WG 2 Policy Recommendation 1 : no need to modify PSI Directive regarding data protection & privacy provisions, but need to complete it or to clarify some questions

Dos Santos, Cristina; FERNANDEZ SALMERON, Manuel; BASSI, Eleonora; JANSSEN, Katleen; POLCAK,, Radim; TEPINA, Polona; VAN DER SLOOT, Bart; de Terwangne , Cécile

Publication date:
2011

Document Version
Publisher's PDF, also known as Version of record

WG 2 Policy Recommendation 1

No need to modify PSI Directive regarding data protection & privacy provisions, but need to complete it or to clarify some questions

(Working draft 3 – July 2011)

PARTNER RESPONSIBLE: CRIDS/FUNDP (University of Namur) – Belgium

AUTHORS:

DOS SANTOS Cristina & DE TERWANGNE Cécile (CRIDS/FUNDP); BASSI Eleonora (Università di Torino); FERNANDEZ SALMERON Manuel (Universidad de Murcia) ; JANSSEN Katleen (ICRI/K.U. Leuven); POLCAK Radim (Masarykova univerzita) ; TEPINA Polona (Informacijski Pooblascenec Information Commissioner) ; VAN DER SLOOT Bart (UVA/Universiteit van Amsterdam)

I. PRELIMINARY QUESTIONS :

The public sector collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, economic, geographical, weather, tourist, business, patent and educational information (Recital 4 of Directive 2003/98/EC[1], hereinafter 'PSI Directive').

Most of this information can be considered as 'personal data' following the provisions of Article 2 (a) of Directive 95/46/EC[2] (hereinafter 'Data Protection Directive'), which states that it "*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*".

This implies that **we have to combine both legislations** if we want to re-use personal data.

The PSI Directive makes reference to the Data Protection rules in the following articles:

- Recital (21): "*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): "*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*

[1] 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.*

[2] **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.* We should stress that **the Data Protection Directive is also currently under the process of its revision**.

and national law, and ***in particular does not alter the obligations and rights set out in Directive 95/46/EC.***"

- And Article 2 (5): "'***personal data' means data as defined in Article 2(a) of Directive 95/46/EC.***"[3]

Following these provisions, and taking into account that the Data Protection Directive already provides the legal framework for the processing of personal data, we have come to the conclusion that there is **no real need to review these articles in the PSI Directive**, as it already guarantees the respect of its principles by making clear reference to the data protection legislation.

However, we are invited to give assistance to the European Commission within the process of future revision of PSI Directive, of which Article 13 (2) states "***The review*** *[of PSI Directive]* ***shall*** *in particular* ***address the*** *scope and* ***impact*** *of this Directive, including the extent of the increase in re-use of public sector documents, the effects of the principles applied to charging and the re-use of official texts of a legislative and administrative nature, as well as* ***further possibilities of improving the proper functioning of the internal market*** *and the* ***development of the European content industry"***[4].

Indeed, in practice, we noted that some Member States have transposed the PSI Directive as regards the data protection aspects either by imposing the total "anonymisation" of personal data before allowing the re-use of data (e.g. PSI Belgian Law[5]) or by obtaining a previous "formal consent" from data subjects, which has hampered the development of a possible market for those data and has created heterogeneity of practices between Member States (and then legal uncertainty to possible "transborders re-users").

Some other Member States have imposed a mix of both solutions as well as a third solution: a legal text must allow the re-use of personal data owned by a public body (e.g. France). Moreover, when those solutions are not met, it could also be an obligation to have a prior authorization from the National Data Protection Supervisory Authority (e.g. the French CNIL obliges possible re-users to address it a prior request of authorization for personal data gathered by public archives).

Such disparities could be avoided by further references to data protection obligations and rights within PSI Directive provisions, as we will see in the following points.

---

[3] Stressed by the author.

[4] Stressed by the author.

