ARTICLE 29 DATA PROTECTION WORKING PARTY

1806/16/EN
WP 239

Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector

Adopted on 8 June 2016

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

1. **INTRODUCTION**

1.1 SCOPE OF THE OPINION

This Opinion explains how to apply the data protection principles to the processing and publication of personal data for transparency purposes in the public sector, in particular when related to anti-corruption measures and the management and prevention of conflicts of interest[1]. This opinion does not seek to address what information should be available via access to public documents/freedom of information legislation of the EU member states[2], does not limit the availability of such public information in accordance with national legislation, nor does it cover the implementation of Regulation 45/2001 and Regulation 1049/2001[3] applicable to EU institutions and bodies.

In general, it may be a requirement for public sector bodies to collect, register and store information about their activities and their staff and to make this information publically available, usually via their official website. This kind of processing is likely to involve processing of personal data, including disseminating it to the public.

This Opinion is addressed to national legislative authorities, national governments, offices or agencies and other competent institutions ("competent institutions") in the public sector dealing with anti-corruption, conflict of interest prevention measures and other transparency obligations, as well as data protection authorities. It makes recommendations based on a common understanding of the data protection framework in which such processing is carried out. Specifically, it addresses the general implementation of Directive 95/46/EC[4] and the General Data Protection Regulation (hereinafter: GDPR) principles and values.

Articles 1 and 4 of Directive 95/46/EC require that, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. Member States shall also ensure that the processing of personal data as part of anti-corruption measures aimed at managing potential conflicts of interest and any related transparency obligations are regulated by the national provisions they adopt pursuant to that Directive and in the light of the GDPR.

---

[1] Public sector - for purposes of this Opinion, public sector means the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law, and it is without prejudice to definitions set up in the legislation of the Member States.

[2] For information, see the WP29 published an Opinion 06/2013 on open data and public sector information ('PSI').

[3] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data and Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

[4] 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

1.2 PURPOSE OF THE OPINION

The aim of this Opinion is to provide practical guidance, recommendations and best practice examples for Member States' legislators and competent institutions on how they can ensure that the right to data protection is respected whilst at the same time balancing and satisfying the legitimate public interest in transparency where legislative and political initiatives on these matters require dissemination of information relating to a natural person. The notion of "transparency"[5] is linked with the principles of openness, good administration and good governance as enshrined in the Treaties[6] and in the Charter of Fundamental Rights of the European Union ('EU Charter')[7].

Impartiality, transparency and professional conduct amongst public sector subjects is recognized as key to ensuring excellence and quality in the performance of relevant public positions. There is a balance to be struck between public sector subjects' rights to data protection[8] on the one hand and the public interest in those individuals fulfilling their duties and responsibilities in a transparent way on the other. Publishing details about public sector subjects' private interests is part of a range of measures used to manage potential conflicts of interest and to increase accountability and public confidence. While legislations and regulations to manage conflicts of interest vary, this opinion advises on how to ensure equal levels of data protection for public sector subjects across Member States.

2. LEGAL FRAMEWORK

Article 7 of the EU Charter provides that everyone has the right to respect for his or her private and family life, home and communications. In addition, Article 8 of the Charter stipulates, among others, that everyone has the right to the protection of personal data concerning him or her. Personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Also, Article 8 of the European Convention on Human Rights (hereinafter: ECHR) states that everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with the exercise of this right, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

---

[5] This reference is without prejudice to the specific definitions set forth in national legislation and policies and it is provided exclusively with a view assisting understanding of this opinion.

[6] See Articles 10 and 11 of the Treaty on European Union and articles 15 and 298 of the Treaty on the functioning of European Union.

[7] See Articles 41 of the EU Charter.

[8] Data protection right has to be understood as rights to be protected by the Data protection Directive and GDPR.

Article 7 of Directive 95/46/EC provides the criteria for making data processing legitimate and sets out the basic personal data processing principles (Article 6 of the Directive 95/46/EC). The GDPR recitals specify that Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information 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 Union and national law.

According to Article 10 of the ECHR, everyone has the right to freedom of expression. The ECHR has, on several occasions, recognised that this right includes "the right of the public to be properly informed" and "the right to receive information" in cases relating not only to the media or to professional journalists[9].

