LAPSI
The European Thematic Network on Legal Aspects of Public Sector Information
http://www.lapsi-project.eu/

LAPSI Policy Recommendation N. 4
Privacy and Personal Data Protection

LAPSI Working Group 2
Privacy Aspects of PSI

Main Authors: **Cristina Dos Santos & Eleonora Bassi; Cécile De Terwagne, Manuel Fernádez Salmerón, Polona Tepina, Bart Van der Sloot**
Substantial Comments and National Examples Received from: **Katleen Janssen, Clarissa Otto, Radim Polčák, Julián Valero-Torrijos**

FINAL VERSION

All the LAPSI policy recommendations are available on the LAPSI website at:
http://www.lapsi-project.eu/policy

Executive Summary

- *The PSI Directive contains only some modest references to the Data Protection Directive (i.e. in Rec. 21, Art. 1(4) and 2(5), Dir. 2003/98/EC), confirming that fundamental rights of privacy and data protection should be respected in cases of re-use. These references are vague and are not enough to avoid poor harmonisation of the PSI Directive throughout Member States and inconsistent usage between public bodies. Indeed, the transposition of PSI Directive as regards data protection provisions is very different between Member States. Such heterogeneity hampers the standardization of rules and best practices, blocking the development of possible markets for re-usable data and creates legal uncertainty for public sector bodies and potential re-users, especially in the perspective of a cross-border re-use market.*
- *The disparities that emerge from different solutions in national data protection and access legislation could be avoided by further detailed references to data protection rules within the provisions of the PSI Directive. Solutions could be found in the review of Articles 7 (transparency) and 8 (licences) of PSI Directive, with further references (e.g. a new paragraph) to the obligation of informing data subjects on processing of their personal data, with inclusion of provision on a clear privacy policy for reusable personal data, and with mentioning of data controllers' and data processors' obligations. A better harmonization of redress mechanisms and a clarification of competences of data protection authorities (DPA's) for the cases of access to information and re-use of personal data are also needed.*
- *The full application of the Data Protection Directive to the re-use of public sector information (PSI) could seriously limit the possibility of re-using of the PSI that contains personal data. The fact of the matter is that re-users are considered as data controllers for the new data processing and should abide by all obligations of the data protection legislation.*
- *As data controllers, public bodies and subsequently the re-users may only process (re-use) personal data if they have legitimate ground for processing (Art. 7, Data Protection Directive) and should respect all obligations and principles imposed by the Data Protection Directive, such as fair and lawful processing, the principle of proportionality, the purpose limitation principle, the data quality principle, limitation of data retention periods, etc. (see Art. 6, Data Protection Directive).*
- *Moreover, data controllers are obliged to respect all data subject's rights, such as the right of access to data, the right of rectification, erasure or blocking of data when their processing does not comply with the provisions of the Data Protection Directive, and the right to object to personal data processing. They are also obliged to provide clear information to the data subjects in order to respect their rights.*
- *We suggest that the PSI Directive makes more references to such obligations in different Articles as, for instance:*
    - *Article 7 of the PSI Directive on transparency, which recommends that "any applicable conditions (...) shall be pre-established and published", should suggest the establishment of a clear "privacy policy" or "information document" by PSI holders and then by re-users; and*

- *Article 8 of the PSI Directive on licences, which states that "public sector bodies (...) may impose conditions, where appropriate through a licence, dealing with relevant issues (...)", should remind about respect of privacy principles and obligations when a licence is established by a public body.*

- *We think that the Article 29 Working Party should also be included in the search for possible solutions for the application of data protection principles to re-use practices. In this respect it would be useful to update the Working Party Opinion 7/2003 on the re-use of public sector information and the protection of personal data – Striking the balance.*

- *In our opinion it would be essential to further address some of the dilemmas regarding the crucial points that could hinder the full implementation of the PSI Directive regarding personal data protection:*

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

  - *How to respect the obligation of the information of data subjects: should it be "individual" or could it be "general" (e.g. in the form of privacy policies)?*

  - *How to obtain formal consent of data subjects?*

  - *What about the current technical possibilities of "privacy by design" in order to enforce data subject's rights within the public sector databases and registries?*

  - *What about the respect of the quality of (personal) data? Could it be enforced through licences? And how could it fit with databases interoperability and with data anonymisation?*

  - *How wide and mandatory should be the recourse to anonymisation techniques? We could suggest anonymisation as a "default rule" for personal data (or a specific kind of it) collected by public bodies in order to facilitate re-use processing, but not as a necessary condition, as it goes beyond the boundaries imposed by Data Protection Directive and as it could imply a great loss of value of the PSI. Nevertheless, we are sceptical of introducing this solution in the PSI Directive.*

- *Because of many opened questions and dilemmas, we therefore suggest that further considerations should be made to data protection principles and their application to the re-use of personal data (especially legitimate grounds for re-use, purpose limitation, data retention...). Privacy by design and data protection impact assessment are two concepts that should be considered, as well as introducing some sort of "privacy policies" for re-usable personal data. However, changing the provisions on data protection issues in the PSI Directive is not a solution by itself; the European Commission should also address the problems that occurred by "bad implementation" of the PSI Directive in some Member States as regards re-use of personal data information, especially in respect of the question of mandatory anonymisation of personal data.*

1 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').

A great amount of these 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 the term 'personal data' "*shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*.

This implies that when personal data is to be re-used, provisions of both legislations have to be applied.

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 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.*"

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 of the PSI Directive**, as it already guarantees the respect of data protection principles by making clear references to the Data Protection Directive.

However, we were invited to give assistance to the European Commission within the process of future revision of PSI Directive. Article 13 (2) of this Directive states that "*[t]he review 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"*.

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[3]) or by obtaining a previous "formal consent"

[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 currently also under the process of revision.

[3] See Article 4 of the Belgian Law of 7 March 2007 on re-use of PSI (*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.*

from data subjects. 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. in France and in Slovenia). Where these solutions are not introduced, another possibility is also the obligation to obtain prior authorization from the National Data Protection Authority (hereinafter 'DPAs')[4].

Such different approaches have hampered the development of possible markets for information and have created a heterogeneity in Member States' practices, which also brings greater legal uncertainty for possible "transborders re-users" of personal data.

These disparities could be avoided by **further references to data protection obligations and rights within the provisions of the PSI Directive**.

2 Interests involved

2.1. 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"[5], as well as to extend the "right to knowledge" as a basic principle of democracy[6], we have to take into account the right to data protection and respect of privacy, since they are fundamental human rights that arise from different European legal instruments[7] and from the extensive case-law of the European Court of Human Rights (ECHR)[8] and the European Court of Justice (EJC)[9].

Therefore, **it is important to respect the data protection rules when personal data are processed, even for the purpose of developing the market for the re-use of PSI**.

As the former wording[10] of PSI Directive did not even impose the re-use of PSI as an obligation to Member States and public bodies, within that legal framework the re-use of PSI could not even be considered as a "right" by itself. As a result, it was not easy to make a clear "balancing test"[11] between both "rights" in order to achieve a satisfactory proportionality balance of interests in the application of both Directives when personal data were at stake. On the contrary, Recital (21) of the PSI Directive corroborated the fact that we had to respect data protection legislation entirely in cases of re-use.

