European Public Sector Information Platform

Topic Report No. 2011 / 3

Open government data: reconciling PSI re-use rights and privacy concerns

Author: Hans Graux

Published: October 2011

Keywords

Open Government Data, PSI Directive, Data Protection Directive, privacy

Abstract

European Open Government Data (OGD) initiatives are frequently forced to balance uncomfortably between two legitimate but occasionally conflicting policy spheres. On the one hand, there are Public Sector Information (PSI) regulations, which aim to enable and encourage the re-use of existing documents held by public sector bodies. This leads to openness, stimulates government transparency, and creates new economic opportunities. On the other hand, data protection regulations aim to create a certain measure of privacy protection over personal data, by determining the circumstances under which personal data can be processed. When PSI consists partially of personal data, tensions between the two policy spheres inevitably occur. This topic report examines how the principal European regulations relate to each other, and describes a few real-life cases of conflicts and how they were addressed.

Table of contents

Abstract

European Open Government Data (OGD) initiatives are frequently forced to balance uncomfortably between two legitimate but occasionally conflicting policy spheres. On the one hand, there are Public Sector Information (PSI) regulations, which aim to enable and encourage the re-use of existing documents held by public sector bodies. This leads to openness, stimulates government transparency, and creates new economic opportunities. On the other hand, data protection regulations aim to create a certain measure of privacy protection over personal data, by determining the circumstances under which personal data can be processed. When PSI consists partially of personal data, tensions between the two policy spheres inevitably occur. This topic report examines how the principal European regulations relate to each other, and describes a few real-life cases of conflicts and how they were addressed.

Content

This topic report examines how the PSI Directive and the Data Protection Directive relate to each other, and describes a few real-life cases of conflicts and how they were addressed.

1 The openness of government data: two policy perspectives

1.1 The tension between the PSI Directive and the Data Protection Directive

The term Open Government Data (OGD) is generally used to refer to the principle or objective that information produced or commissioned by government or government controlled entities should be made available for free use, re-use and redistribution by anyone[1]. In EU policy initiatives, this objective as such has no clear legal basis, in the sense that there is no generic obligation to make all government data available for free re-use. Rather, the PSI Directive[2] tackles this issue from a different perspective: it regulates the obligations of public sector bodies in the Member States when they decide to allow for re-use of their data, and provides corresponding rights to re-users. However, it does not define a general 'right to re-use' as such.

None the less, the PSI Directive certainly aims to stimulate the internal market by encouraging the development of services that can build on the information held by European public sector bodies[3], and presents the publication of generally available public

[1] See e.g. http://opengovernmentdata.org/what/, http://data.gov.uk/about, and http://gov.opendata.at/site/history

[2] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, Official Journal of the European Union L 345, 31/12/2003 P.90-96.

[3] See Recitals (1)-(5), (15) and (25) of the PSI Directive

sector information as a "fundamental instrument for extending the right to knowledge, which is a basic principle of democracy"[4]. Clearly, the PSI Directive builds on the principle that there are clear benefits to be reaped from PSI availability and re-use.

The data to which the PSI Directive applies is defined in Article 2.3 as "(a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audio-visual recording), or (b) any part of such content".[5] This is obviously a broad description that may cover "a wide range of information in many areas of activity, such as social, economic, geographical, weather, tourist, business, patent and educational information"[6]. Because of the wide net that is cast by the PSI Directive, its scope of application may overlap with a separate key legislation: the Data Protection Directive[7].

The Data Protection Directive aims to protect the fundamental right to privacy of natural persons with respect to the processing of their personal data[8]. It strives to reach this goal by creating a common legal framework that determines the conditions under which personal data can be processed. As with the PSI Directive, the basic building block of the Data Protection Directive has been given a broad definition: personal data is defined in Article 2 (a) of the Data Protection Directive 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". The recitals to the Data Protection Directive clarify that in order "to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person"[9]. Generally, whenever information can be reasonably linked to a specific individual, it is likely to be qualified as personal data.

It is clear that much of the information targeted by the PSI Directive will also constitute personal data, and it will therefore also be subject to the specific restrictions of the Data Protection Directive. This creates an immediate tension: one Directive aims to favour openness and re-use, whereas the other emphasizes the importance of privacy protection rules. How do these frameworks relate to each other, and how can public sector bodies ensure that they comply with both?