In light of the aforementioned provisions, it is recommended that the following principles are considered when processing personal data in the context of conflict of interest measures and associated transparency.

3. PERSONAL DATA PROCESSING PRINCIPLES

Article 6 of Directive 95/46/EC stipulates that personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

The aforementioned requirements are in line with the equivalent provisions in the GDPR.

[9] However, until recently the ECtHR has stated that the freedom to receive information, as guaranteed by Article 10, could not be construed as imposing on a State a positive obligation to disseminate information or to disclose information to the public (see the cases of Leander v. Sweden (1987), Gaskin v. United Kingdom (1989), Guerra v. Italy (1998) and Sîrbu v. Moldova (2004)). Only in two recent cases, the Court seems to have advanced towards a broad interpretation of the notion of freedom of information (see the 2006 decision on the application's admissibility in the case of Sdruˇzeni Jihoˇceské Matky v. Czech Republic and the 2009 decision in the case of Társaság a Szabadságjogokért v. Hungary).

3.1 FAIR AND LAWFUL PROCESSING

The legal basis for processing personal data in the context of conflict of interest measures can be found in Article 7(c) of Directive 95/46/EC[10]. This states that personal data may be processed if the processing is necessary for compliance with a legal obligation to which the controller is subject. In this context, the processing must be determined by law [11]. The introduction of general and blanket provisions should be avoided, so that the controller would not have an undue degree of discretion on how to comply with the legal obligation[12].

In these circumstances, legislators have a duty to ensure that legal obligations balance the various interests involved. Indeed, legislation should be compatible with the right to private and family life and to the protection of personal data in accordance with Article 8 of the ECHR, and Articles 7 and 8 of the EU Charter[13]. This implies that the legal obligation to process personal data should be necessary and proportionate to the legitimate aims pursued and compliant with the purpose limitation principle .

Institutions may also be able to rely on Article 7(e) of Directive 95/46/EC as a basis for processing personal data in this context. When determining whether the processing operations comply with Article 7(e) and bearing in mind the various interests at stake, institutions need to be satisfied that:

- the processing activity is a task carried out in the public interest or it is conducted in the exercise of official authority[14];
- the processing operation is necessary for the performance of this task or for the exercise of this authority (i.e. such operations must be appropriate for attaining the objective pursued and not go beyond what is necessary to achieve it).

---

[10] For more detailed analysis see Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217. In some countries it may be possible to rely on Article 7 (f) as a basis for processing this type of personal data.

[11] In the Opinion 6/2014, the WP 29 acknowledged that for Article 7(c) to apply, the obligation must be imposed by law which has to fulfil all relevant conditions to make the obligation valid and binding. In that regard, the WP29 noted that „the legislation may in some cases set only a general objective, while more specific obligations are imposed at a different level, for instance, either in secondary legislation or by a binding decision of a public authority in a concrete case“. In that regard, recital 41 of GDPR clarifies that „Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned“. See also art. 6, par. 3 of GDPR.

[12] Ibidem

[13] See European Court of Justice 20 May 2003, Rundfunk, Joined Cases C-465/00, C-138/01 and C-139/01 and 9 November 2010, Volker und Markus Schecke, Joined Cases C-92/09 and C-93/09

[14] As the WP 29 emphasised in Opinion 6/2014, the public task or the official authority should be based on, or derived from, a legal provision. See Section III, par. 2.5, as well as recital 41 and Article 6 par. 3 of GDPR.

EXAMPLE: The indexation[15] of the personal data provided on a transparency platform, to allow citizens to search into it, would be considered a necessary operation. Indexation of identity data for an external search engine would not be considered necessary, by default, to achieve the transparency purpose.

3.2 PROPORTIONALITY, MINIMISATION AND DATA QUALITY PRINCIPLES

To implement these principles, first of all it is necessary to determine the main purposes of the data processing. For instance, transparency initiatives may be intended to foster wide-spread knowledge about the decisions and actions of government and its administrative bodies, offering basic insights into their processes, operations and personnel. In turn, this allows the public to hold governments to account about the ways in which they perform tasks and manage public resources, thus promoting efficiency and effectiveness. The measures addressed in this Opinion aim to prevent, detect and sanction conflicts of interest, with a view to avoiding the influence of private interests on the exercise of public duties and to strengthen the integrity, objectivity, impartiality of public sector subjects, as well as build up the confidence of citizens in Government.

