Geographic data as personal data in four EU member states

de Jong, A.-J.; van Loenen, Bastiaan; Zevenbergen, J.A.

DOI
10.5194/isprsannals-III-2-151-2016

Publication date
2016

Document Version
Final published version

Published in
XXIII ISPRS Congress, Commission II

Citation (APA)
de Jong, A.-J., van Loenen, B., & Zevenbergen, J. A. (2016). Geographic data as personal data in four EU member states. In L. Halounova, S. Li, V. Safár, M. Tomková, P. Rapant, K. Brázdil, W. Shi, F. Anton, Y. Liu, A. Stein, T. Cheng, C. Pettit, Q.-Q. Li, M. Sester, M. A. Mostafavi, M. Madden, X. Tong, M. A. Brovelli, K. Haekyong, H. Kawashima, ... A. Coltekin (Eds.), *XXIII ISPRS Congress, Commission II* (Vol. III-2, pp. 151-157). (ISPRS Annals of the Photogrammetry, Remote Sensing and Spatial Information Sciences; Vol. III-2). Copernicus. https://doi.org/10.5194/isprsannals-III-2-151-2016

GEOGRAPHIC DATA AS PERSONAL DATA IN FOUR EU MEMBER STATES

A. J. de Jong[a], B. van Loenen[b,], J. A. Zevenbergen[c]

[a] Vicrea, the Netherlands - annejop@gmail.com
[b] Faculty of Architecture and the Built Environment, Knowledge Center Geo-information Governance, Delft University of Technology, the Netherlands - b.vanloenen@tudelft.nl
[c] Department of Urban and Regional Planning and Geo-information Management (PGM) of the ITC, Twenty University, the Netherlands - j.a.zevenbergen@utwente.nl

Commission II, ThS14 - Recent Developments in Open Data

KEY WORDS: Geographic data, data protection, privacy, topography, INSPIRE, open data

ABSTRACT:

The EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data aims at harmonising data protection legislation in the European Union. This should promote the free flow of products and services within the EU. This research found a wide variety of interpretations of the application of data protection legislation to geographic data. The variety was found among the different EU Member States, the different stakeholders and the different types of geographic data. In the Netherlands, the Data Protection Authority (DPA) states that panoramic images of streets are considered personal data. While Dutch case law judges that the data protection legislation does not apply if certain features are blurred and no link to an address is provided. The topographic datasets studied in the case studies do not contain personal data, according to the Dutch DPA, while the German DPA and the Belgian DPA judge that topographic maps of a large scale can contain personal data, and impose conditions on the processing of topographic maps. The UK DPA does consider this data outside of the scope of legal definition of personal data. The patchwork of differences in data protection legislation can be harmonised by using a traffic light model. This model focuses on the context in which the processing of the data takes place and has four categories of data: (1) sensitive personal data, (2) personal data, (3), data that can possibly lead to identification, and (4) non-personal data. For some geographic data, for example factual data that does not reveal sensitive information about a person, can be categorised in the third category giving room to opening up data under the INSPIRE Directive.

1. INTRODUCTION

In 1957, the Treaty of Rome was signed, and the European Economic Community (EEC) established. One of the goals of the Treaty was the creation of a common market. In 1992 the Treaty of Maastricht was signed and in 1993 the creation of a single market was realized. In this internal market companies are able to produce and sell products without barriers (European Commission, 2014). However, today barriers for companies operating in the single market exist. Reusers of the data have problems with varying licensing, pricing and transparency norms in Member States to create value added products on the European internal market (European Commission, 2011a). Also differences in the implementation of personal data protection legislation are problematic from a reuser's standpoint. When geographic data is considered personal data, there are strict conditions for storing, using and processing the geographic data. At first it may appear no geographic dataset can be considered personal data, but this is not necessarily true. Research shows that EU Member States implement the Personal Data Protection Directive in different ways (Korff, 2002 and 2010). To what extent geographic data is considered personal data differs between the different Member States.

The differences in implementation of personal data protection legislation between EU Member States raises questions about the extent to which geographic data is personal data and why the different datasets are considered personal data. In this research implementation of the EU Directive on personal data protection in respect to geographic data in four Member States is studied. This research gives recommendations for further harmonised personal data protection regulations in the European Union to support a common European market for geographic data.