---

[4] See Recital (16) of the PSI Directive

[5] Excluding a number of categories of data, such as documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies; documents for which third parties hold intellectual property rights,; documents which are excluded from access by virtue of the access regimes in the Member States; documents held by public service broadcasters, education and research establishments or cultural establishments.

[6] See Recital (4) of the PSI Directive

[7] 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 , 23/11/1995 P. 0031 – 0050

[8] Article 1 of the Data Protection Directive

[9] See Recital (26) of the PSI Directive

1.2 The primacy of fundamental rights

The relationship between both frameworks is partially resolved by the PSI Directive itself. It contains a number of direct acknowledgements of the importance of data protection, and indeed references the Data Protection Directive directly. Specifically:

- Recital (21) of the PSI Directive notes that: "This Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with 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 of the free movement of such data."

- Article 1 (4) of the PSI Directive confirms that: "This Directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Community and national law, and in particular does not alter the obligations and rights set out in Directive 95/46/EC."

- Article 2 (5) finally emphasizes, for the avoidance of doubt, that the PSI Directive applies the same definition of personal data as the Data Protection Directive.

The result is fairly clear and unambiguous, at least in theory: when re-using personal data covered by the PSI Directive, the Data Protection Directive must be adhered to at all times. Thus, any entities processing personal data in the course of re-use (including the public sector bodies that produce or collect the data and make it available, service providers that re-use the data to provide services, and any consumers that access or use the data through these services) will need to ensure they comply with the provisions of the Data Protection Directive[10].

This principle appears to be relatively simple, especially in cases where the data being re-used can be unambiguously classified as personal data (e.g. identity information, health or tax records, information on social status, etc.). However, complexities can easily arise. In some cases, this can simply be the result of the national implementation of the Directives. In Belgium for instance, the federal law governing the re-use of public sector information stipulates[11] that public sector information which contains personal data may only be made available for re-use if the public sector body has first taken the necessary precautions to conceal the identity of any persons who may be implicated in the information, specifically by anonymising the data in accordance with the rules of a specific Royal Decree. This very strict approach essentially eliminates any overlap between the PSI sphere and the data

[10] This position was also affirmed by the Article 29 Working Party, which acts as an independent European advisory body on data protection issues, in its 2003 Opinion on the re-use of public sector information and the protection of personal data; Opinion 7/2003, WP 83 of Article 29 Working Party, adopted on 12 December 2003

[11] Article 4 of the Law of 7 March 2007 transposing the PSI Directive (Wet tot omzetting van de richtlijn 2003/98/EG van het Europees Parlement en de Raad van 17 november 2003 inzake het hergebruik van overheidsinformatie | Loi transposant la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public)

protection sphere: as long as data protection laws apply, re-use is not permitted.

But even in the absence of laws that exceed the requirements of the European legal framework, the simple principle of observing data protection rules when re-using data can present serious challenges. This is mainly the result of the broad interpretation given to the concept of personal data, which means that data protection rules will apply in many more cases than the simple examples mentioned above, including in cases where public sector bodies or re-users might not intuitively recognize a privacy risk. In the sections below, we will examine a few real life cases where re-use initiatives were met with privacy challenges, and look at how they were resolved.