EXAMPLE: The role of the competent institutions is to determine the value of assets the public sector subject had at the beginning and the end of his/her term of office and to identify how these assets were funded. To achieve this it may be necessary to collect information about spouses and relatives and their assets. However it does not necessarily follow that it is appropriate or proportionate to make all of this information publicly available online. Any incursion in the individual's private life should be necessary and proportionate to the legitimate purpose of the processing.

3.2.1 PROPORTIONALITY

The proportionality principle should be respected during each processing activity and especially at the stage of collection and any subsequent publication.

The European Court of Justice (hereinafter: ECJ) has highlighted the importance of a proportionate approach to processing personal data in several cases. In the aforementioned joined cases C-465/00, C-138/01 and 139/01, the ECJ approached this point by asking, "*whether stating the names of the persons concerned in relation to the income received is proportionate to the legitimate aim pursued and whether the reasons relied on before the Court to justify such disclosure appear relevant and sufficient*" (paragraph 86), and emphasised that the competent national courts should, "*ascertain whether such publicity is both necessary and proportionate to the aim (...), and in particular to examine whether such an objective could not have been attained equally effectively by transmitting the information as to names to the monitoring bodies alone*" (paragraph 88). Furthermore the ECJ asked

[15] Definition of indexation :

whether alternative ways to attain the legitimate aim pursued, that were likely to affect the privacy of the individuals concerned to a lesser extent, would have been feasible[16].

Moreover, in paragraph 74 of the aforementioned joined cases C‑92/09 and C‑93/09, the ECJ clearly stated that, "*it is settled case-law that the principle of proportionality, which is one of the general principles of European Union law, requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it (Case C‑58/08 Vodafone and Others [2010] ECR I‑0000, paragraph 51 and the case-law cited).*

Member States should carefully consider the scope of individuals covered by conflict of interest and transparency measures. When determining whose data is going to be processed Member States may wish to draw up relevant objective criteria such as an individual's public power, ability to spend or allocate public money, salary, term of mandate, received benefits, etc. bearing in mind that processing should not go beyond what is, "*necessary for achieving the legitimate aims pursued, having regard in particular to the interference with the rights guaranteed by Articles 7 and 8 of the Charter resulting from such publication*"[17].

On-line publication of information that reveals irrelevant aspects of an individual's private life is not justified in light of the principles of fairness and proportionality.

- Implementing proportionality:
  - *Differences between collecting and on-line publishing of data*

Conflict of interest measures generally cover two main processing activities: the exclusive non-public processing of personal data within the competent institutions and on-line publication of certain data. Relevant legal provisions should explicitly provide which individuals are obliged to submit reports to the competent institutions. They should also specify which personal data the reports need to contain and which personal data should be proactively published. This Opinion does not attempt to determine what personal data should be collected by the competent institutions dealing with conflict of interest measures, nor does it seek to define what information should be disseminated on-line. However, it is appropriate to highlight that, when deciding whether to make information publicly available on-line, competent institutions should always bear in mind the consequences of doing so. Some of the personal data collected may constitute intimate information about the public sector subjects and consequently its on-line publication may have a serious effect on their private lives and data protection rights. It is also relevant to note that what is of interest to the public is not the same as what is in the public interest.

[16] In the context examined, the ECJ asked specifically whether "*it would not have been sufficient to inform the general public only of the remuneration and other financial benefits*". See paragraph 88 of the Court decision in Rundfunk, joined cases C-465/00, C-138/01.

[17] European Court of Justice expressed in the Judgment on the Joined Cases Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v Land Hessen, paragraphs 79 and 80.