2. EU DATA PROTECTION

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, sets the legislation to regulate the processing of personal data in the EU. It aims at harmonising the data protection in the EU to improve the internal market to ensure that not only personal data is able to flow freely from one Member State to another, but also that the fundamental rights of individuals are safeguarded (recital 3; European Commission, 2012a). The purpose of the directive is to harmonise personal data protection laws amongst the EU Member States. To reach this goal the Directive sets a minimum level of protection (Fromholz, 2000, p.468).

Directive 95/46/EC defines personal data as: "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" (European Union, 1995, article 2a).

National laws must guarantee that processed personal data is up-to-date, accurate, relevant, and not excessive (European Union, 1995). Also processing personal data that contains information about "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or concerning health or sex life" is firmly confined and can only be processed if the person has given written permission (European Union, 1995, p.40; Cate, 1995, pp. 433-434).

The objectives of the Personal Data Protection Directive have only been partially achieved (European Commission, 2012a). Data collection and data sharing across borders has increased with the use of Internet, this led to challenges to the objectives of Directive 95/46/EC.

A challenge to the harmonisation is the different implementations of Directive 95/46/EC by the Member States, due to the differences in definition of personal data. The differences in enforcement, implementation and interpretation between EU Member States have also hinder the internal market, and cooperation between public authorities. Facilitation of free flow of data in the internal market is compromised by these differences and have led to legal fragmentation with high costs, the administrative burden has been estimated at three billion euros (European Commission, 2012a).

Business transactions are often supported by information technology, this leads to a flow of personal information. Online services are accessible to all EU Member States, resulting in different flows of personal information across borders. The fragmentation in the personal data protection stems from the different interpretations of the broad definitions in Directive 95/46/EC (European Commission, 2012a).

A part of the discussion focusses on the differences between Member States on the ‘identifiability’ of a person. Recital 26 of Directive 95/46/EC (European Union, 1995) describes identifiability as: “Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonable to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable;” (European Union, 1995, recital 26).

The focus of the discussions is on the “all the means likely reasonable to be used” (European Union, 1995, recital 26). Another definition in the recital that led to differences in implementation by Member States is “to be used either by the controller or by any other person to identify the said person any other person” (European Union, 1995, recital 26). An example of this form of identification is the use of biometrics. Biometrics are a unique identifier, but the knowledge and access to biometric databases are hard to obtain for the average person (Cuijpers and Marcelis, 2012).

The definition of possible identification may lead to a stretch of the concept of personal data. This stretched definition is further used in opinions of the Article 29 Working Party (Cuijpers and Marcelis, 2012). When this stretched definition is used on an open source, for example the Internet almost all of the data on the internet is personal data. Examples are HTTP cookies and IP-addresses. Because use of this data in combination with other data can lead to identification of a person, the Article 29 Working Party considers this personal data.

The European Commission proposed a reform of the data protection rules. Some key features of this reform are the right to be forgotten and one set of data protection rules for the European Union (European Commission, 2012).

The proposed General Data Protection Regulation adds a new category of personal data to the personal data suite: pseudonymous data. It defines pseudonymous data as: “personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution” (European Parliament, article 4.2a, 2014).

However, the proposed General Data Protection Regulation does not reform the personal data definition but rather extends the definition.

3. GEOGRAPHIC DATA

Geographic data is data with a link to a place on earth, or an address, for example coordinates, and zip-codes. One way of dividing geographic data is in two types: administrative and factual geographic data.

The administrative type of geographic data contains datasets with addresses, zip-codes and cadastral outlines. This type of data is virtually present, but not factual on the earth. The factual type of geographic data contains datasets with topographic maps, elevation and (aerial) photographs of the environment. This type of data represents a factual place on earth (Van Loenen et al., 2008). Geographic data with the highest reuse rate (Fornefeld et al., 2008) is:

1. Topographic information
2. Cadastral information, including addresses and coordinates.
3. Aerial photography.

The themes from the Infrastructure for spatial information in the European Community (INSPIRE) include both themes regarding administrative types of geographic data, and factual geographic data (INSPIRE themes, 2014).