However, the new version of the European Commission's proposal for amending the PSI Directive introduces the principle of a "re-use of PSI right"[12], which would create further confusions for the application of both legislations. It will certainly be useful to have further case law of the European Courts in order to understand how to manage both issues whether the European Parliament and the

19.04.2007).

4 See some national examples below in chapter 4.

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

6 See Recital (16) of PSI Directive.

7 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.

8 See the case law of the European Court of Human Rights concerning the protection of personal data on: http://www.coe.int/lportal/c/document_library/get_file?uuid=ec21d8f2-46a9-4c6e-8184-dffd9d3e3e6b&groupId=10227.

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 (re-use of PSI) 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 See European Commission, *Proposal for a Directive of the European Parliament and of the Council Amending Directive 2003/98/EC on re-use of public sector information,* COM(2011)877 final.

Council accept this new version of the PSI Directive[13].

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

On the one hand, the position of PSI producers and/or holders has to be taken into account. Public bodies and institutions collect vast amounts of personal data (e.g. citizens' identity data, marital status, health data, social data, etc.) and produce, reproduce and disseminate it in order to fulfil their public tasks in public interest. From the Data Protection Directive's standpoint, public sector bodies must be considered as "first controllers"[14] of personal data. Therefore, they are obliged to comply with all the provisions of this Directive and ensure all data subjects'[15] rights.

On the other hand, from the perspective of users or potential re-users of public sector information, which often comprise personal data, successful re-use can imply gaining information related to specific individuals, most notably in cases where it is crucial to learn more about public officials' activities. Re-use of personal data, as well as all other information, is therefore a key to increase the value of democratic participation of citizens, civil society associations and non-profit organizations. Obstacles to free access to and re-use of all personal data (not only personal data relating to citizens but also those concerning civil servants/public officials) could very well hamper the "market" for re-use of PSI.

Again, the frontier between access to information (which falls under the Freedom of Information's regimes of each Member State) and use or re-use of PSI is extremely tight and complicated to define[16]. This is linked to the fact that the definition of re-use is not limited only to commercial use of PSI but encompasses also non-commercial re-use.

3 Some National examples as regarding re-use of personal data

In this section, we stress the fact that the transposition of PSI Directive as regards data protection provisions is very different in national legislations of the Member States. Such heterogeneity of solutions has lead to different interpretations by public sector bodies and potential re-users, especially in the perspective of cross-border markets of re-use of PSI.

This "non harmonisation" of solutions should therefore be taken into account by the European Commission in order to provide further guidance in the revised text of the PSI Directive.

Below is presented a non-exhaustive list of Member States legislation, mainly based on the contributions of the LAPSI members involved in this document. Other countries may have adopted different legislative solutions.

Belgium (*By Cristina DOS SANTOS & Cécile DE TERWANGNE)*

As Belgium is a Federal State, the PSI Directive has been transposed at several levels of

[13] See also the EDPS' Opinion quoted on point (v.) 3., below in the text.

[14] 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*".

[15] 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).

[16] See also considerations of the LAPSI Working Group 6 about 'Constitutional, Human Rights and Environmental Perspectives' in its "*Policy Recommendations on Rights of Access to Public Sector Information*", available on: http://www.lapsi-project.eu/materials#4

governance.

At federal level, the Law of 7 March 2007 on the transposition of Directive 2003/98/EC[17] has been adopted. It has incorporated the general principles governing the re-use of public sector information, while the Royal Decree of 29 October 2007 sets up the procedure and time limits for dealing with requests for the re-use of public sector information. It also sets up a "Transparency Committee" whose tasks are mainly to help the External Communication service of the Federal Administrative Streamlining Agency (ASA)[18] to carry out its assignment. For example, this Committee should keep a register in order to provide potential users with information about the re-use of the administrative documents available and the re-use conditions[19].

Article 2, §1, 3° of the Law of 7 March 2007 refers to the definition of 'personal data' stated by the Belgian Data Protection Law[20]. Particularly, its Article 4 states that:

> "*An administrative document that includes personal data can be re-used only under the condition that the public authority has taken all necessary measures of precaution in order to hide the identity of the data subject, particularly by anonymizing them (...)*"[21].

A Federal Commission of Appeal has also been created[22]: it is empowered to vet and take decisions on appeals lodged by private individuals against decisions of a public body or in the event of a failure to comply with one of the clauses in a licence for re-use (or any other access condition).

At the regional levels, the Belgian Communities and Regions[23] have transposed the PSI Directive by their side, at different moments. For instance, the Flemish Community has adopted three Decrees[24] in 2007, after the federal law; while the Walloon Region has adopted two decrees[25], even before (in December 2006). The latter has adopted the same wording as the Federal Law as regards the re-use of personal data, i.e. imposing the total anonymisation of the individual identities (Article 4)[26].

---

17 *Op. cit.*

18 The '*Agence pour la Simplification Administrative/Dienst Administratieve Vereenvoudiging'*, was created in 1998 as a service accountable to the Belgian Prime Minister. This Agency is in charge of the transposition of PSI Directive at Belgian federal level, while it should coordinate the transposition activities at other levels of governance. More information on: http://www.simplification.fgov.be/showpage.php?iPageID=721&sLangCode=FR

19 There is no information about the state of the work of this Committee after December 2008. Source: English version of the ASA website about re-use of PSI on http://www.simplification.fgov.be/doc/1235491058-5398.pdf

20 Belgian Data Protection Law of 8 December 1992 on the protection of privacy in relation to the processing of personal data *(Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, version consolidée, M.B. 18 March 1993)*, Article 1 (1).

21 Free translation by the author. The text in French states that: "*Art. 4. Un document administratif qui comporte des données à caractère personnel ne peut être réutilisé qu'à condition que l'autorité publique ait pris les mesures de précaution nécessaires afin d'occulter l'identité de la personne à laquelle les données à caractère personnel ont trait, en particulier en rendant les informations anonymes (...)".*

22 See the Belgian Federal Commission on Access to and Re-use of Administrative Documents (implemented by the Royal Decree of 29 April 2008 on the composition and activities of the Commission on Access to and Re-use of Administrative Documents). To date, there is no case brought to the second section about re-use of administrative documents of this Commission (see information also provided by website http://psi.belgium.be/fr/legal - last consultation on 3rd September 2012), while the first section on access to administrative documents already received several demands.

23 In Belgium, there are five communities or regions, entitled to edit norms: the Flemish Community, the Walloon Region, the French-speaking Community, the Brussels-Capital Region, and the German-speaking Community.

24 See Decree of 27 April 2007 on the re-use of public sector information; the Government of Flanders Decree of 19 July 2007 on the re-use of public sector information in the context of the various departments within the Flemish Ministries and in the context of internally autonomous agencies without legal personality; and the Government of Flanders Decree of 19 July 2007 on the creation of a professional body for the public conduct of the administration and re-use of public sector information (available on: http://www.simplification.fgov.be/doc/1235491058-5398.pdf, p. 6).