[5] See Article 4 of the Belgian Law (Loi du 7 mars 2007 transposant la directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *M.B. 19.04.2007*).

II. INTERESTS INVOLVED

1. Object: Market and democracy

Although the PSI Directive clearly aims to increase the potential of the European internal market and to favour the development of the European "content industry"[6], as well as to extend the "right to knowledge" as a basic principle of democracy[7], we have to take into account that data protection and the respect of privacy are fundamental rights that arise from different European legal instruments[8] and from an extensive case-law of European Courts of Justice (ECHR and ECJ)[9].

Therefore it is important to respect Data Protection rules when personal data are processed, even for purposes of development of the market for re-use of PSI. As the PSI Directive does not even impose the re-use of PSI as an obligation to Member States and public bodies[10], in the current legal framework re-use of PSI cannot be considered as a "right" by itself for potential re-users.

As a result, we cannot make a clear "balance"[11] between both rights in order to find a satisfactory compromise (or solution) in the application of both Directives when personal data are at stake. On the contrary, we have to entirely respect data protection legislation in cases of re-use. This is for a matter of fact corroborated by Recital 21 of PSI directive.

2. Subjects: PSI producers, holders, users and re-users

On the one hand, we have PSI producers and/or holders – public bodies and institutions – that collect personal data (e.g. citizens' identity data, marital status, health data, social data, etc), produce it (to deliver a service to citizens), reproduce and disseminate it, in order to fulfil their public tasks in the public interest.

From the Data Protection Directive viewpoint, these actors must be considered as "first controllers"[12] of those personal data processing operations. Therefore, they are obliged to comply with all the provisions of this Directive and to ensure data subjects'[13] rights.

---

6 See Article 13 (2) and Recitals (1), (5) and (25) of PSI Directive.

7 See Recital (16) of PSI Directive.

8 See European Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 8) (ECHR); Charter of Fundamental Rights of the European Union (Articles 7 & 8); Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention n°108) of the Council of Europe; etc.

9 See relevant case-law on : http://ec.europa.eu/justice/policies/privacy/law/index_en.htm#caselaw

10 See Recital (9) and Article 3 of PSI Directive.

11 The word "balance" suggests a balance between two rights of equal value while one is dealing here with a fundamental right (privacy) and a kind of policy that has not even been granted the status of an individual right (which would in any case not be as strong as a fundamental right).

12 Following the provisions of Article 2 (d) of Data Protection Directive, a '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.

13 A 'data subject' is a natural person who can be identified or is identifiable by any information relating to him/her (see Article 2 (a) of Data Protection Directive that defines what a 'personal data' is).

On the other hand, from the perspective of users or potential re-users of public sector information that holds personal data, sometimes information referring to a specific person could be crucial to know more about public officials' actions and therefore to increase the value of democratic participation of citizens, civil society associations and non-profit organizations, for instance. Blockages to access to all personal data of data subjects (not only those concerning citizens but also those concerning civil servants/public officials of concerned public bodies) could not only hamper the market for re-use of PSI, but also possibilities of eDemocracy by a greater transparency of public administration.

Again, the frontier between access to information (which falls under the Freedom of Information's regimes of each Member State) and use of such information or re-use of PSI is extremely tight and complicated to define.

III. INTERESTS PROTECTED UNDER THE CURRENT LEGAL FRAMEWORK

The current wording of the PSI Directive suggests that the respect of Data Protection rules is important when developing a market of re-use of PSI containing personal data.

Indeed, in their quality of data controllers, public bodies have to respect all the obligations and principles imposed by the Data Protection Directive[14] such as:

- the lawfulness of personal data processing (the personal data must be processed fairly and lawfully),
- the principle of proportionality (personal data processing must be adequate, relevant and not excessive for the purposes for which they are collected),
- the purpose principle (personal data must be collected only for specified, explicit and legitimate purposes **and not further processed in a way incompatible with those purposes**),
- the data quality (data must be accurate and kept up to date when necessary),
- a "time of conservation" that permits **identification of data subjects for no longer than it is necessary for the purposes for which the data were collected** (Art. 6 (1)).