2 A practical perspective: data protection challenges in real life PSI cases

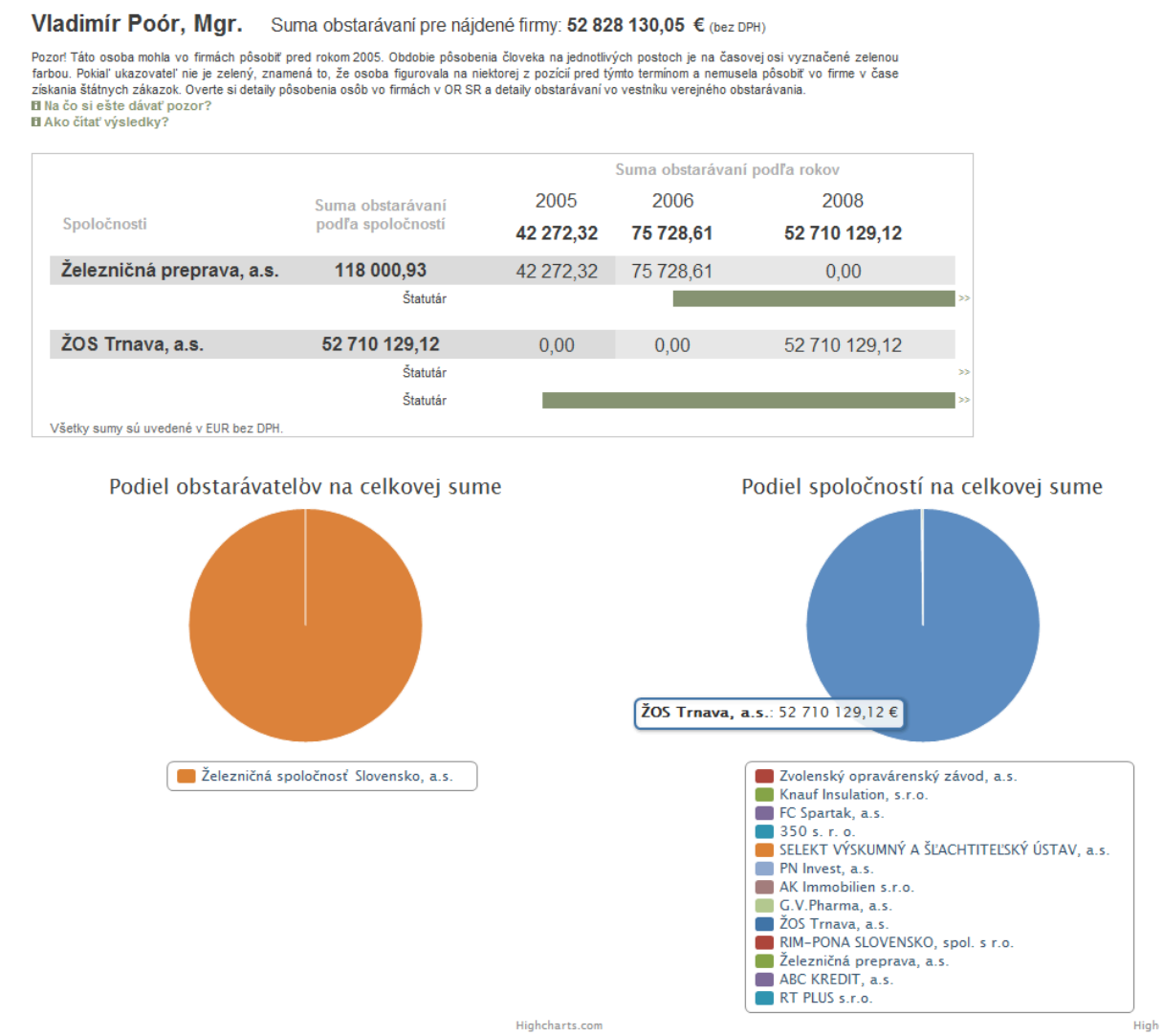
2.1 Fair-Play Alliance: combining publicly available personal data and publishing the result can be unlawful

A recent example of privacy rights colliding with a PSI initiative occurred in Slovakia, and involved an award winning application created by the Fair-Play Alliance, a Slovakian NGO with a stated mission of pushing for ethical, transparent, professional and effective public administration and political representation[12]. One of its initiatives was the Znasichdani.sk site, which offered a simple yet compelling service to the public: by entering a specific individual's name, the site would create a quick overview of any public procurements won by an entity in which that individual has a leading role, along with the amounts awarded to these entities. The name Znasichdani.sk is derived from the Slovak 'z našich daní', meaning 'from our taxes'.

Fair-Play argued that this would be a useful tool to detect potential corruption, since it would allow site users to determine how often an individual citizen was successful in procurements, irrespective of the company they were using to participate in a bid. This could allow investigators to determine cases where an individual could be said to be unusually (or possibly even suspiciously) successful in public procurement contracts.