4. RESEARCH METHODOLOGY

To look at the differences between the EU Member States, different EU Member States have been selected as case studies. The selection is based on the differences in policy on open geographic data and the differences in the interpretation of the Directive 95/46/EC.

The first case is the Netherlands. The Netherlands is among the higher ranked open data countries (see Table 1). There is also a lot of open geographic data available. The case is used to give an insight into how personal data is defined and how geographic data is defined, and to what extent geographic data is considered personal data.

Country	Ranking Global Open Data Index	Ranking European Union Privacy Index
Belgium	35	10
Germany	26	4
The Netherlands	8	21
United Kingdom	2	28

Table 1 Ranking case study countries in Open Data Index (Open Data Index, 2015) and Privacy Index (Privacy International, 2007)

The second case is Belgium. The choice for Belgium is based on the high rank in the privacy index (Privacy International, 2007). The culture resembles the Dutch culture, and the same language is spoken.

The third case is Germany. Germany has one of the strictest views on personal data protection. It is in the shared fourth rank of the privacy index (global level) (Privacy International, 2007). An example is the resistance to Google Street View (Focus Magazin, 2009).

The fourth and last case is the United Kingdom, because it is part of the 'big three' of most powerful EU member states that took initiative for the Personal Data Protection Directive (Newman, 2008). In the UK, there is a less strict definition of data protection than elsewhere in the EU (Janssen in Van Loenen, 2011). It is also the most open EU Member State (Open Data Index, 2015), this makes it a typical case to see in what way geographic data can be considered personal data.

The case studies are focused on INSPIRE data consisting of (1) topographic maps and addresses and building data, and (2) mobile mapping data consisting of geographic data collected via photographs such as 360 panorama shots and aerial photography, for example, Google Street View images, aerial photographs of homes and satellite images of homes.

The case-studies are analysed based on the different interpretations of the concept of personal data. In our assessment we included the four countries and the perspectives of different stakeholders within a country. First the perspective of the legislator is analysed, and after that the executers of the legislation, the data protection authority and the courts. In this research the differences are interpreted and after that interpretation analysed and a solution to harmonize the different interpretations is proposed. In this way the internal market profits, and it eases cross border operations by businesses.

5. CASE STUDY RESULTS

In the Netherlands, there is no concern from the Data Protection Authority (DPA) about the use of images of a property. Only if the data use has consequences for a natural person, for example taxation, it is considered personal data. This is a result of research in 2001 by the Dutch DPA on the use of panoramic 360 degrees images of public roads in a database (CBP, 2001). Google Street View images are considered personal data according to the Dutch DPA, because they can be used to identify natural persons and they can have consequences for the data subject, and it should be processed according to the Dutch data protection act. Regarding Google Earth, one court ruled that nowadays, the use of Google Earth cannot be seen as an exceptional technical tool, because it is available for anyone with an internet connection. The court ruled that only a limited infringement has been made on the privacy, and based on the police law there was a legitimate reason to use Google Earth (Rechtspraak, 2011).

In another case, the court ruled that the display of the address and the images on an Internet site are not personal data, because they lack information about the inhabitant. Since Google also does not facilitate possibilities to link this information to the inhabitant, the Court ruled that the name of the street and house number is only a location of a property and not address data. Address data would mean the data would be considered personal data (Rechtspraak, 2013).

In Belgium, Google Street View was discussed in the Senate. The Belgium DPA considers photos of an asset personal data. So pictures of a home are considered personal data. The Belgium DPA requires a specified and explicit purpose description for Street View, and also different levels of data protection for different purposes and datasets. The Belgian DPA makes a distinction between maps without persons or cars, and maps with natural persons and objects.

In Germany, the DPA (Datenschutz) judges that photos taken of a home cannot be prevented, and with use of Internet different datasets can be linked together and this can lead to identification of an inhabitant (BR-Drs, 2010). However, Google Street View interferes with the right to privacy, when it processes photos of houses that have a fence, and not directly visible from the street (KG Berlin, 2010). Such photos of objects behind a fence are considered personal data. The German Federal Court judged that a spatial object could reflect someone's personality (BVerf, 2006).

The DPA of the German state Schlewig Holstein is opposed to Street View in the State, because it invades the right to privacy of the inhabitants (Datenschutzzentrum, 2008; see also Datenschutz Baden-Württemberg, 1999, p.138). Google Street View is disseminated via Internet and shows the state of the buildings.