These provisions seriously limit the possibility of re-using public sector information containing personal data. Indeed, re-users in turn also become data controllers (for the new data processing[15] linked to the re-use) in case the re-use of personal data would be allowed, and should be submitted to all obligations and rights of the data protection legislation.

Moreover, **there are also limited criteria for having a legitimate data processing** that are provided by Article 7 of Data Protection Directive. Public bodies (PSI holders) and potential re-users also have to comply with them in their role of controllers, such as:

- Obtaining the unambiguous consent of the data subject, or
- Proving the necessity of the processing 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

---

[14] As provided by Article 6 (2) of Data Protection Directive.

[15] Following the definition given by Article 2 (b) of Data Protection Directive a 'processing of personal data' or 'processing' shall mean "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, 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*".

- Proving its **necessity for compliance with a legal obligation to which the controller is subject**[16], or
- Proving its necessity to protect the vital interest of the data subject, or
- Proving the necessity of the processing 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
- **Proving its necessity for the purposes of the legitimate interests**[17] **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).

There are also special categories of data the processing of which is in principle prohibited by Article 8 of the Data Protection Directive, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or data concerning health or sex life (so-called "sensitive data"). The processing of such data is only authorised in certain cases corresponding to the limited admitted exceptions of paragraphs 2 to 5 of the same article.

Furthermore, we have to take into account that data controllers are obliged to provide clear information to the data subjects in order to respect their rights (such as the right of access to data, the right of rectification, erasure or blocking data when their processing does not comply with the provisions of the Data Protection Directive (Art. 12), and the right to object to personal data processing (Art. 14).

Therefore, the PSI Directive could make more reference to such an obligation in the text of its Article 7 on transparency that recommends that "*any applicable conditions (…) shall be pre-established and published*", **by suggesting the establishment of a clear "privacy policy" by PSI holders,** for instance.

It could also make reference to it in its **article about "licences" (Article 8)** that states that "*public sector bodies (…) may impose conditions, where appropriate through a licence, dealing with relevant issues (…)*", **by also reminding the respect of privacy principles and obligations when a licence is established by a public body,** for instance.

[16] This is the main criterion that justifies the main personal data processing operations done by the public bodies, which fall within a specific legal framework – the Administrative Law or the Public Law - in some EU Member States (e.g. Civil Law systems).

[17] This is the main criteria that could be used by potential re-users when dealing with processing of personal data, and it is the balance of both "legitimate interests" (of the controller and of the data subject) that will determine the legitimation of the data processing concerned.

IV. LEGAL PROBLEM:

1. Rules are there but unclear : clarify

As stressed before, the PSI Directive makes clear reference to the Data Protection legislation. However, addressing problems that arise from the re-use of PSI when re-using personal data would be a **great opportunity** not so much to determine an explicit modification of the Directive on specific points, but **to generate a global debate on the issues related to the "tension" between the use of information held by public bodies and the respect for personal data** that could be introduced into the general approach of the Directive.

Furthermore, for some members of our working group, there are **different points** that **deserve more attention by PSI Directive reviewers**:

For some reviewers, a strong effort should be made in order to seriously try to establish the differences (clear in a theoretical perspective but that have increasingly being confused) between:

- Access to personal data;
- Access to public information under Freedom of Information (FOI) Acts, and
- Access to PSI for re-use purposes.

As re-use of PSI does not always have commercial aims, this characteristic considerably increases some of the already mentioned **"confusions" between the different types of "access" to information held by public bodies**.

For others, another issue that arises from some national laws transposing PSI Directive in this field is that there are also **problems in defining what "anonymisation" is and how far it should go**. And what is the "common meaning" of this word (if there is one)?