Generally, the amount of personal data published on-line is likely to be more limited than that submitted to the competent institutions, since proactive disclosure of some information is likely to be inappropriate, given the probable impact publication would have on the data subjects. Furthermore, some of the information not subject to proactive disclosure may be disclosed when legislation on access to information applies in accordance with the law and/or other relevant legislation or upon a judicial decision requiring its disclosure. When determining whether obtaining and/or publishing personal data of the public sector subjects is necessary, one should take into account whether the affairs and/or transactions of the public sector subjects (financial, contractual or others) took place prior to them assuming their office, when they were private persons without a public mandate. Competent institutions are not prevented from collecting this data on this basis, especially in situations where suspicious activities have taken place. Nevertheless, automatic on-line publication of all the affairs/transactions of the public sector subjects prior to when they took office, searchable by name and including all details with no distinction based on the nature, type and extent of such data may go beyond what is necessary for achieving the legitimate aims pursued.

When considering publication of personal data on-line it is necessary to consider the potential risks of such a disclosure. Where routine or extensive publication is envisaged a privacy, impact assessment is strongly recommended. This should also consider alternatives ways of providing some personal details, such as in summary or in collective form where individuals cannot be identified.

It is also appropriate to consider whether the nature and extent of the personal data being published may pose risks other than those related to data protection. For example, publishing personal data related to a data subject's economic situation may make them vulnerable to criminals. That does not exclude the disclosure of these data to competent institutions in charge of collecting and processing these data.

Also, when publishing information related to public sector subjects' contractual and/or similar relations, competent institutions should be aware that certain data could represent a secret (trade, bank, professional or other). In these cases, it may be necessary to balance data protectionrights, secrecy protection and the public interest in access to such information.

EXAMPLE: Personal data of a public sector subject's household or family members, such as names, contact details, addresses, etc. can be collected by the competent institutions in order to carry out their duties in this area; however the on-line publication of the entire information may not be proportionate, though each case should be assessed on its own merits.

- *Processing operations with regard to different groups of persons concerned*

A selective approach to processing personal data should be taken, differentiating between different groups of people, cases and purposes and taking into account specific situations with regard to the content of the personal details being published. Different methods of making the information available should be used as appropriate.

When evaluating whether the processing should include the public dissemination of personal data through on-line publication, different situations should be handled in different ways. Competent institutions may wish to take into account the extent to which the public institution or the public sector subject concerned is exposed to the risk of corruption or to situations of conflicts of interest; the scope of their actions or tasks to be accomplished in the public interest and the amount of public funds the individuals manage. Generally speaking, it may be appropriate to differentiate depending on hierarchical and decision making responsibilities between politicians, senior public sector subjects or other public figures holding positions involving political responsibilities; individuals in a "common public sector management position" who do not hold elective offices but only perform executive management positions and "common public sector subjects" who have no decision making responsibility of their own.

In this regard, while for the first group the on-line dissemination of personal data via the website of the competent institution concerned may be considered proportionate, the same solution might not be applicable for the second or the third groups. For the second group the name and position might be publicly available while no personal data on agents would be published by default (even if only with regard to personal data about actions taken in their capacity as public sector subjects or concerning their professional activities[18]). This is without prejudice to the availability of those data under the national rules on public access to documents.

It is advisable to make a distinction between different groups of public sector subjects, civil servants and other individuals under this specific legislation, depending on the aforementioned criteria and to determine different levels of reporting obligations to the competent institutions, based on such distinctions. The legislator should bear in mind this distinction especially in relation to any on-line publication obligations.

This approach would facilitate the delivery of different quantities and types of personal data depending on the group of individuals and would therefore help to ensure the fulfilment of the proportionality requirements, according to which processing of personal data shall cover only the minimum necessary to achieve the legitimate purpose (detecting and sanctioning conflict of interest).

[18] In this respect, in the Rundfunk joined cases C-465/00, C-138/01, the ECJ draws attention to the jurisprudence of the ECHR about the scope of the expression '*private life*' referring that it '*must not be interpreted restrictively*' and that '*there is no reason of principle to justify excluding activities of a professional ... nature from the notion of "private life"*'. See paragraph 79 of the Court decision.

EXAMPLE: The publication of personal data relating to conflicts of interest declarations of public sector subjects exercising tasks involving only administrative responsibility has been considered disproportionate, in some instances, taking into account that they do not hold elective or ministerial offices. On the contrary, the deposit of these documents at the competent control authorities has been deemed justified for the purposes of strengthening the integrity and impartiality of those persons and preventing, detecting and sanctioning conflict of interest situations[19].