The German courts state that when automatic linking between object and natural person is not possible there is no interference with the right to privacy and personal data protection (LG Waldshut-Tiengen, 1999; VG Karlsruhe, 2000; KG Berlin, 2010; BVerfG, 2006; BVerfG, 2006a). The courts state that when it is possible to automatically link geographic data to other data sources, the geographic data may become personal data and is an interference with the right to privacy and personal data protection.

The United Kingdom DPA states that data in Google Street View is not considered personal data, because "Data protection is about people's personal information; so an image of a house held on Street View is not a data protection matter" (ICO, 2009).

	Personal Data?	Argumentation
Netherlands		
Legislator	No	The processing of Google Street View images are not considered personal data when a person's face and license plate of a car is blurred
Data Protection Authority	Yes	If the images, are used in the context of identifying, or the images have societal consequences for a person the images are considered personal data.
Jurisprudence	Street View No	If images of a home are blurred and the images lack a link between the inhabitant and the property
	Google Earth: No	The images are available to everyone, only a limited infringement of right to privacy.
Belgium		
Legislator	No	Digital images of a house are not mentioned. Only faces and licence plates.
Data Protection Authority	Street View: Yes	An image of a house could lead to identification.
	Aerial Images: Yes	The images show parcels (all information) belonging to (concerning) to a natural person, the urban planning division is able to identify the owners of the building (identified or identifiable).
Jurisprudence	Not	Not available

	available	
Germany		
Legislator	No	The data subject has the right to blur face, body and house. Otherwise considered personal data.
Data Protection Authority	Street View Yes	Picture of a home is considered personal data. It can be used for economic value assessment, and possibly theft.
	Satellite images: Yes	With a higher resolution than 40cm per pixel satellite images are considered personal data, based on the jurisprudence
Jurisprudence	Street View No	Images of homes are not personal data, because it is not possible to lead to identification.
	Aerial images Yes	Aerial images of a home are an invasion of privacy, because it shows a characteristic of a person. It shows more than a view from the public road.
United Kingdom		
Legislator	Not mentioned	
Data Protection Authority	No	Data protection is about people's personal information; so an image of a house held on Street View is not a data protection matter
Jurisprudence	Not Available	Not available

Table 2 Overview of the perspectives on mobile mapping data in EU Member States

Three of four case studies consider the Google Street View images personal data and aerial images are also personal data. The UK DPA is the only DPA that despite complaints of citizens does not see Google Street View as personal data. With this statement the ICO claims that it is not possible to use the images from Google Street View to identify a person. Between the EU Member States the reasoning regarding the panorama pictures of streets differ. The DPA in the Netherlands has a focus on the context of the collection, if the purpose is to identify a person, or it has societal consequences this is considered personal data. In Belgium, the possibility to identify a natural person is dominant in the reasoning and in Germany the possible consequences for an inhabitant are one of the reasons for considering the image of a home as personal data.

In the United Kingdom these reasons do not apply. The UK DPA (ICO) uses information on a house as an example to explain the definition of personal data: "Context is important here. Information about a house is often linked to an owner or resident and consequently the data about the house will be personal data about that individual. However, data about a house will not, by itself, be personal data (ICO, 2012, p.12)." So the data about the house is not personal data when it is about the house and not linked to a person. The context of the processing and the goal of the processing is of importance according to the UK DPA. This use of the personal data definition is in line with the more narrow definition by the European Court of Justice, for example when an analysis contains personal data the analysis itself is not considered personal data, but only the personal data. The UK DPA states that when data is about an individual, for example, the address of the individual or when the data is used in decisions or deliberations affecting the individual, for example data on the electricity bill of an individual it is considered personal data (ICO, 2012).

Within each EU Member State there are also differences among between different institutions. In the Netherlands and Germany the *courts* claimed that Google Street View does not constitute an invasion of the right to privacy. While the Dutch and German *DPAs* state that Google Street View contains personal data. Also the difference between Street View and Google Earth is remarkable, because the Dutch court ruled that the use of Google Earth for the tracking of crimes was an –allowed- interference with the right to privacy.