This is certainly a challenge, as sometimes some information could be "formally anonymised" (and therefore Data Protection Directive does not need to be applied) but it could not be enough to avoid the identification of individuals (e.g. some kinds of geographic information combined with other data could allow specific identification of people). Anonymisation is a technical problem and a functional concept.
A legislator cannot state what anonymisation is (in a technical sense), but should require it (or a specific kind of it), for instance, for specific categories of personal data. E.g. the Italian legislation prescribes anonymisation in some cases (e.g. for the re-use of judicial data for legal information purposes), but without any reference to a generic possible re-use.
We could suggest the way of anonymisation as the "default rule" for personal data collected by public bodies in order to facilitate the processing of them (including the re-use), but not as a necessary condition for the re-use (as it is done by some Member States PSI legislation).

Nevertheless, we are not sure that this solution should be introduced in the PSI Directive, rather than in the Data Protection Directive and/or in the national legislations on data protection and re-use of PSI.

From our viewpoint, the **Article 29 Working Party**[18] **is the "right arena" to discuss such questions**, as it deals with ensuring uniform interpretation of the Directive between the national data protection authorities (NSAs) of different Member States. In fact, this is a simple question of application of data protection to a "reality" probably still fairly new, which is the reuse of PSI. Therefore, the Article 29 Working Party (hereinafter 'Art. 29 WP') could allow a discussion grouped around this theme, leading to harmonized interpretations of what are the data protection requirements in the presence of re-use.

Then, **it should also be the moment to adapt and update Art. 29 WP's working papers (WP) on re-use of PSI that have already been produced**, and especially its opinion on the re-use of public sector information and the protection of personal data[19] delivered in 2003.

This working paper has already stressed some key points[20], as for instance:

- "*the **data protection Directive is fully applicable once personal data in the sense of that Directive are requested for re-use** (…). According to Article 30 of Directive 95/46/EC, **the Working Party may make recommendations on all matters relating to the protection of personal data in the Community***" (p. 2).

Such assertion just confirms our position in this field, that it is **Art. 29 WP that is the right actor to help the European Commission to solve problems of combination of both directives** when there is re-use of personal data held by public sector bodies (PSI holders).

- "*It is **important to underline the difference between access to personal data in terms of the data protection Directive**, access to documents of the public sector under freedom of information laws **and making available of public sector information containing personal data for re-use purposes.** (…) A re-use of personal data envisaged under the re-use Directive is, as opposed to the two cases mentioned above, intended as input for commercial activities, thus presents an economic asset for business, which neither has the human rights not the transparency aspect (…). **The present document is meant to give guidance for this latter case only, as regards access to personal data for re-use purposes**.*" (p. 3);

We can criticize **such a statement** of Article 29 WP: it **should be updated** in the sense that limiting its assessment to the re-use of personal data only when it is for commercial purposes is making a clear limitation of the re-use principle (when allowed) that does not appear in the text of the PSI Directive. Indeed, Article 3 of PSI Directive clearly states that "*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 (…)*".

So, should we consider that the Art. 29 WP is suggesting that when the reuse of personal data is done for non-commercial purposes it is always allowed? How can we avoid such "discrimination" between both purposes (and possible "manoeuvres" of potential re-users that want to circumvent this obstacle by using false non-commercial purposes)?

- "*The question of whether the data protection Directive allows the re-use of public sector information that contains personal data **requires a careful and case-by-case assessment in***

---

[18] This group was created by Article 29 and following of Data Protection Directive. See its role and competences on: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

[19] *Opinion 7/2003 on the re-use of public sector information and the protection of personal data – Striking the balance*, WP 83 of Article 29 Working Party, adopted on 12 December 2003.

[20] In bold: stressed by the author.

