platform? How many servers at which location you have to run the City platform? Do you have a cloud computing platform?	
	Did you perform all the mandatory procedures related to your Privacy Authority for managing personal data within the iCity platform?	
	Did you provide the Privacy Notice in the online Registration form?	
	Did you collect the consent in the online Registration form?	
	Did you inform the end-user concerning the specific process about profiling and analytics activities?	
	Did you identify your developer community, to be able to contact him/her in case of infringement to the terms of service?	
	Did you check that all your (public and private) datasets, when linked to each other do not permit to de-anonymize the person?	
	Did you obtain from each iCity manager the authorization every time a developer is using the APIs or its datasets?	
	Did you log the process of the authorization between the developer and the iCity managers?	
IPR of the dataset		
	Did you obtain the open data license for the datasets from the iCity managers?	
	Did you obtain the open source for the API license from the iCity managers?	
	Are the licences of the datasets provided by iCity compliant with each other, with a reasonable amount of content?	

Economical Conditions		
	Did you collect the consent to the terms of service coming from the developers/ end-users?	
	Did you provide all the obligatory information with respect to the eCommerce directive?	
	Did you provide all the obligatory information as stipulated in the Consumer Law directive?	
Temporary aspects		
	Did you provide a disclaimer concerning the temporary information connected with the dataset?	

9. Check list for the iCity Manager

This is a check list that each City manager should use to evaluate the risk connected with the dataset and API.

This check list must be signed by the City Manager and stored in the iCity platform in a machine-readable way.

Privacy	**To check**	**Yes/No**
	Is the dataset free of any personal data as defined in the directive?	
	Is the dataset free of any indirect personal data that could be used for identifying the natural person? If so, is there a law that authorize the PA to release them?	
	Is the dataset free of any sensitive personal data? If so is there a law that authorize the PA to release them?	
	Is the dataset free of any information that combined with common data available in the web, could identify the person? If so, is there a law that authorize the PA to release them?	
	Is the dataset free of any information related to human rights (e.g. refugees, witness protection, etc.)?	
	Do you use a tool for calculating the range of the risk of de-anonymization?	
	Are you using geolocalization capabilities ?	
	Did you check that the iCity platform respect all the privacy regulations ?	
	Do you know who are the iCity platform controller and processor of the privacy data of the system?	
IPR of the dataset		
	Do you have created and generated the dataset ?	
	Are you the owner ?	
	Are you sure to not use third party data without the proper authorization and license ?	

Licences		
	Did you release the dataset with an open data license ?	
	Did you include the clause: "In any case the dataset can't be used for re-identifying the person" ?	
	Did you release the API with an open source license ?	
	Did you check that the iCity platform license regime is compliance with your IPR policy ?	
Limitation to the publication		
	Did you check the limitations for the publication stated by your national legislation or by the EU directives ?	
	Did you check if there are some limitations connected to the international relations, public security or national defence ?	
	Did you check if there are some limitations concerning the public interest ?	
	Did you check the international law limitations ?	
Economical Conditions		
	Did you check that the dataset could be released for free ?	
	Did you check if there are some agreements with some other partners in order to release the dataset with a reasonable price ?	
	Did you check if the iCity platform terms of service include a clause of "non liability agreement" regarding the dataset and API provided ?	
Temporary aspects		
	Do you have a temporary policy for updating the dataset ?	
	Do you have some mechanism for informing the end-user that the dataset is updated at a given time to avoid mis-usage and so potential risk of damage ?	
	Did you check if the dataset for some reason can't be indexed by the research engines (e.g. Google, Yahoo, etc.) ?	
	In case of personal data, do you have a reasonable technical mechanism for collecting request of deletion (e.g. right to be forgotten)?	

10. Conclusions

This document discussed the complexity of the legal aspects to be considered by cities willing to become smart by offering services that relate to privacy, data protection, data retention, data transferring and database protection. As discussed in this deliverable, this process can become even more complex when data transactions involve players and locations in different countries and/or continents.