5.1 INSPIRE data

Also for INSPIRE data we found differences among the case countries. In the Netherlands, the Data Protection Authority judged that the use of some INSPIRE themes led to implications for the personal data protection, because it was possible to link data to other datasets which resulted in the identification of a natural person. The Dutch DPA has the same opinion as the Dutch legislator on the absence of personal data in topographic maps. The Register of Addresses and Building may contain personal data when data in the register is linked to other datasets.

The Belgian DPA advised the Flemish government about the implementation of the INSPIRE Directive and the opening up of INSPIRE data, the DPA has given a negative advice on both (CBPL Advies 32, 2008; CBPL Advies 40, 2006), but the Flemish government still published the data.

In Germany, the DPA argues that at a mapping scale larger than, i.e. more detailed than, 1:10.000, the data should be considered personal data because at these scales it is possible to trace the use of the land, state of buildings and possible identify natural persons (Bundestag 16, 2008; Karg, 2008).

The German and Belgian authorities differ on the use of a privacy safe scale. The Netherlands decided that topographic information did not contain personal data. This is an interesting judgement, because when linking it, it could lead to identification and the topographic maps that are freely disseminated show information about the use and state of land. The differences inside and between the Member States focus on the identifiable part of the personal data definition. The Member States differ on the opinion in what way topographic maps tell something about a person and should be considered personal data.

6. HARMONISING THE PATCHWORK OF DATA PROTECTION

The definition of personal data has sparked some discussion in the literature. It is mentioned that the definition of personal data is broad that has tendency to extend with the development of technological possibilities to identify natural persons. The concept of Personally Identifiable Information (PII) 2.0 may overcome some of the issues of the current definition. Schwartz and Solove define personal data as Personally Identifiable Information (PII) and created a model with what they call PII 2.0. The model makes a distinction between identified, identifiable and non-identifiable information (Schwartz and Solove, 2011). Data is placed on a continuum on one end there is no risk of identification and on the other end it concerns identified natural persons. The three features of the model are (Schwartz and Solove, 2011).

1. Identified: An identified natural person is a person whose identity is determined. This data has a high risk level.
2. Identifiable: There is an immediate chance on identification of a natural person. This data has a moderate to low risk level.
3. Non-identifiable: Data with only a remote risk of identification. With means reasonable likely to be used for identification this data cannot be related to a natural person.

Sometimes identifiable data should be considered identified data, this is the case when the data processor is able to link data and with this link identify a natural person. Schwartz and Solove (2011) advise to develop an assessment for this category of data. This assessment should take the lifetime of the stored information and development of relevant technology in consideration. The assessment is also mentioned by the EDPS, the rules for the assessment should be defined in the Draft Regulation (EDPS, 2012). A possible solution is the traffic light model as proposed by Karg (2008, p55 and further) providing four categories of personal data, each with a different colour. The traffic light is composed of the colours/ categories:

Red: Sensitive data as defined in Directive 95/46/EC, article 8: "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 data is prohibited from dissemination on the Internet.

Orange: Personal data (identified). This is a definition partly based on Directive 95/46/EC: "'personal data 'shall mean any information relating to an identified natural person ('data subject') (European Commission, 1995, article 2a). This definition focuses on an identified person. The data needs to identify the person directly. Examples are your name, or social security number.

Yellow: Personal data (identifiable). Data that can possibly lead to identification (IP-addresses, building data, address). This data refers to identifiable natural persons, persons that are indirectly identifiable, for example through combining several datasets. For this type of data it is important to create a risk assessment. For example, to consider the context of the processing, and with that context in mind give a go to the dissemination or prohibit access to the data.

Green: No personal data. This data is not subject to the data protection rules. This may be factual data with no reference to a person or publicly available data with no influence or very limited influence on a person's privacy (Karg, 2008, p.55).

The traffic light model gives indications for the risk to identify natural persons. However, it does not have strict boundaries of personal data. This model is more focused on the context of processing instead of a strict divide between personal data or non-personal data. Although the model is simple and intuitive, we believe that it can be a valuable start for a discussion of normalisation of the complex concept of personal data as applied to geographic data.