***order to strike the balance between the right to privacy and the right to public access**. **Public sector bodies will have to consider whether public disclosure would be legitimate in the concrete case, according to the criteria set out in the Directive**. Given that **the examination of the finality principle is crucial in this context**, this opinion provides a number of elements that have to be taken into account in this assessment. **In case disclosure is envisaged, public sector bodies will have to observe data subject's rights, such as the right to be informed or the right to object to disclosure**, in particular if the data are intended to be re-used for commercial, for instance direct marketing, purposes.*" (p. 11).

On the one hand, the main problem with this statement is that **such "case-by-case assessment" could easily lead to heterogeneity of practices and solutions** either between public bodies (even for the same personal data) or between different levels of public sector bodies, and therefore between Member States. That would **create greater legal uncertainty and an additional obstacle to the re-use of personal data gathered by public sector**.

On the other hand, even if such case-by-case assessment is not ideal in a context of re-use of PSI market, **some room should be left to public bodies**, as it could not totally be avoided without making too general assessments (which would probably lead to restrictions "just to make sure everything is covered").

Then, we could consider that some "general assessments" should be made by the Art. 29 WP at the pan-European level (by "consensus" of all members and in collaboration with the PSI Group[21], for instance) via a new (or updated) opinion. Therefore, the "case-by-case assessments" should be made by each national supervisory data protection authority (NSA's) in order to take into account national legal specificities and special categories of personal data for certain kinds of re-use.

The Art. 29 WP should make more clear guidance about some crucial points as:

- **How to respect the purpose principle** when re-use of personal data is allowed?

In principle, re-users are not obliged to justify why they want the data, but in case of re-use of personal data and in order to be compliant with the Data Protection Directive this is an essential requirement to fulfil. This mentioning of the purpose of the intended re-use is necessary to assess the character compatible or not of this purpose with regard to the initial purpose of collection of the data. Generic re-use is not a compatible purpose, but the re-users should declare the specific re-use purpose, in order to permit the controller (e.g. the public administration) to allow that specific re-use.

One should distinguish when access to personal data is possible, when it is allowed for further use (as for journalistic reasons, for instance), and when it could be allowed for possible re-use (and then the purpose principle applies for the new data processing).

- **How to respect the obligation of the information** of data subjects: should it be "individual" or could it be only "general"?

This obligation could be respected by the public body by **providing a clear "privacy policy" in its website**, which could give the information of a possible re-use of the data processed. However, the "second" data controller **(the re-user) should in turn put in place its own system of information of data subjects' rights** for the new data processing of the re-use.

---

[21] This is a group of experts on PSI Group that has been set by the European Commission in 2002 to exchange good practices and initiatives and to discuss and to recommend solutions in different fields. See http://ec.europa.eu/information_society/policy/psi/facilitating_reuse/psigroup/index_en.htm

- **How to obtain the formal consent of data subjects** when re-use of personal data is allowed by public bodies? **What about the current technical possibilities of privacy by design within public sector databases and registries?**

It could be possible to **provide a kind of opt-out/opt-in system by the way of the public body website**, for instance, **or by obtaining this consent (preferably in writing) at the moment of the first collection of the data**, when it is possible.

Or public sector databases and registries could also include a kind of **technical system that help public bodies to anonymize personal data after the storing time** of their first processing in order to automatically allow re-use of these data after this anonymisation.

These two examples of privacy by design could be completed or changed by other tools following the "sensitivity" of the personal data concerned.

- **What about the respect of the quality of data**?

As mentioned before, **the system of licences provided by PSI Directive could be a good tool to reinforce data protection by PSI holders and further re-users**, as well as **to help them to clearly define responsibilities of the data controllers**.

One should also take into account that at the national level some Member States set out other supervisory authorities in the field of access to public documents (like the CADA[22] in France) and/or for re-use of PSI (as a kind of authority of "appeal" of re-use of PSI practices, like in Belgium[23]), **therefore both authorities should collaborate in order to avoid disparities of solutions and opinions.**

2. Rules are there but not functioning : change

Our main objective, within the LAPSI WG2 network, is to rightly determine the requirements the protection of privacy imposes on the re-use of PSI and to identify the possible problems such requirements could lead to.