25 See Walloon Decree of 14 December 2006 transposing Directive 2003/98/EC of the European Parliament and the Council of 17 November 2003 on the re-use of public sector information; and the Walloon Decree of 14 December 2006 transposing Directive 2003/98/EC of the European Parliament and the Council of 17 November 2003 on the re-use of public sector information and relating to the public conduct of the administration for matters where the Region exercises the powers of the French-speaking Community.

26 The same goes for the Order of 6 March 2008 of the Brussels-Capital Region (in its Article 4), for instance, while the Flemish Decree did not provide any information about that.

It is interesting to notice that the Belgian Data Protection Law has created different "sectorial committees"[27] within the Belgian NDA – *la Commission de la protection de la vie privée* (CPVP). One of these committees - the Sectoral committee of the Federal Authorities - is competent to authorize the electronic disclosure of personal data by any federal public service or any public authority with a legal personality belonging to the federal authorities.

Indeed, Article 36bis of the Belgian Data Protection Law requires "interested persons" to ask for permission to receive communication of data hold by federal public bodies. It states on comma 3 that:

> "*Except for cases determined by the King, any electronic disclosure of personal data by a Federal Public Service or a public institution with a legal personality that is under the jurisdiction of the Federal Government, shall require an authorization of principle by this Sectoral Committee, unless the disclosure is already subject to an authorization of principle of another Sectoral Committee established within the Commission for the Protection of Privacy*"[28].

A form of prior request of authorisation was provided for by the CPVP in its website at the end of 2011[29]. Following the requirements written at that time, such request should be "complete, clear and justifiable" and respect a certain number of obligations. The "applicant" should provide information about, notably: its identity (kind of public authority/service or unit); the recipient(s) or categories of recipients; some information about the data requested (exact needs, proportionality proof, conservation period); the purpose of the processing for which "*the access or the communication of personal data are required*"; the mention of the law, decree or order that "*obliges the applicant to request such data*"; etc.

At that time, this form also mentioned *"the interest of the communication for the applicant within the framework of its business"*[30]. Also, we have noticed in a previous version of this policy recommendation[31] that it was interesting to note that this last point seemed to refer to the possibility of re-use as intended by PSI Directive[32]. The word "business", even if not clear, clearly did not seem to refer to a "public task" or mission of the applicant. Currently, such form is no more available with this content in the CPVP website[33].

Nevertheless, the existence of the mandatory system of anonymisation of personal data put in place by the Belgian PSI Federal Law still reveals inconsistency with the PSI Directive and the Data Protection legislation (at national and European level). We can also report that Article 36bis of the Belgian Data Protection Law seems to create a further "discrimination" between potential re-users:

---

[27] There are six "sectorial committees" ('*Comités sectoriels'*): on the National Registry Number, for the National Health System, for the Federal Authority, about the Crossroad Bank of Enterprises, a Surveillance Committee on the Phenix System (judicial system), and a Surveillance Committee on Statistics.

[28] Free translation by the author. In French, Article 36bis, comma 3, states that: *"Sauf dans les cas fixés par le Roi, toute communication électronique de données personnelles par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale, exige une autorisation de principe de ce comité sectoriel à moins que la communication n'ait déjà fait l'objet d'une autorisation de principe d'un autre comité sectoriel créé au sein de la Commission pour la protection de la vie privée."*

[29] See new procedure (on September 2012) on: http://www.privacycommission.be/fr/procedure-autorisation-af#section-0

[30] Information provided by the website of the CPVP, under the 'competences' of the "*Comité sectoriel pour l'Autorité Fédérale*" on November 2011.

[31] A previous version of our Policy Recommendation was issued at the end of November 2011 and was disseminated by the LAPSI wiki website on: http://www.lapsi-project.eu/wiki/index.php/Policy_recommendation_on_privacy

[32] Article 2 (4) of PSI Directive defines re-use as "*the use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced*.".

[33] On May 2012, a member of the CPVP took an "informal contact" (by telephone) with us as regards our former interpretation and the form of prior request was modified in the new version of the CPVP website launched recently. The new version of the form avoids this misunderstanding.

whilst public bodies could have the possibility to re-use other public bodies' personal data under certain conditions, individuals and/or businesses couldn't.

France (*By Cristina DOS SANTOS)*

Article 13 of the French Law n° 78-753 of 17 July 1978 about access to and re-use of PSI[34] - also called 'CADA Law' - states that "*the re-use of PSI holding personal data is subject to the respect of the provisions of the [Data Protection Law*[35]*]"*[36], and authorises the re-use of personal data in three cases: when the data subject has given his/her consent; when the personal data have been anonymised; and/or when a legislative rule or a regulation allows it.

In the case of public archives, for instance, re-use of personal data is also subject to the conditions provided by the French Patrimony Code – *Code du Patrimoine* - especially for the respect of the time of conservation of public archives (see also Article 20 of CADA Law). Furthermore, the French NDA – the CNIL[37] - obliges possible re-users to address it a prior request of authorization for personal data gathered by public archives.

For instance, the CNIL's Recommendation of 9 December 2010[38] defines the conditions when commercial re-use of personal data held by archives could be possible (and when not):

- it excludes the re-use of the so-called "sensitive data" (Articles 8 and 9 of the French Data Protection Law)
- it excludes the re-use of the mentions made in the civil status' Acts[39], even those of dead people: even if those data could be accessed following the CADA law and the Patrimony Code, the CNIL imposes their anonymisation or their masking in case of re-use, taking into account "*the interests of the data subjects' beneficiaries/legal claimants (in French: "Ayant droits")*";
- however, the CNIL authorises the (commercial) re-use of other personal data if some "precautions" are followed, as:
  - the provision of a "general, clear and complete" information of the data subjects (especially when their data could be spread by Internet): additional guarantees could be requested by the CNIL in certain cases (e.g. when an individual information has not been possible). Furthermore, any living individual has the right to obtain the removal of his/her data without conditions;
  - the respect of the data subjects' rights and of their beneficiaries/legal claimants rights: the latter could, for instance, ask for the updating of those data (following the provisions of Article 40 of the Data Protection Law), and even obtain the removal of these data if

[34] See Law of 17 July 1978 modified by the Order of 6 June 2005 *(Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'améliorations des relations entre les administrations et le public et diverses dispositions d'ordre administratif, social et fiscal, modifiée par l'ordonnance n° 2005-650 du 6 juin 2005 et par l'ordonnance n°2009-483 du 29 avril 2009).*

[35] See Law of 6 January 1978 modified by the Law of 6 August 2004 (*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*), also called «*Loi Informatique et Libertés»*.