3.2.2 MINIMISATION PRINCIPLE

As for the minimisation principle, a strict assessment of the necessity and proportionality of the processed data should take place (Article 6 of the Directive 95/46/EC and in the GDPR provisions). The amount and type of processed personal data has to be clearly determined. When personal data need to be processed, such data must be adequate, relevant and not excessive for the specified purposes, according to the law, and any information that is not necessary for achieving such purposes should not be processed in any way. The processing of personal data when implementing conflict of interest and transparency measures should be focussed on and relevant to, the legitimate purpose in order to avoid unnecessary data processing. This, in turn, is likely to make the processing more effective and efficient.

On-line publication might not always be necessary to achieve the purpose of the processing; in some cases, providing basic general information about a particular area of government or reporting details of public sector decisions and actions in the form of performance indicators may be enough. In depth and more comprehensive data may be submitted to the competent oversight authorities, allowing, if necessary, on-line publication or the public availability of those data under the national rules on access to public documents.

EXAMPLE: Where it is necessary to collect and publish information on the assets of individuals related to the public sector subject (such as partner, children and other family or household members) on-line, consideration should be given to the minimisation principle whether the assets of family member should be published in a disaggregate way or should be limited to their total amount of value. The extent to which publication of the identities of all family or household members is necessary to achieve the aim pursued should also be considered.

[19] See Conseil constitutionnel de la République Française, Décision n ° 2013-675 DC of 10.09.2013 concerning the "Loi organique relative à la transparence de la vie publique" (Projet de loi the adopté 17 septembre 2013 - TA No. 209)

EXAMPLE: Some national rules on transparency provide for the on-line publication of information concerning the amount of individual income and remunerations received by persons discharging high level administrative tasks (for example, holders of senior administrative positions). Generally to comply with such obligations, according to the minimization principle, it may be sufficient to publish the total amount of money received by the individuals concerned. However, it is unlikely to be proportionate to publish data, such as Tax ID, entire financial reports, detailed data extracted from tax returns or individuals' pay slips, bank details or home addresses, personal phone numbers or personal emails.

EXAMPLE: When it is about to publishing on line the financial data of the individuals (i.e. – debts, loans etc), it is recommendable, pursuant to minimization principle – to publish only necessary and / or basic information, having in mind the vulnerability of these data and potentional risks arising out of such on-line publication. Therefore, it is advisable that law stipulates the publishing details when on line publication of financial data take place in order to avoid possible abuses or excessive on line publication of these data which may go beyond the reasonable and / or legitimate purposes, considering at the same time the public interest as well.

❖ Type of Data

When processing personal data as part of conflict of interest and transparency measures in the public sector, one of the purposes will be to determine that changes in the financial standing of the public sector subjects are legitimate. In general, any data collected and/or published should be functional; for example to reveal whether such individuals have illegally acquired assets, infringed any conflict of interest measures or committed any illicit or dishonourable acts. It is not appropriate to collect and further process personal data which are not helpful to evaluating such infringements and/or detecting any possible misconduct. It is recommended that legal and practical frameworks are designed which focus on the achievement of the legitimate management of conflicts of interest and associated transparency, in order to prevent any unnecessary, illegitimate and unfair personal data processing.

EXAMPLE: The business relations concluded during the period in public office may indicate illicit conduct and could be subject to deeper analysis by the competent institutions. Thus, information may be processed if it is relevant to verify whether the public sector subject has achieved, inappropriate financial or other gain directly or indirectly (via a relative or partner).

3.3 PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA (SENSITIVE DATA)

Article 8 (1) of Directive 95/46/EC identifies personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life as special categories. The GDPR broadens the special categories of personal data to also encompass genetic data, biometric data in order to uniquely identify a person and sexual orientation data. Both, Directive 95/46/EC and the GDPR determine the prohibition of processing of such data as a general rule, specifying several exceptions where such data can be processed.

Furthermore, Article 8(5) of Directive 95/46/EC stipulates that the processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. A similar provision has been included in the GDPR.