The application was relatively simple from a technical perspective, as it relied on two already public databases: on the one hand a database of public procurement contracts (the Bulletin of Public Tenders) that indicated which entities had won specific bids, and on the other hand a company register (the Business Register of the Slovak Republic) that indicated which individuals had controlling roles in specific entities. Thus, an individual's name could be linked to any number of relevant companies, which in turn could be linked to awarded procurements. The result was a nice visual overview of the public funds (including specific amounts) which flowed to any companies that the individual was involved in:

[12] See http://www.fair-play.sk/index_en.php



Results of a sample search, using an example published on EPSIplatform.eu[13]

The application was generally well received, and won first prize at the June 2011 Open Data Challenge during the Digital Agenda Assembly in Brussels.

From a privacy perspective, the application might at first seem innocent enough. After all, it does not publish information that cannot also be found by searching the two source databases, which are already (and presumably legitimately) publicly accessible. Thus, no new information is created by the application; it merely facilitates the collection and analysis process.

None the less, the application raises certain data protection concerns. It is clear beyond discussion that the information provided by the application is personal data as defined in the Data Protection Directive, as it allows the identification of a specific individual. Indeed,

[13] http://epsiplatform.eu/news/news/open_data_challenge_winner_ordered_to_remove_certain_data.

the primary function of the application is precisely to allow users to obtain information relating to specific individuals. As a result, the rules of the Data Protection Directive apply to the application. This raises several questions.

One of the key principles of the Data Protection Directive is the purpose restriction: personal data may only be collected for specified, explicit and legitimate purposes, and it may not be further processed in a way incompatible with those purposes (Article 6.1(b) of the Data Protection Directive). The Znasichdani.sk application processes personal data by retrieving information from two source databases, and combining it into an overview that creates a clear added value. However, one might question whether obtaining personal data from these sources and re-using it for the purposes of publishing the results of public procurements is compatible with the purpose restriction.

This depends largely on the purpose for which personal data in the original sources is made available. If, for instance, data in the Companies Register is made available only for the purposes of allowing third parties to determine if company decisions were lawfully made (e.g. whether a contract was indeed signed by an authorised representative of a company), then using this information for entirely different purposes (e.g. to provide indications of possible wrongdoings such as violations of Slovak procurement laws or anti-corruption laws) could be a violation of the purpose restriction rule.

Of course, in this case the possible violation depends on the stated purpose of the Companies Register in the Slovak Republic, and on the stated purpose of Znasichdani.sk. On the latter purpose, the website indicates that "Znasichdani.sk is based on the assumption that if people get access to this kind of detailed information, management of public money in Slovakia will become more transparent. Procurement of overpriced goods and services will get a new dimension if citizens are able to connect the benefits from these procurements with specific names and faces."[14] Thus, Znasichdani.sk is declared to primarily be a tool for improving procurement transparency. Provided that this is compatible with the purpose for which information in the Companies Register is made available, the purpose restriction rule should not present any problems.

The legitimacy of the Znasichdani.sk site was called into question in a recent case, where a specific individual obtained an injunction from a court in Bratislava, ordering her name and the link to any procurement values relating to her to be censored from the search results[15]. While the arguments presented in the case and the reasoning of the judge are not yet available, the order provided by the court – namely the blurring of the individual's name in order to make the results unlinkable to her – strongly suggest that the issue was driven by data protection concerns.

The outcome is rather bizarre: not only does the order only apply to this specific applicant – thus leaving the information of any other Slovak citizen available for searching – but even searching for the applicant's name and obtaining the relevant results is still possible. Only

[14] See http://znasichdani.sk/info

[15] http://spectator.sme.sk/articles/view/43180/2/court_orders_removal_of_public_procurement_data.html

the presentation of the results has changed, with some information being blurred in the overview of procurements. Perhaps more importantly, the proceedings have done the applicant very little favours with respect to her privacy, as the case – including her name and employment details – have now been widely published.

The decision of the court in Bratislava has been appealed, and should additionally be followed by a full hearing on the merits of the case. Hopefully, this will clarify the reasoning behind the dispute, and clear up the legitimacy of the Znasichdani.sk platform. Meanwhile, PSI application developers will need to carefully consider whether their intended re-use of personal data is compatible with the intended purpose of its publication.

2.2 Crime maps in the UK: a detailed map may breach data protection laws

In the Slovak example above, the applicability of data protection laws was a fairly clear matter, since the information related directly to an identified natural person. However, the scope of data protection laws can also extend to other types of data, in which the link to a natural person may not be as immediately clear.