[36] Free translation by the author. Article 13, in French, states that: *"Les informations publiques comportant des données à caractère personnel peuvent faire l'objet d'une réutilisation soit lorsque la personne intéressée y a consenti, soit si l'autorité détentrice est en mesure de les rendre anonymes ou, à défaut d'anonymisation, si une disposition législative ou réglementaire le permet. La réutilisation d'informations publiques comportant des données à caractère personnel est subordonnée au respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés".*

[37] Commission Nationale Informatique et Libertés (http://www.cnil.fr/).

[38] See the CNIL's «*Déliberation n°2010-460 du 9 décembre 2010 portant recommendation relative aux conditions de réutilisation des données à caractère personnel contenues dans des documents d'archives publiques»* (available on : http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/250/).

[39] In French: "*mentions apposées en marge des actes de l'état civil*".

their demand is "justified";

- the necessity of implementing further security and confidentiality measures when an indexing is done: for instance, search engines' indexing shall be impossible for personal data of people born less than 120 years (and the CNIL has the right to impose further conditions if necessary);
- the necessity of addressing a prior demand of authorization or opinion to the CNIL (Article 36 of the Data Protection Law), except when the formal consent of data subject has been obtained: especially when there are cross-border flows of personal data with subcontractors outside the UE and when there are possibilities of interconnexion between public archives and other files (Art. 25, 5° of the Data Protection Law). The CNIL could also use its powers of control *a posteriori* to verify whether such guarantees are followed.

In France there is also another independent administrative authority - the CADA[40] - that deals with access and re-use of public documents: it is interesting to notice that in some cases, when personal data are at stake, the CADA refers the claimant to the CNIL's opinion on that matter, in order to be consistent with the French Data Protection Law[41].

Germany (*By Clarissa OTTO)*

The PSI Directive has been implemented into German legal framework. The Re-use of Public-Sector Information Act (*Informationsweiterverwendungsgesetz*, IWG) came into effect on 19 December 2006. The IWG is a Federal law, which has effect upon Federal authorities (*Bund*), Federal State authorities (*Länder*) and municipal bodies in the same way.

Regarding the topic of personal data, Article 1 (3) of the IWG states that:

> "*Provisions on the protection of personal data laid down by other legislative acts governing the re-use of public-sector information or more extensive rights conferred by such legislative acts shall not be affected*".

The re-use of public documents that contain personal data is not standardized uniformly in Germany. Instead, the Federal State data protection laws (*Landesdatenschutzgesetze*) and a number of special administrative laws standardize how the public sector bodies have to deal with those documents. Also, Article 1 of the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) states that:

> *"(1) The purpose of this Act is to protect individuals against infringement of their right to privacy as the result of the handling of their personal data.*
>
> *(2) This Act shall apply to the collection, processing and use of personal data by*
>
> *1) public bodies of the Federation,*
>
> *2) public bodies of the Länder, where data protection is not covered by Land legislation and where the Länder*
>
> *a) execute federal law, or*
>
> *b) act as judiciary bodies and administrative matters are not involved,*

[40] Commission d'accès aux documents administratifs (http://www.cada.fr/).
[41] See http://www.cada.fr/les-informations-a-caractere-personnel,6125.html.

3) private bodies

that collect data for use in data processing systems, or use such systems to process or use data, or collect data in or from non-automated filing systems, or use such systems to process or use data, unless the data are collected, processed or used solely for personal or domestic activities.

(3) Where other federal laws apply to personal data and their publication, they shall take precedence over the provisions of this Act. The obligation to abide by legal obligations of secrecy or professional or special official secrecy not based on law shall remain unaffected.

(4) The provisions of this Act shall take precedence over those of the Administrative Procedures Act where personal data are processed in ascertaining the facts.

(5) This Act shall not apply in so far as a controller located in another European Union Member State or another state party to the Agreement on the European Economic Area collects, processes or uses personal data inside the country, except where such collection, processing or use is carried out by a branch inside the country. This Act shall apply in so far as a controller not located in a European Union Member State or other state party to the Agreement on the European Economic Area collects, processes or uses personal data inside the country. In so far as the controller is to be named under this Act, information on representatives located inside the country shall also be furnished. Sentences 2 and 3 shall not apply where data storage media are used solely for the purpose of transit through the country. Section 38 (1) first sentence shall remain unaffected."

Czech Republic (*By Radim POLČÁK)*

In the Czech Republic, the PSI Directive has been transposed into the Freedom of Information Act (Act No. 106/1999 Sb.). Technically, the transposition added only one Article that deals with licensing of PSI for re-use, while all other regulatory framework of PSI re-use, including its relation to data protection, is being used from the Freedom of Information Act.

Similarly to that, all related case law is not primarily on the re-use, but rather on access rights with respect to personal data.

The Act No. 106/1999 Sb. provides for priority of protection of personal data and privacy over access rights. It means that whenever it is technically possible, public sector information containing personal data is anonymised. The only exception is the case where the individual (data subject) is a beneficiary of public funding.

Upon this provision, Courts have recently decided upon a couple of cases of access to public sector information regarding wages of high ranking employees of the State (they were first provided anonymised what courts found insufficient pursuant to the exception laid down in Art. 8b of the Act).

Italy *(By Eleonora BASSI)*

The PSI Directive has been implemented into Italian legislation by *D. Lgs. 36/2006* (modified by *L. 96/2010*). Regarding the re-use of personal data, the Italian PSI Decree refers to the Italian Privacy legislation (*D. Lgs. 196/2003, Codice della Privacy*[42]), which contains data protection safeguards. This means that Italian legislation has no specific rules for the re-use of personal data.

Indeed, for this reason, the case law on the re-use of personal data is not primarily based on the re-

[42] See Decreto Legislativo 30 giugno 2003, n. 196, "*Codice in materia di protezione dei dati personali*", Gazzetta Ufficiale n. 174 del 29 luglio 2003 - Supplemento Ordinario n. 123.

use legislation, but rather on the legitimacy of the processing (re-using) personal data, according to the data protection legislation.

Nevertheless, the Italian Data Protection Authority – *il Garante per la Protezione dei Dati Personali*[43] - decided upon several cases concerning the re-use of PSI containing personal data. The *Garante* pointed out the most crucial principles and rules of data protection legislation for lawful re-use of personal data: the principle of data quality[44], the principle of data subject consent, the crucial role of the information concerning the data processing to the data subject.

By the Provision adopted on 13th May 2008 (*doc. Web 1521775*), the *Garante* stated that the commercial re-use of personal data of public databases by a private company is prohibited if the information concerning the data processing is not provided to data subjects (Art. 13, c. 4, Italian Privacy Code, and also Art. 10 (c), Dir. 95/46/EC).