On the one hand, data protection rules should not be used like a "mere excuse" by public bodies to excessively restrict the re-use of PSI (when it implies personal data). On the other hand, we have to take into account situations where data protection provisions are really welcome to protect individuals' rights against abuses from potential re-users.

One crucial point that we have already addressed is that the **Data Protection Directive is currently under review process (this should be achieved at the beginning of 2012) and it is important to associate both revisions in this field**. In this project, we rather shall address the impact data protection rules may have on the re-use of PSI and identify possible problems, like excessive blocking solution Belgian example and very large differences in interpretation of these requirements by the

[22] Commission d'accès aux documents administratifs (Commission of access to administrative documents, which also deals with re-use of PSI French law) : http://www.cada.fr/index.htm

[23] Commission d'accès aux et de réutilisation des documents administratifs (Commission of access to and of re-use of administrative documents: the first one is about access and gives opinions about it, the second one is a kind of "appeal authority" to solve litigations between public bodies and re-users): http://www.fedweb.belgium.be/fr/actualites/nieuws_20090212_hergebruik.jsp

authorities of a country relative to another - if there is this - which could lead us to propose to send a signal to find a solution at European level to reduce these differences.

Changing PSI Directive provisions regarding data protection issues is not a solution in itself. Initially, European Commission should rather address the problem of "bad transposition" of PSI Directive by Member States as regards re-use of personal data information provisions. Then, **PSI Directive reviewers should introduce a clear reference in this directive as regards the existence of National Data Protection Supervisory Authorities at national level, in order to "invite" (or oblige) potential re-users to address their requests to these authorities when personal data are at stake**[24].

V. ARGUMENTS IN FAVOUR OF ....AND RELATED COUNTER-ARGUMENT

1. **PSI Directive already clearly mentions the application of Data Protection Directive** when personal data are at stake.

   Nevertheless, the practice shows us that **it is not enough to avoid bad harmonisation of solutions** between different public bodies and Member States.

2. **Data Protection Directive already contains enough provisions** that could solve possible blockage of re-use of personal data.

   Nevertheless, problems related to the implementation and the applications of this directive are also very important. **It is important to put in relation the revision of PSI Directive and of Data Protection Directive at the European Commission level by both reviewers.**

3. **Making more references** to such rules **in other articles of PSI Directive could be enough** to clearly remind which actors are concerned by interpretation of both directives (Art. 29 WP, NSA's, etc).

   The problem is that **increasing such textual references could make the text of PSI Directive more "indigestible" for potential re-users and even more complex for its implementation**.

VI. ARGUMENTS AGAINST ... AND RELATED COUNTER-ARGUMENT

Re-using public sector information might trigger the Data Protection Act when it involves personal data. These are defined under the directive as any information relating either directly or indirectly to an identified or identifiable natural person. Both objective and subjective information qualify; the form in which it is kept is irrelevant. Information may relate to a person either *qua content*, if information refers to a person, *qua purpose*, if the information is used to evaluate or influence personal behaviour, or *qua result*, if the consequence of data processing is that a person might be treated or looked upon differently.

Given the general scope of the definition of personal data, many governmental documents will contain personal data. Both the government and the party receiving the public sector information will need to fulfil three major categories of obligations in the Data Protection Directive: first, the

[24] See solutions already provided by "*Deliverable 3 – Solutions for eGovernment*" of the Modinis Study "Breaking Barriers to eGovernment: overcoming obstacle to improving European public services", 'Section 4: Legal Solutions to Barriers to eGovernment', DE TERWANGNE C. & DOS SANTOS C.: 'Re-use of Public Sector Information' (pp. 72 to 78), version of 23/12/2007.

required legitimate purpose, secondly, respecting the safeguards spelled out by the directive and finally, respecting the rights of the data subject in connection with the transparency principle.