Maps are an interesting case in point. Intrinsically, a map only needs to provide certain geographic information allowing it to be linked to a specific location. Simple maps that contain only information on a landscape will have no clear link to natural persons, and will therefore not fall within the scope of data protection law. However, this situation changes when information is added to the map. Adding the outlines of houses already provides information on the persons who live there. Satellite imagery will enhance the picture by showing the type of dwelling, as well as flagging who in your neighbourhood owns outdoor swimming pools, saunas and extensive terraces. Adding real estate values will provide a decent indicator of the income category or of the assets of the inhabitants. The more detailed and fine grained the information becomes, the more likely it is that a map is qualified as personal data. After all, a map containing all of the information above will certainly provide information on natural persons, namely the socio-economic status of individuals who can be identified simply by visiting the location. Thus, any sufficiently detailed map is bound to eventually cross the line into personal data.

This issue can also be highly relevant in the PSI sector, where geographic information can be linked with other data sources to provide useful information on the characteristics of a region, city, neighbourhood or street. An interesting example is the crime maps that have been published recently in the UK, driven in part by the UK's open data policies[16]. A multitude of such applications exist[17], including the national crime mapping website, Police.uk[18], and UKCrimeStats[19]. The latter application provides access to crime statistics at the national level, but also for specific neighbourhoods and streets, based on official police

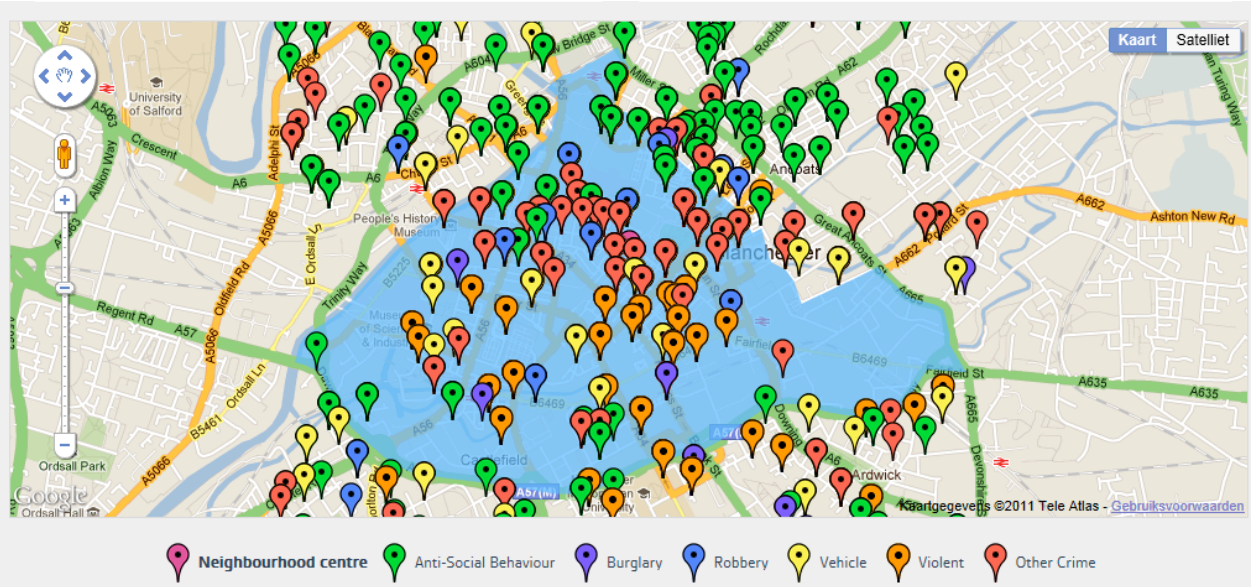
[16] See http://data.gov.uk/

[17] See the list at http://data.gov.uk/apps, specifically in the 'crime' subcategory (http://data.gov.uk/search/apachesolr_search/?filters=tid%3A245 type%3Aapps&retain-filters=1)

[18] See http://www.police.uk/

[19] See http://www.ukcrimestats.com

reports. It breaks the crimes up into several categories (including anti-social behaviour, burglary, robbery, vehicle crime, violent crime, and others[20]), and links these incidents to the specific locations where they occurred via easily searchable maps.