In Italy, providing general information towards data subjects is only allowed after an exemption by the Garante from the obligation of individual information[45]. In this regard, by the Provision adopted on 26th March 2010 (doc. web 1721169), the Garante stated that the commercial re-use of personal data, extracted from the public databases of the Public Education Office, is allowed according to D. Lgs. 36/2006 on the re-use of public sector information. Moreover, it is not required to inform all data subjects individually on the data processing, considering the disproportionate use of resources this would entail. A private company acquired non-sensitive personal data relating to teachers, enrolled in the lists for the inclusion in the public education regular staff (name, surname, date and province of birth, teacher identification number, ranking, scores, etc.), extracting them from documents available on the websites of the Italian provincial education offices, which were freely accessible (and therefore available without the data subject consent, according to art. 24, §1, c) of the Italian Privacy Code), in order to re-use them for commercial purposes. The re-user provided an online commercial service addressed to temporary teachers with the desire of better understanding their real job opportunities related to their ranking within various provincial public education offices. The re-user asked to be exempted from the individual information release on the data processing to each teacher, considering the disproportionate use of resources this would require. After evaluating "the undeniable social utility" of the project, and referring to the Italian law on the re-use of public sector information (D.Lgs. 36/2006), the Garante exempted the re-user from the duty to individually inform the data subjects, with the sole condition of providing an online publication of the appropriate information on the personal data processing.

The Netherlands (*By Bart VAN DER SLOOT)*

The Dutch implementation of the PSI-Directive is to be found in the '*Wet Openbaarheid Bestuur*' (Law on Governmental Transparency).

In Chapter V of the law with the title "Exceptions and Limitations", Article 10 §1 sub d holds that the dissemination of information may be omitted when it regards personal data (for the definition reference is made to the Dutch implementation of the Data Protection Directive, the '*Wet bescherming persoonsgegevens*' (Law on the protection of personal data)), unless there is no infringement on the personal sphere/life.

Interestingly, the limitation regards privacy rather than data protection infringements.

Article 10 §2 sub e holds that the dissemination of information may also be omitted when the

[43] See more information on Italian NDA website: http://www.garanteprivacy.it/garante/navig/jsp/index.jsp

[44] By the Decision adopted on 5th June 2008 (*doc. Web 1535726*), the Italian Data Protection Authority ruled on a case of re-use of personal data extracted from public records concerning mortgages and foreclosures, and stated that data must be complete, accurate and updated in accordance with the principle of data quality pursuant Art. 11, §1, c) and d) of the Italian Privacy Code.

[45] See the Provision adopted on 26th March 2010.

interest it serves is not proportional in relation to the interest of the protection of the private sphere/life.

Slovenia *(by Polona TEPINA)*

Slovenia transposed the PSI Directive in the Access to Public Information Act, making a clear bond between the access to public information and the re-use of such information. Information, intended for re-use, is subject to the same eleven exemptions as information in the regime of access to information. One of these exemptions is protection of personal data, where a reference to Personal Data Protection Act is made.

Paragraph 6, Article 6 of the Access to Public Information Act states, *inter alia*, that the applicant's request to re-use information is denied if the request relates to:

1) Any of the exemption from free access to information in accordance with Paragraph 1, Art. 6 of the Access to Public Information Act (e.g. personal data protection exemption);
2) Information, for which another Act stipulates accessibility only to authorized persons.

In Slovenian data protection legislation, personal data can be processed by the public sector only if the processing of personal data and the personal data being processed are provided by statute or if the statute provides that certain personal data may only be processed on the basis of personal consent of the individual.

Most common legal basis for accessing (and therefore also re-using) of personal data are:

- Statutes that prescribe publicity of personal data, e.g. public registers (e.g. land register, etc.).
- Legal basis in the Access to Public Information Act itself – regardless of exemptions to free access and re-use, information relating to the use of public funds, the execution of public functions or employment relationship of the civil servant, is considered public.
- One possible legal basis is also in the Personal Data Protection Act regarding processing of personal data for historical, statistical and scientific-research purposes, whereas the user of such information may only receive data in an anonymised form (unless the individuals give their consent).

The Slovenian regulatory body - *the Information Commissioner* - which is an appeal body, issued around 19 decisions regarding re-use of PSI.

In three cases the question of re-use of personal data was posed:

1. A list of apple and vegetable growers held by the Ministry of Agriculture, Forestry and Food (Decision No. 021-35/2005/3, 18 July 2005):

> The applicant requested a list of apple and vegetable growers from the Ministry of Agriculture, Forestry and Food and specified he intended to use it for commercial re-use (for possible business cooperation). The body rejected the applicant's request due to personal data protection exemption.
>
> However, *the Information Commissioner* referred the case back to the first instance body for a new procedure and decision. The body did not take into consideration that the register of apple and vegetable growers does not comprise only data of natural persons, but also of legal persons, which - by definition - do not enjoy the protection of personal data.

In the new procedure, the body should consider that the Agriculture Act, which states that the data from registers is public, foresees an exception for personal data and trade secrets.

2. A list of substitute child support recipients held by the Public Guarantee and Maintenance Fund (Decision No. 021-77/2005/5, 17 October 2005):

The applicant's request and appeal for a list of all the recipients of the substitute alimony (child support) from the Public Guarantee and Alimony Fund of the Republic of Slovenia were denied due to personal data protection. The Fund pays the alimony when liable persons (mostly parents) fail to comply with this responsibility and then recover the fee from the liable person.

The Commissioner observed that the requested list comprised many personal data about children, recipients of substitute alimony (including personal ID number, address), their statutory representatives and persons, liable for paying the alimony.

The Commissioner warned that the principle of proportionality was at stake. This principle is established in the Personal Data Protection Act, which states that the processed personal data must be adequate and in their extent appropriate in relation to the purposes for which they are collected and further processed. There is no legal basis for revealing personal data from the list, so the exemption of personal data protection from Point 3., §1 of Art. 6 of the Access to Public Information Act apply and re-use cannot be granted. Also, the Guarantee and Alimony Fund of the Republic of Slovenia Act states that transmission of personal data to other users may only be granted if the users are authorised by the law or with the individual's consent.

3. Register of foster carers held by Ministry of Labour, Family and Social Affairs (Decision No. 021-92/2005/18, 2 February 2006):

The request and appeal for re-use of register of foster carers was denied due to data protection. The register contains personal data of foster carers, such as name, surname, personal ID number and address. The Commissioner warned also that indirect identification of foster children, placed with a foster family, is possible if name and address of foster carers is revealed, which would represent a serious breach of the child's privacy and dignity.

Spain (*By Manuel FERNÁNDEZ SALMERÓN and Julián VALERO-TORRIJOS)*

Spanish PSI Act (*Ley 37/2007*) transposing PSI Directive includes a generic referral to the specific legislation of the right to the protection of personal data (*Ley Orgánica 15/1999*) for the re-use of documents containing personal information.

Thus, Act 37/2007 does not directly forbid the re-use of such documents, although it sets up hard penalties if those documents are re-used causing serious damage to this fundamental right (Article 11.5, Act 37/2007).

The statutory development of this Act (Royal Decree 1495/2011) is more specific, stating that:

"1. Access to documents containing personal data or private information shall be reserved to the persons such data or information are about, who shall also be able to exercise the right to change, cancel or oppose their personal data in accordance with the personal data protection laws and Article 37.2 of Law 30/1992, of November 26. [...]

2. However, when technical and economic means make it possible, data dissociation procedures shall be applied under the terms derived from the provisions in Article 3.f of

Organic Law 15/1999, of December 13, on personal data protection, and Article 5.1.e of Royal Decree 1720/2007, of December 21, approving said law's enforcement regulations, so that the information can be re-used by other persons".