7. CONCLUSION

Concluding, to construct personal data protection in the European Union it is important to tackle the problems with the differences in definition on what is considered personal data. Some geographic data is considered personal data in the Netherlands, Germany and Belgium, and it is not considered personal data in the United Kingdom. The perspectives of different stakeholders in the Member States also differ, leading to new difficulties in harmonization. With use of the personal data definition in the current Directive 95/46/EC and the Draft General Data Protection Regulation, some types of geographic data should be considered personal data in the EU context, because it is data that could lead or contribute to the identification of a person.

The analysis shows that opening up of geographic data and the interpretation of personal data protection legislation is still a blind spot for legislators in Europe. 360 degree images, and aerial images are considered personal data by the national Data Protection Authorities in the Netherlands, Germany and Belgium, because these images could lead to identification of individuals. This possible violation of the personal data protection legislation is not discussed in the Parliaments of these EU Member States. The Data Protection Authorities have a clearer view on the application of the data protection legislation on geographic data, but these views differ. Data Protection Authorities consider some geographic data personal data.

Interpretation in jurisprudence also differs from the other perspectives (legislator and DPAs), and the between courts in Member States. In the jurisprudence there are often references to general privacy legislation, but not so much to the specific personal data legislation, and some cases have a very specific context, for example using Google Street View in law enforcement.

The introduction of a traffic light model for personal data (see Karg, 2008) may result in a clearer view on the applicability of personal data protection legislation to geographic data. With geographic data the context of the processing stays important. If the geographic data can be linked to a natural person and it is possible to get an insight in the state of a building or yard, it may be considered personal data. But other types of geographic data, for example factual data that does not reveal sensitive information about a person, is less personal data and may be disseminated with less restrictions than normal personal data. This gives room to opening up data under the INSPIRE Directive and the PSI Directive.

The Draft General Data Protection Regulation could implement the traffic light model and should then contain clear rules on the risk assessment to harmonise the different interpretation between and inside EU Member States.

8. REFLECTION

This research aims at providing suggestions for harmonizing the data protection legislation in the different EU Member States. This harmonization should create opportunities for businesses operating in the internal market. The cultural aspect of personal data protection in the different countries should be studied in more depth, because data protection legislation and opinions on personal data protection shift from strict to less strict in different times and different cultures. This research did not address the cultural aspect.

Because the opening up of geographic data is a recent topic, there has not been very much jurisprudence on the subject. When there is more case law and more political attention towards this topic of opening up geographic data and the interpretation of data protection legislation this could result in a more extensive research results. We highly encourage the extension of this research given the manifold nuances of what is considered personal geographic data in the European Union.

The research was conducted through a literature study on four case-studies. This has some advantages, like it is an opportunity to study several parts of the European Union consistently, and it gives some interesting and useful examples to compare. But more interviews with different stakeholders on the subject would give a better insight into the motivation and future processes and the role of technology for example in linking of data.

ACKNOWLEDGEMENTS

The presented research was performed as part of the MSc. thesis project of the MSc. program Geographical Information Management and Applications (GIMA).

REFERENCES

BR-Drs (2010). Gesetzesantrag der Freien und Hansestadt Hamburg Entwurf eines Gesetzes zur Änderung des Bundesdatenschutz-gesetzes. Drucksache 259/10. 24-04-2010.

BVerfG (2006). BVerfG, Urteil des Zweiten Senats vom 02. März 2006 - 2 BvR 2099/04 - Rn. (1-142).

BVerfG (2006a). Beschluss der 1. Kammer des Ersten Senats vom 02. Mai 2006,- 1 BvR 507/01 - Rn. (1-24).

Cate, F.H. (1995). The EU Data Protection Directive, Information Privacy, and the Public Interest. *Iowa Law Review*, 431, pp. 431-443.

CBP (2001). Digitale beelden van openbare omgeving vallen soms onder privacywetgeving.

CBPL Advies 40 (2006). Bijhouden van gemeentelijke registers van onbebouwde percelen waarvan sprake in artikel 62 van het Vlaams Decreet van 18 mei 1999 houdende de organisatie van de ruimtelijke ordening en hun bekendmaking op het Internet via het toekomstige geoloket. SA2 / A / 2006 / 030.