Crime in Manchester – primarily anti-social behaviour outside the city centre; mainly violent crime and other crimes within

Undoubtedly, such maps are useful tools for anyone looking for a new residence, allowing them to get a first impression of crime prevalence. Equally importantly, it allows existing residents to assess how much crime objectively occurs (or more accurately, how much crime is reported) in their neighbourhood, rather than having to rely on impressions[21].

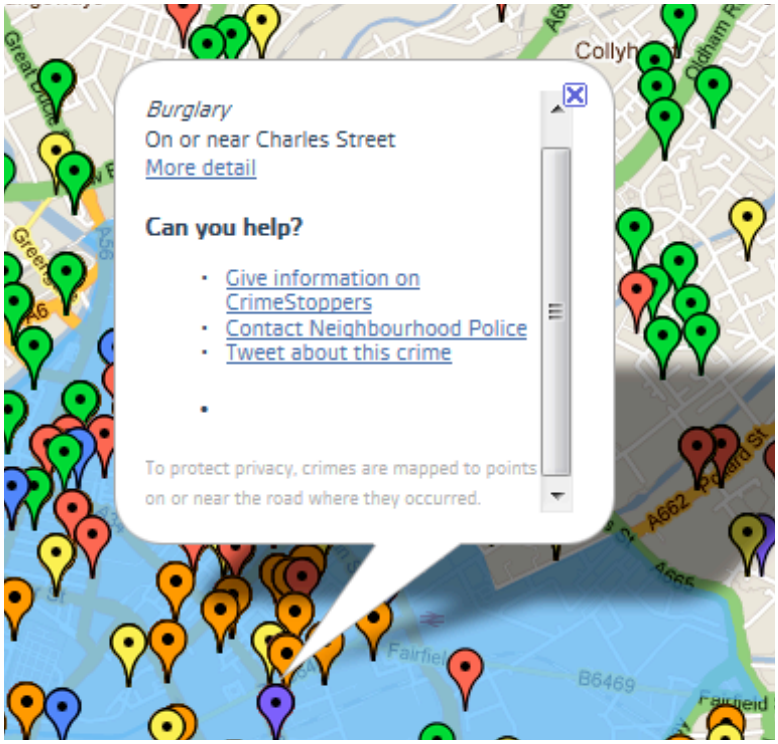
None the less, there is also a clear privacy risk. Conceptually, it is perfectly possible to pinpoint each crime to a precise address. However, this approach meets with serious problems. Firstly, the location of a crime is of course not always an indicator of who committed it: a violent crime being committed at a specific address does not suggest that the inhabitant of that address was the perpetrator. Indeed, he or she may instead be the victim, or the incident may simply have occurred on their doorstep. None the less, there is a real risk that observers of this data might draw the wrong conclusions, possibly led by their own presumptions or biases about the inhabitants. Clearly, this would not be a desirable outcome.

From a data protection perspective, the main question is whether the provided information can be qualified as personal data. According to the definition of the Data Protection Directive, this is the case when the information relates to an identified or identifiable natural person. Even indirect identification can meet this definition: while real estate value only relates directly to an object (the property itself), it can also relate indirectly to a

[20] The latter including sex offences, which are not identified separately as a privacy enhancing measure. See http://www.guardian.co.uk/uk/2011/feb/01/online-crime-maps-power-hands-people
[21] For an overview of applications, see http://www.bbc.co.uk/truthaboutcrime/crimemap/

natural person (namely when a natural person lives there)[22]. The same also applies to crime information linked to a specific location: even if the information does not necessarily identify a person as a perpetrator, victim, observer, or simply a person who lives near the incident, it can certainly relate to them on one of those points. For this reason, crime information attached to sufficiently detailed maps can be considered personal data, meaning that all of the requirements of the Data Protection Directive must be met. This can be particularly burdensome for PSI application providers in this sphere, since the requirements for processing sensitive personal data (namely crime data) can be very stringent.