The most recent regulation passed on this issue is the Regulation 3/2010, adopted by the Supreme Council of the Judicial Power (October 28, 2010) about re-use of judgments and other judicial decisions. Its Article 5 only states that:

"6. The recipients of licenses shall be entitled: [...] b) that the information will be delivered in electronic files, properly treated, homogenized and with its personal data removed".

However, this provision has been recently overruled by the Spanish Supreme Court[46] arguing that the wide powers of self-organization conferred to that Council do not justify the interference of this body in the exercise of powers assigned by the Spanish Constitution to State central institutions. Therefore, according to the Supreme Court decision, the PSI Act should have been specified by the national Government even in this field.

4 Interests protected under the current legal framework

The former wording of the PSI Directive suggested that the respect of data protection rules is important when developing a market for the re-use of PSI containing personal data. The new proposal for amending the PSI Directive does not change this matter of fact.

Indeed, in their quality of data controllers, **public bodies have to respect all the obligations and principles imposed by the Data Protection Directive** that is still in force[47], 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 limitation 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)[48],
- a "time of conservation" (**retention period**) 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[49] linked to the re-use) in case the re-use of personal data would be allowed, and should be subject to all obligations and rights of the data protection legislation.

[46] See more information on: http://www.lapsi-project.eu/esruling

[47] See chapter 6 below, as regards the on-going review of Data Protection Directive.

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

[49] 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*".

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

- Obtaining an **unambiguous consent of data subjects**, 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
- Proving the necessity for **compliance with a legal obligation** to which the controller is subject[50], or
- Proving the 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**[51] or in the **exercise of official authority** vested in the controller or in a third party to whom the data are disclosed, or
- Proving the necessity for the purposes of the **legitimate interests[52] pursued by the controller or by the third party** or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1) [of Data Protection Directive].

There are **also special categories of data, 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 (the so-called "sensitive data"). The processing of such data is only permitted in certain cases corresponding to the limited admitted exceptions of paragraphs 2 to 5 of the same Article.

Furthermore, it has to be taken 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 should make more references to these obligations in different articles, as for instance on:

- **Article 7 on transparency**, which recommends that "*any applicable conditions (...) shall be pre-established and published*", **should suggest the establishment of a clear and (when possible) specific "privacy policy" or "information document" by PSI holders**.
- **Article 8 about licences**, that states that "*public sector bodies (...) may impose conditions, where appropriate through a licence, dealing with relevant issues (...)*", **should remind the respect of privacy principles and obligations in a specific clause** (e.g. lawfulness of data processing, proportionality and purpose principles, time of conservation, necessity to inform

[50] 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 Member States (e.g. in Civil Law systems).

[51] *Ibidem.*

[52] This legal ground 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 data controller and of the data subject) that will determine the legitimacy of the data processing concerned. However, in this regard we could face different approaches or interpretations by Member States, which would again mean that the harmonisation is incomplete and cross-border re-use hindered.

about the data controller, the recipients of the data, etc), **when a licence is established by a public body**.

5 Legal Problems

5.1. Rules exist but are unclear: A need to clarify rules

As it was stressed before, the PSI Directive makes clear reference to the Data Protection legislation. However, addressing problems that arise from the re-use of PSI containing personal data has been a great opportunity not so much for modifying the PSI Directive on specific points, but mainly 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. **The outcome of such a debate could be introduced into the general approach of the PSI Directive.**

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

a) For some of us, **a stronger effort should be made to establish the differences** (which are clear from a theoretical perspective but increasingly confused in practise) **between**:

- **Access to public information**[53],
- **Access to personal data**[54], and
- **Access to PSI for re-use purposes**[55].

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.

b) 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[56]), but it could not be enough to avoid further identification of individuals (e.g. some kinds of geographic information combined with other data could allow specific identification of people).

Anonymisation is a more technical problem and a functional concept. **A legislator** cannot strictly state what anonymisation is (in a technical sense) and how it should be realized, but **should require it** (or a specific kind of it), for instance, **for specific categories of personal data**[57].

---

[53] This is provided by the national Freedom of Information (FOI) Acts.

[54] This should fall under the provisions of the data protection legislation (data protection national laws transposing the Data Protection Directive).

[55] This is provided by the national laws transposing the PSI Directive, referring to Data Protection laws when PSI contains personal data.

[56] In fact, Recital (26) of Data Protection Directive states that: "*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 reasonably 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; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible*".

[57] For instance, 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 processing of such data (including the re-use), but not as a necessary condition for the re-use (as it is done by some Member States PSI legislation), as it goes beyond the rules that the data protection legislation imposes[58].

It should also be considered that Article 29 Working Party[59] has clarified that "*anonymisation must be completely irreversible for the Data Protection Directive to no longer apply*"[60].

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.

c) From our viewpoint, **the Article 29 Working Party is the "right arena" (hereinafter 'Art. 29 WP') to discuss such questions**, as it deals with **ensuring uniform interpretation of the Directive** between the national data protection authorities (NDAs) of different Member States.

In fact, this is a question of application of data protection principles to practice, which is still fairly new, i.e. the re-use of PSI. Therefore, the Article 29 Working Party could allow a discussion grouped around this theme, leading to harmonized interpretations of what are the data protection requirements in the context of re-use.

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[61] delivered in 2003. This working paper has already stressed some key points, 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 a question of 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).

[58] Indeed, the processing of personal data is not forbidden by the data protection legislation, even for the public bodies, but it should be processed following the respect of different principles (mentioned above).

[59] 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

[60] See Article 29 Working Party, *Opinion 1/2008 on data protection issues related to search engines*, WP 148 adopted on 4 April 2008, §5.3, p. 20.

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

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 (...)*". Therefore, such wording could lead to a kind of "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 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 increased 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"). Conversely, there are also national restrictions to the re-use of personal data and there could be hardly any room for public bodies to perform such assessment, when data protection rules are clear [62].

Then, we could consider that **some "general assessments" should be made by the Art. 29 Working Party at the pan-European level**[63]**) and, preferably, in collaboration with the PSI Group**[64].

Therefore, the "case-by-case assessments" should be made by each national data protection authority (NDAs) in order to take into account national legal specificities and special categories of personal data for certain kinds of re-use. **More communication** on such specific national "case law" should also be provided between NDAs within the Art. 29 WP "arena", and also towards potential re-users, to favour more cross-border re-use.

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

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

[62] For instance, in Slovenia, data protection exemption for access and re-use is absolute (it is not a relative exemption).

[63] Indeed, Article 29 WP is composed by a member of each NDA and by the European Data Protection Supervisor – the EDPS (who is the data protection authority for the EU institutions), this should favour a better "harmonisation" of solutions or, at least, a great consensus on the specific solutions adopted by each other (and the exchange of "best practices" solutions).