It will be difficult for the re-using party to have his/her processing of personal data considered as a legitimate purpose for the processing of personal data. Usually, the re-use of the information will not be necessary for the performance of a contract, or to comply with a legal obligation, a public task carried out in the public interest or to protect the vital interest of the data subject and getting the consent of every person of whom personal data is contained in the information will be a too laborious process. The most likely legitimate purpose to apply is the so called balancing provision, with which the interest of the controller or the third party to which the data is disseminated is balanced with the interest of the data subject, especially with regard to the respect for his fundamental rights to privacy and data protection. Only if another fundamental right is served by the re-use of public sector information containing personal data, most commonly the right to freedom of speech, will there be a situation in which the two equal interests must be balanced. If it regards processing of sensitive personal data, relating to sexual, medical, political or criminal information, this regime is even stricter.

Next to the obligation with regard to the legitimate purpose for data processing, the directive spells out several safeguards. Most importantly, personal data may only be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Thus, governmental organizations must see to it that the purpose for processing by the third party is not incompatible with its own reasons for processing the data. In any case, the Working Party 29 emphasizes that if personal data are to be re-used for commercial purposes, this secondary purpose may be considered as incompatible. Furthermore, since governments will usually have gathered personal data in relation to serving the public interest, security matters or legal obligations, it will often prove difficult for re-using third parties to circumvent the purpose limitation.

Finally, account should also be taken of the transparency principle and the rights of the data subject. For example, a governmental organization disseminating public sector information to third parties needs to see to it that every data subject is adequately informed of this matter. Furthermore, the third parties are under a similar obligation. Data subjects have a right to access and objection to the processing of their personal data. Current practice disregards these rights of the data subject.

All three categories of obligations thus cause serious problems for the re-use of public sector information. Good solutions are very few and far between. Seeing the difficulties, a total prohibition of the re-use of public sector information might be the most feasible solution, however it would leave the economical potential of the European public sector information unutilized. On the other hand, the disregard of the Data Protection Directive, as a practical solution, would leave the fundamental rights of citizens to data protection and privacy unprotected. A third solution for the tension between the re-use of public sector information and the rights to privacy and data protection may be found in anonymisation techniques. However, since it is true that ‘data can be either useful or perfectly anonymous but never both’, anonymisation would mean a gross loss of value of the public sector information.

That is why **a new solution is proposed: personal privacy settings**. By letting every citizen register which data of his could be used by whom, for what purpose and for how long, citizens could give their specific consent and know at the same time which parties want to use their data. They are also at liberty to ask a lump sum for their private data or a share of the profit. By this way, re-using parties will obtain a legitimate purpose, namely consent, the data will not be ‘further processed’ since re-

using parties will get the personal data from the subjects directly and they will be able to inform the citizens of their use and allow them both the right to object. [25]

VII. IF POSSIBLE: WHAT IS HEAVIER BETWEEN V. AND VI.?

It seems quite evident that the last solution (VI) would be virtually impossible to implement at this stage. Indeed, it does not answer to the new questions that could arise:

- How to ensure that any citizen has access to his/her personal privacy settings within each public body processing his/her personal data?

- Who will assume the costs to implement such a policy? The citizens (who have already paid for the service), the public bodies (that are currently subject to budgetary restrictions), the potential re-users (how to identify them and oblige them to pay)?

- How to overcome the lack of "digital literacy" of some citizens, as well as all educational issues related with the "real" understanding of people as regards their privacy threats and the implications of a "commercialisation" of their rights in the long term?

It is the role of the European legislator to ensure that data protection provisions apply for each kind of "data subject" who could be concerned by the re-use of personal data, even and moreover when it has also to take into account the improvement of the information market.

[25] See VAN DER SLOOT B., *Personal privacy settings for the re-use of PSI: Towards a new model for the re-use of PSI in the light of the right to Data Protection*, Paper presented during the 1st LAPSI Public Conference, Milano 5-6 May 2011.