Of course, these observations only apply if the crime information can be linked to a natural person, either because the details of the report include such a link, or because of the geographical inference mentioned above. If the report only mentions the type of incident (without details of personal involvement) and has no clear link to a specific location, then the information doesn't relate to a natural person and will not be considered as personal data. Indeed, when clicking on a 'crime pin' on the UKCrimeStats map shown above, the following pop-up appears:



No details on the crime or its exact location

The information provided via the UKCrimeStats application does not provide details on who was involved in the burglary (as a perpetrator, victim or observer), nor does it indicate the precise location. It only states that it occurred 'on or near Charles Street', and stresses that "crimes are mapped to points on or near the road where they occurred", as a privacy

[22] The example is also referred to in the Article 29 Working Party's 2007 Opinion on the concept of personal data; Opinion 4/2007, WP 136 of Article 29 Working Party, adopted on 20 June 2007.

protecting measure. The result is that the information does not relate to an identified or identifiable natural person, and thus no longer qualifies as personal data. In effect, it has been anonymised to eliminate the privacy risk (and the applicability of data protection law) without unduly harming the usefulness of the application.

This solution seems ideal, but can be difficult to apply in practice. The information maps are automatically generated by linking maps to crime reports, an approach which doesn't necessarily take into account population density. In the City of Manchester, stating that a crime occurred on or near a specific street provides no real link to an identifiable person. However, in a very sparsely populated region where perhaps only a few residents live in a radius of several kilometres, even such generalized information can provide clear indications of a person's relation to a crime. If this problem is not addressed, the information will still need to be qualified as personal data and processed in accordance with data protection laws.

For this reason, the UK Information Commissioner (ICO), who monitors compliance with data protection laws in the UK, has issued specific guidelines[23] on crime maps and data protection compliance. The ICO noted that relevant factors for assessing compliance would include:

- the granularity of the crime-map,
- the regularity of data uploads,
- the sensitivity of the crime,
- the information recorded on the map, and
- the availability of other sources of information.

The guidelines require those who publish crime maps to implement appropriate procedures to address the concerns of victims of crime who fear that the maps reveal their identity, or the objections of house owners whose property value diminishes as a result of incorrectly attributed data. The ICO also explicitly warns against any practices that would allow a specific household to be linked to a particular crime, noting that this would likely constitute an unfair processing of personal data. Thus, the recommendation is to clearly avoid making the information needlessly specific.

Of course, this approach is not too surprising, and is indeed in line with general data protection principles, and mainly the principle of data minimisation: the processed personal data should be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed" (Article 6.1(c) of the Data Protection Directive). In terms of PSI, this implies refraining from the use of personal data (i.e. avoiding links to identifiable natural persons) whenever possible for the purposes of the re-use, and limiting the use of personal data to the maximum extent possible in all other cases. This approach will undoubtedly become more and more important as open data

[23] Crime-mapping, privacy and transparency: advice from the Information Commissioner's Office, published on 24 November 2010; see http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/crime_mapping_advice.ashx

applications spread to other sectors with comparable data protection concerns, including health, education, justice and transportation[24].

[24] See http://www.cabinetoffice.gov.uk/news/government-publish-new-data-health-schools-courts-and-transport for a summary of comparable open data initiatives, as well as http://www.guardian.co.uk/news/datablog/2011/jul/07/government-transparency-data-releases

3 Conclusion: striking a balance between PSI re-use and data protection?

The two examples above illustrate some of the data protection challenges that may occur when designing and offering PSI applications, from two entirely different perspectives. In the Slovak case, the application inevitably resulted in the processing and publication of personal data, as this was a part of its core functionality. Here, the main question is (and currently remains) whether the re-use of the personal data is compatible with the purposes for which it was made available by the data sources. In the UK case, the application did not inherently require personal data, and the focus was more on mitigating privacy risks by eliminating the processing of personal data in as far as possible, including through the use of anonymising techniques, and providing means of redress if any incidents occurred.

Both cases however show an important principle, namely that the PSI context does not provide any unique rules or exemptions for data protection compliance. The same questions that were raised in these cases could have occurred and would need to be resolved in the same way if the information sources had been made available by a private sector body. From that perspective, the terminology of striking a balance between PSI re-use and data protection seems somewhat deceptive, despite its common use[25]: both in theory and in practice, the current legal framework does not call for a balancing of interests in PSI and privacy, but for compliance with both sets of rules.