[64] 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

In principle, re-users are not obliged to justify why they require the data, but in the 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[65], 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 or historical 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 principle of proportionality when re-use of personal data is allowed?***

Prior information of the PSI holder ("first data controller") to data subjects about the purpose of data processing in case of the re-use is also an essential requirement in order to know whether the principle of proportionality is respected (such respect could be controlled either by the first collector/"owner" of the data – the public authority, or by the NDAs – when the notification of the re-use processing is done[66], or even by the data subject himself, for instance).

As mentioned before, this principle imposes that personal data processing "*must be adequate, relevant and not excessive for the purposes for which they are collected and/or further processed"* (Article 6 (c) of Data Protection Directive).

- ***How to respect the obligation of the information of data subjects: should it be "individual" or could it be only "general"[67]?***

This obligation could be respected by the public body by providing a clear "privacy policy" in its website, which could give the information of the possibility of re-use of the data processed. This information could be, if appropriate in a Member State, implemented as a complementary measure of the previous "assessment" done by each NDA, for instance.

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[68].

- ***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?***

Could it be possible to provide a kind of "opt-in"[69] system by the way of the public body website,

[65] First, when they make the request of re-use before the PSI holder/public administration body, but also when the data have not been directly obtained from data subjects: the "new" data controller (the re-user) should also provide information to the data subjects, except when "*the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law*" (see Article 11 of Data Protection Directive).

[66] Following the provisions of Article 18 of Data Protection Directive, there is an obligation to notify the supervisory authority (NDA) "*before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes*". Such notification must content specific details including, between others, "*the purpose or purposes of the processing*" (Article 19 (1) (b) of Data Protection Directive).

[67] See the Italian example provided above (chapter 4).

[68] As it is imposed by the provisions of Article 11 of Data Protection Directive (see above).

[69] Some LAPSI partners doubt that an "opt-out" system (which is opposite to prior consent – opt-in) could be considered as a possibility in this case: opt-out could only be possible if there is a legal basis for processing (re-using) in the first place and then the individual would have the possibility to forbid the processing of its personal data.

for instance, or by obtaining this consent (preferably in writing) at the moment of the first collection of the data (when possible)?

However, we have to warn that probably not all national legislations would allow public sector to transmit personal data to re-users on the basis of personal consent[70].

Public sector databases and registries could also include a kind of technical system that would 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. This solution should meet the national legislations that already impose total anonymisation of identities (e.g. Belgium), but the questions still remain whether it is technically feasible and would it allow a kind of "interoperability" between systems.

These two examples of privacy by design could be completed or changed by other tools following the "sensitivity" of the personal data concerned. Such an assessment should be, as mentioned before, first done by Art. 29 WP and then, possibly, by NDAs in order to meet all national legal specificities.

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

As mentioned before, the system of licences provided by Article 8 of 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 in France) and/or for re-use of PSI (as the authority of "appeal" of re-use of PSI practices, like in Belgium), therefore both authorities should collaborate in order to avoid disparities of solutions and opinions[71]. In other Member States, as in Slovenia, the PSI Directive has been implemented in the Access to Information Act, where there is only one "supervisory authority" competent for both access and re-use complaints (and for personal data protection as well).

5.2. Rules exist but are not functioning: A need to change rules

Our main objective, within the LAPSI WG2 network, is to rightly determine the requirements that are imposed by data protection and privacy rules on the re-use of PSI and to identify possible problems that such requirements could cause.

On the one hand, data protection rules should not be used as a "mere excuse" by public bodies to excessively restrict the re-use of PSI (when it implies personal data), when there is a legal basis for processing of personal data. On the other hand, we have to take into account situations where data protection provisions are necessary and welcome to protect individuals' rights in the wide information content market.

In this project, our aim was to address the impact data protection rules may have on the re-use of PSI and identify possible problems (like excessive blocking solution in Belgium for example) and large differences in interpretation of these requirements by authorities –in different Member States.

All this led us to propose that finding a solution at European level to reduce these differences is crucial for the development of the re-use market.

---

[70] Slovenia did not have such a case, but it is questionable if this would be allowed, because processing of personal data on the basis of personal consent in public sector is very limited.

[71] Or maybe the "access supervisory authority" should refer the case to the "data protection authority/NDA" when personal data are at stake, to avoid discrepancies of decisions/opinions (as in France, for instance, in the case of re-use of personal data of public registries – see the CNIL's Recommendation quoted before).

Changing PSI Directive provisions regarding data protection issues is not the only solution: 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 also consider the role of National Data Protection Authorities at national level, which could play an important role of advisors and/or regulators when there is a need to re-use personal data.

5.3. Rules are changing: In what way?

One crucial point that we have already stressed is that the Data Protection Directive and PSI Directive are under review process since the end of 2011, and **it would be important to associate both revisions** in this field.

Unfortunately, it seems that it is not the case, as we can see on last versions issued by European Commission that still circulate for review:

- **On 12 December 2011 the European Commission has issued a proposal to review the PSI Directive**[72] within its 'Open Data Strategy for Europe'[73] Policy. The new version of the PSI Directive proposed changes about the subject matter and the scope of the Directive[74], about a new "general principle" in the sense that a "right of re-use" of PSI has been created (under certain conditions), etc.

However, **no improvements on data protection issues have been proposed and articles on that matter have not been changed, improved or clarified at all**.

- **On 25 January 2012, the European Commission launched a proposal for a "General Data Protection Regulation"**[75] in order to replace the Data Protection Directive in force since 1995. This paper does not want to do a specific analysis of the entire proposal, but aims to begin a discussion on issues related to the re-use of PSI. Then, despite the fact that the European legal framework on data protection would become more binding for the Member States[76], **such proposal still does not tackle the "re-use of PSI" issue**.

In fact, new definitions and principles have been introduced or specified (such as the data minimisation principle[77], the transparency principle[78], the principle of accountability[79], etc), further

[72] European Commission, *Proposal for a Directive of the European Parliament and of the Council Amending Directive 2003/98/EC on re-use of public sector information*, *op. cit*.

[73] European Commission, *Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Open data: an engine for innovation, growth and transparent governance*, COM(2011)882 final.

[74] For a deeper analysis of this proposal see: JANSSEN K., European Public Sector Information Platform, *Topic Report No. 2012 / 3: The amendment of the PSIdirective: where are we heading?*, published on April 2012.

[75] European Commission, *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)*, Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD).

[76] Instead of several national laws to transpose the Data Protection Directive, there should be only one Regulation with the same provisions for all, which would avoid disparities between legal frameworks on one hand, but would increase "tensions" between Member States as their national specificities would not be taken into account, on the other.

[77] See new Article 5 of the Data Protection Regulation.

[78] E.g. new Article 11 which introduces the obligation on controllers to provide "transparent and easily accessible and understandable information", inspired in particular by the Madrid Resolution on international standards on the protection of personal data and privacy (adopted by the International Conference of Data Protection and Privacy Commissioners on 5 November 2009).

[79] New article 22 takes account of the debate on a "principle of accountability" and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance (see explanations of page 10 of the Data Protection Regulation).

conditions have been established (for consent to be valid as a legal ground for lawful processing, or the controller's information obligations towards the data subject), and new «actors» have been created (such as the data protection officers[80], the new European Data Protection Board which would replace the Art. 29 WP[81], etc).