CBPL Advies 32 (2008). Advies inzake het voorontwerp van decreet betreffende de Geografische Data-Infrastructuur Vlaanderen. A/2008/032.

Cuijpers, C., P. Marcelis (2012). Oprekking van het concept persoonsgegevens beperking van privacybescherming? *Computerrecht*, 6, pp. 397-409.

Datenschutzzentrum (2008). Keine Straßenerfassung in Schleswig-Holstein ULD hält Google Street View für rechtswidrig. 01-10-2008.

Datenschutz Baden-Württemberg (1999). Zwanzigster Tätigkeitsbericht des Landesbeauftragten für den Datenschutz in Baden-Württemberg, p.138).

EDPS (2012). Opinion of the European Data Protection Supervisor on the 'Open-Data Package' of the European Commission including a Proposal for a Directive amending Directive 2003/98/EC on re-use of public sector information (PSI), a Communication on Open Data and Commission Decision 2011/833/EU on the reuse of Commission documents. Pp. 1-13.

European Commission (2011a). Results of the online consultation of stakeholders "Review of the PSI Directive".

European Commission (2012). Reform of data protection legislation.

European Commission (2012a). COMMISSION STAFF WORKING PAPER Impact Assessment. SEC(2012) 72 final.

European Commission (2014). The EU Single market. An historical overview.

European Union (1995). 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. Official Journal L 281, pp.31-50.

European Parliament (2014). European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

Focus Magazin (2009). "Street-View-Start noch dieses Jahr". 27th of April 2009, p. 20.

Fornefeld, M., G. Boele-keimer, S. Recher and M. Fanning (2008). Assessment of the Reuse of Public Sector Information (PSI) in the Geographical information, Meteorological Information and Legal Information Sectors. Dusseldorf: MICUS Management Consulting GmbH.

Fromholz, J.M. (2000). The European Union Data Privacy Directive. *Berkely Technology Law Journal,* 15, pp.461-484.

ICO, (2009). Common sense on Street View must prevail, says the ICO. Press Release via the national Archives online.

ICO (2012). Determining what information is 'data' for the purposes of the DPA. Version: 1.1, 12-12-2012.

INSPIRE themes (2014). Data specifications.

KG Berlin (2010). Google Street View. KG Berlin, Beschluss v. 25.10.2010, Az. 10 W 127/10

Korff, D. (2002). EC study on implementation of data protection directive comparative summary of national laws. Human Rights Centre, University of Essex, Colchester.

Korff. D. (2010). Data protection laws in the EU: The difficulties in meeting the challenges posed by global social and technical developments, study commissioned by the European Commission. Working Paper No.2.

LG Waldshut-Tiengen. Erfassung und Verbreitung digitaler Gebäudeabbildungen. MMR 2000, 172, 175.

Loenen, B. van, J.A. Zevenbergen, and J. de Jong (2008). Geo-informatie: wat is het en wat is de juridische context? In L van Wees & S Nouwt (Eds.), Recht en locatie; geo-informatie in een juridische context (pp. 11-33). Den Haag: Elsevier Juridisch (Reed Business bv).

Loenen, B. van and Y. Verdonk (2011). Open Data: van ideaal tot realiteit. NCG 55, pp. 1-33.

Newman, A.L. (2008). Building Transnational Civil Liberties: Trans governmental Entrepreneurs and the European Data Privacy Directive. *International Organization*, 62, pp. 103-130.

Open Data Index (2015). Global Open Data Index.

Privacy International (2007). National Privacy Ranking 2007.

Rechtspraak (2013). Gerechtshof Amsterdam, Vordering tot gebod verwijdering persoonsgegevens van websites Google Maps en/of Google Street View. In hoeverre zijn gegevens Google Maps persoonsgegevens in zin van Wbp?. Zaaknummer 200.105.659.

Rechtspraak (2011). Rechtbank ’s-Gravenhage, Medeplegen van valsheid in geschrifte en (al dan niet mede) plegen van fiscale delicten. Zaaknummer 09/997127-09.

VG Karlsruhe (2000). Elektronische Häuser- und Gebäudekarte. MMR 2000, 181.

van der Sloot, B. (2011). De wegen van Google zijn ondoorgrondelijk: over Street View en dataprotectie. *Privacy & Informatie*, 14(4), 176-190.