None the less, there is still a large gray area and much uncertainty in the application of data protection law. Good practices are certainly emerging, as witnessed by the crime maps case and the ICO opinion, which highlight the importance of data minimization, privacy by design and anonymisation[26]. In some cases however, the processing of personal data is unavoidable. The Slovak example of Znasichdani.sk showed the difficulty of measuring the legitimate interest of the re-users and the Slovak public in having optimally effective access to PSI, against the privacy interest of an individual who was personally impacted by this newly established transparency. A ruling on the merits is still missing in this case, and will undoubtedly impact how such issues are examined in the future.

In the meantime, PSI re-users will need to face the challenge of complying with data protection rules in an evolving regulatory landscape. This is no small task, but its successful completion will be crucial to ensure the legitimacy and positive public perception of PSI re-use in the future.

[25] Most notably in the aforementioned Article 29 Working Party Opinion 7/2003 on the re-use of public sector information and the protection of personal data, subtitled "Striking the balance"

[26] See e.g. the recent paper by the Information and Privacy Commissioner of Ontario, Ann Cavoukian, "Don't Stop Anonymizing the Data – It remains a safe, secure way to protect Privacy"; http://www.ipc.on.ca/english/Resources/News-Releases/News-Releases-Summary/?id=1085

Online resources

- http://opengovernmentdata.org/ - website of the Open Government Data Working Group of the Open Knowledge Foundation.
- http://data.gov.uk/ - OGD website operated by the UK government
- http://gov.opendata.at/ - Overview of Austrian OGD initiatives
- http://www.lapsi-project.eu/ - European Thematic Network on Legal Aspects of Public Sector Information, including an overview of relevant European cases: http://www.lapsi-project.eu/decisions
- http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_en.pdf - Opinion 7/2003 on the re-use of public sector information and the protection of personal data - Striking the balance; publication of the Article 29 Working Party, adopted on 12 December 2003
- http://znasichdani.sk/l?l=en – website of the Znasichdani.sk application
- http://epsiplatform.eu/news/news/open_data_challenge_winner_ordered_to_remove_certain_data - article on the Znasichdani.sk dispute
- http://spectator.sme.sk/articles/view/43180/2/court_orders_removal_of_public_procurement_data.html - article on the Znasichdani.sk dispute
- http://www.edri.org/edrigram/number9.15/slovak-open-data-court-order - article on the Znasichdani.sk dispute
- http://blog.okfn.org/2011/07/18/why-censoring-slovak-spending-app-means-bad-news-for-open-data/ - article on the Znasichdani.sk dispute
- http://www.police.uk/ – national crime statistics in the UK
- http://www.ukcrimestats.com, an application which links official crime statistics (including categories of crime) to specific locations
- http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf - Opinion 4/2007 on the concept of personal data; publication of the Article 29 Working Party, adopted on 20 June 2007
- http://www.guardian.co.uk/news/datablog/2011/feb/01/crime-maps-data-top-100-streets - Article on the scope and content of crime map data
- http://www.cabinetoffice.gov.uk/news/government-publish-new-data-health-schools-courts-and-transport - announcement of open data plans in key sectors in the UK
- http://www.bbc.co.uk/truthaboutcrime/crimemap/ - overview and demonstration of crime map possibilities
- http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/crime_mapping_advice.ashx - Guidance on crime-mapping, privacy and transparency from the Information Commissioner's Office, published on 24 November 2010
- http://law-in-society.blogspot.com/2011/02/privacy-risks-from-crime-mapping-jamie.html - analysis of data protection challenges related to crime mapping by Jamie Grace, Lecturer in Law in the School of Law & Criminology at the University of Derby.

About the Author

Hans Graux is a bar lawyer and founding partner at the Brussels based law firm time.lex (www.timelex.eu), which specializes in ICT law and ICT policy challenges. In addition, he is an affiliated researcher at the Interdisciplinary Centre for Law and ICT (www.icri.be) at the K.U.Leuven. He also acts as the independent legal advisor to the Vlaamse Toezichtscommissie (Flemish Supervisory Committee - http://www.vlaamsetoezichtscommissie.be/), which supervises personal data exchanges within Flemish public sector bodies.

Copyright information