However, the process of revision is on-going and it is unclear which further changes could be introduced by the new General Data Protection Regulation or another legal instrument in its place.

- Finally, **on 18 April 2012, the European Data Protection Supervisor (EDPS) issued a new Opinion on the "Open-Data Package" including the Proposal amending the PSI Directive**[82]. This document has quoted the work done by the LAPSI WG2 in the previous version of our policy recommendation and has raised further issues that this Recommendation did not take into account due to the fact that the process of developing this Recommendation has begun in 2010.

Therefore, **we recommend that the European Commission, in a new version of the proposal for amending PSI Directive, should refer more to the EDPS opinion as it tackles different problems raised by the new version of the Directive**.

In particular, the Commission should take into account that the new "right of re-use" principle would increase data protection issues even more.

Hereafter, **we outline the EDPS recommendations that should be**, in the opinion of LAPSI WG2, **especially taken into account by the European Commission and the reviewers of the PSI Directive**:

- **The applicability of the principle of re-use of personal data should be clarified and made subject to additional conditions**: the EDPS recommends, among others, that the new Article 1(2)(c) should be amended and that the notion of 'protection of privacy and personal data' should be specifically mentioned among the examples of possible grounds for exclusions from access regimes (point 36, p. 7).

The EDPS also recommends that the Proposal should specify that **before a public sector body makes personal data available for the re-use, it should carry out an assessment (also called «data protection impact assessment»)** to decide whether the personal data involved can be made available for re-use (Point 40).

- On the **partially anonymized and/or aggregate data**: the EDPS stresses that they may also include personal data, therefore **adequate levels of anonymisation should be ensured**, unless the previous data protection impact assessment has established that the personal data may be made available (Points 43 to 46).

Moreover, the EDPS stressed that **an exception for costs of anonymisation should be taken into account in the article on charges** (Points 61 to 65)[83].

- **On « licensing »**: the EDPS refers to our idea and stresses that **a data protection clause should be included in the license terms, when available**, and that the re-user should

[80] See new Article 35 of the Data Protection Regulation.

[81] See new Article 64.

[82] EDPS, *Opinion 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*, 18 April 2012.

[83] This issue has been also addressed by the LAPSI Working Group 01 in its "*Policy recommendations as to the competitive issues that the re-use of PSI raises*" (also available on LAPSI wiki website: http://www.lapsi-project.eu/materials#4

demonstrate how the risks are addressed and that (binding) purposes for re-use should be clearly mentioned in such a license (Points 49 to 56).

EDPS, as our paper, also refers to the Art. 29 WP as the right actor to obtain further guidance on anonymisation and licensing (Points 66 and 67) and regrets that « *he has not been consulted on the draft Decision before its adoption* » by the European Commission.

We warmly recommend to the European Commission to consider this EDPS Opinion as well as our policy paper before adopting a new revised version of the PSI Directive, in order to improve the respect of the data protection principles in the re-use of PSI market.

6 Arguments in favour of (v.) and related counter-argument

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

- Nevertheless, the practice shows that it is not enough to avoid bad harmonisation of solutions between different public bodies and Member States.
- 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. They could be simplified when the new data protection rules will be in force, however **only the practice will show us whether the changes will be for the better or for the worse**.
- **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**. We warmly recommend to the Commission to consider this advice, even more in the light of the recommendations issued by the EDPS.
- **Making more references to such rules in other articles of the PSI Directive could be enough to clearly remind which actors are concerned by interpretation of both directives** (Art. 29 WP, NDA'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.

However, as stressed before, **simple solutions could be found in the review of Articles 7 (transparency) and 8 (licences) of PSI Directive, with further references (e.g. a new paragraph) to the obligation of information of data subjects** (when their personal data are requested for the re-use), **a clear determination of the responsibility of each "actor"** (data controller and data processor obligations, rights of data subject, obligation to notify the data processing to NDAs, when there are transfers of personal data to third countries, etc), **clear references to data protection principles, the levels of anonymisation or not required, and the purposes for re-use that are allowed** (and under what conditions).

The EDPS Opinion deeply analysed those issues, so we recommend to the European Commission to take his Opinion into account.

Finally, **an additional reference should be made (e.g. by a new article) as regards the existence of NDAs and/or other "supervisory authorities" that already monitor data protection and privacy issues and/or the implementation of other rules** (e.g. competition authorities, access authorities, etc), **and their existence should be taken into account if a new re-use of PSI authority would be created** (as it seems to be the case in the proposal). At least, **the proposal should include a specific clause that deals with the "collaboration"/cooperation between those authorities.**

As we can see, **the proposal for amending the PSI Directive seems to increase the existing problems in this matter and a deeper analysis should be made by the European Commission before implementing it.**

7 Arguments against (vii.) and related counter-argument[84]

Re-using public sector information may trigger the use of data protection laws when the re-use 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 four major categories of obligations in the Data Protection Directive: firstly, the proper legal basis for processing of personal data, secondly, required legitimate purpose, thirdly, respecting the safeguards embedded in the Directive and finally, respecting the rights of data subjects in connection with the transparency principle.

It will be difficult for the re-user to demonstrate a legitimate legal basis 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 basis 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.

Along with the obligation to prove legitimate legal basis for data processing, the Directive includes several data protection 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

[84] See, for more comprehension of this point: 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. This opinion does not reflect the overall opinion of the other WG2 members.

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 public sector bodies will usually gather personal data in relation to serving the public interest, security matters or legal obligations, it will often prove difficult for re-users 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 public sector body disseminating public sector information to third parties needs to see to it that every data subject is adequately informed on 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 data subjects.

All four 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[85].

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[86]. 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 basis, 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. However, as it was stated above, some national legislations currently prevent transmitting personal data to re-users on the basis of consent of data subjects.

8 If possible: what is heavier between (v.) and (vii.)?

It is submitted[87] that the last solution (vii.) would be virtually impossible to implement at this stage. Indeed, it does not answer some new questions that arise:

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

ii. 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)[88]?

iii. How to overcome the lack of "digital literacy" of some citizens, as well as all educational

[85] Some other partners do not agree that anonymised data is totally useless: for instance, if we look only at the case of re-use of court judgments, they are all anonymised, but still re-using of judgments (alongside legal texts) creates quite a big information market, and there are many other cases.

[86] As stated above, national legislations might prevent transmitting personal data to re-users only on the basis of consent of data subjects.

[87] For the core group of WG2 members, this last solution (vii.) is not heavier than v., and seems unfeasible within the current legal framework in almost all Member States. A member of the EDPS team, invited during the LAPSI 2nd Public Conference held in Brussels last 23-24 January 2012, has also strongly criticised it while he outlined our other main recommendations points.

[88] See, for instance, the Italian example above (Article 52, c. 1-bis of the CAD).

issues related with the “real” understanding of people as regards their privacy threats and the implications of “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 inform.