In this perspective, municipalities and city authorities should be aware of the existing obligations and laws when undertaking smart city projects. Particular attention should be devoted to the specific obligations and constraints imposed in each city, country and/or region with respect to aspects directly affecting personal data collection, storage and processing.

As discussed in the last part of this document, laws can be quite different when changing region and when “smart city services” imply data transactions across regions regulated by different rules the situation can become quite difficult and impede the overall service offering.

Cities should therefore closely follow the evolution of both the European and national and local policies and rules. Legislation is dynamic and can change at any time with heavy consequences for the development of a smart city. This is why it is very important that municipalities closely monitor the evolution of the relevant legal aspects to prevent problems.

References

[1] T. Mertens, C. Rotthier, M. Van Oyen. MGM 2011-2012. Guidelines to become a Smart City with the iCity-Platform.

[2] Cuijpers, C., Leenes, R., Olislaegers, S., & Stuurman, K. (2011). De wolk in het onderwijs (privacy aspecten bij cloud computing services). Tilburg: Tilburg Institute for Law, Technology, and Society.

[3] [European Convention on Human Rights. (1950, November 4). Rome.

[4] Charter of Fundamental Rights of the European Union. (2000, December 7).

[5] Directive 95/46/EG of the European Parliament and if the Council of 24 October 1995 the protection of individuals with regard to the processing of personal data and on the free movement of such data, Pb.L. 281 of 23.11.1995, pp. 44–50.

[6] European Parliament; Council. (1995, November 23). Data Protection Directive. Date May 10, 2012, http://eur-lex.europa.eu/: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML

[7] Wikipedia. (2012, June 2). Data Protection Directive. Date May 12, 2012, Wikipedia: http://en.wikipedia.org/wiki/Data_Protection_Directive

[8] [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, Pb.L. 201 of 31.07.2002, pp. 37-47.

[9] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

[10] [U.S.-E.U. Safe Harbor Agreement. (2000). Date Mei 27, 2012, Export.gov: http://export.gov/safe-harbor/index.asp

[11] European Commission. (2000, July 26). Commission Decision. Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and Council on the adequacy of the protection 96 sources provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce.

[12] [Wikipedia. (2012, March 21). International Safe Harbor Privacy Principles. Date 05 27, 2012, Wikipedia: http://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles

[13] [Murphy, A. (2012). Storing Data In The Cloud Raises Compliance Challenges. Forbes, 2.

[14] Oracle. (2012). Oracle Database Appliance. Date June 8, 2012, Oracle: http://www.oracle.com/us/products/database/oracle-database-appliance-ds-495410.pdf

[15] 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, Pb.L. 105 of 13.04.2006, pp. -63.

[16] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Pb.L. 77 of 27.03.1996, pp.0-28.

[17] European Commission - Databases. (2011, May 23). Date May 25, 2012, EC Europa: http://ec.europa.eu/internal_market/copyright/prot-databases/prot-databases_en.htm

[18] Fioretti M., Open Data: Emerging trends, issues and best practices, report of the DIME Eu Project, June 2011, http://www.dime-eu.org/files/active/0/ODOS_report_2.pdf

[19] Fioretti M., Open Data, Open Society, report of the DIME Eu Project, June 2011, http://www.dime-eu.org/files/active/0/ODOS_report_1.pdf

[20] Vickery G., Review of Recent Studies on PSI Re-Use and Related Market Developments. http://ec.europa.eu/information_society/policy/psi/docs/pdfs/report/psi_final_version_formatted.docx

[21] Pollock, R., Welfare gains from opening up Public Sector Information in the UK, University of Cambridge, undated, accessed 1 March 2011, available at: http://rufuspollock.org/economics/papers/psi_openness_gains.pdf

[22] eGovernment Survey 2012, UNPAN, unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

[23] Heli Koski, The Research Institute of the Finnish Economy.Marginal "Does Cost Pricing of Public Sector Information Spur Firm Growth?"

[24] The protection of individuals with regard to automatic processing of personal data in the context of profiling (recommendation CM/Rec(2010)13 and explanatory memorandum

[25] How private is Personal Data ?ISBN 978-92-871-7791-9 IRIS plus 2013-6