Taking into consideration the aforementioned provisions, proactive disclosure of such data should be exceptional, supported by a specific legal basis and always taking into consideration the appropriate balance between privacy protection and the legitimate public interest.

EXAMPLE: If it is needed in the process of candidature, it may be acceptable to publish information relating to elected individuals representing political parties that would disclose their links to some political or trade-union groups.

3.4 RETENTION PERIODS

The period for retaining personal data in a form which permits identification of data subjects, should be determined according to the legitimate purposes for which they are held. The data should only be processed for the period necessary to achieve those relevant legitimate purposes. Processing within competent institutions should be considered separately from the purpose of publishing personal data. It is preferable that the retention periods are clearly stated and also include provisions on on-line availability.

Different steps may be defined: a period for the processing of the data for the main purpose, a period for the publication of the data and a period for any archive. Different periods may apply to different data or datasets.

3.5 ACCURACY OF THE DATA

Personal data should be accurate and, where necessary, kept up to date. In accordance with Article 6 of Directive 95/46/EC, every reasonable step must be taken to ensure that data are kept accurate and up to date, having regard to the purposes for which they were collected or for which they are further processed. Moreover, in light of the GDPR, the public sector subject will have the right to obtain from the competent institutions, without undue delay, the rectification of their personal data which are inaccurate or out of date. Also, Article 16 of the GDPR states that, depending on the purposes for which data were processed, the data subject will have the right to obtain completion of incomplete personal data, including by means of providing a supplementary statement.

When the law requires that certain data should be published on-line, it is advisable that, in the light of accuracy principle, competent institutions create clear/unique form(s) /declaration(s) which would contain only relevant data.

It is also recommended that competent institutions implement adequate procedures to keep the collected personal data accurate and up to date in line with Article 6 of Directive 95/46/EC

and in the light of GDPR. It is a good practice to indicate the date of publication, or of last update, on any published dataset.

3.6 PURPOSE LIMITATION

The collected data can only be processed in the framework of the specified purposes and for other compatible purposes. Article 6(1)(b) of Directive 95/46/EC stipulates that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.

Also, in light of GDPR a similar provision states that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of personal data for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.

It is notable that in some EU Member States certain data controllers have added specific information to explain the limits of reuse of published data. Indeed, as the WP 29 highlighted in the Opinion 06/2013 on open data and reuse, potential re-users would have to comply with data protection law, as data controllers, when they are dealing with personal data, unless their processing activities fall within the household exemption under Article 3 of Directive 95/46/EC.

When deciding whether the personal data should be globally accessible via external search engines, it is appropriate to bear in mind the purpose of making the information widely available. If there is a global public interest in making such data available, especially having in mind the category of data subjects, then such dissemination is likely to be justified. This is provided that any potential impact on the data subjects' rights and freedoms has been taken into account. However, if there is no global public interest or such wide dissemination is deemed inappropriate it may be preferable to make the data available via internal search engines[20] or through other selective access mechanisms (for example with a login or captcha).

It is recommended that reuse of data is explicitly defined as allowed or forbidden, and the eventual conditions for the reuse should then be stated[21].

4. SECURITY MEASURES

The competent institutions, as data controllers, shall undertake appropriate technical and organisational measures to protect personal data, prevent from accidental loss or destruction, alteration or unauthorized disclosure or access and all other unlawful forms of processing.

[20] To that end, specific access rules may be coded within each text file (e.g. via the noindex/noarchive metatags and the robots.txt file, to be configured in accordance with the Robot Exclusion Protocol). This is without prejudice to the use of any tools that can facilitate retrieval of the information and documents to be disseminated on a public body's official website.

[21] See Opinion WP207 of the Art. 29 Working Party

Protection measures must be appropriate to the nature of the competent institutions processing activities.

To that end, appropriate measures should be implemented to reduce the risk that the information and documents available on the Internet may be erased, amended, altered and/or taken out of their context – for instance, reliable sources may be specified from which the said documents may be retrieved; electronic signatures may be used to ensure the authenticity and integrity of the documents; "context data" may be inserted into files posted on official websites such as versioning information, expiry, administrative body in charge).

5. DATA SUBJECTS' RIGHTS

To assure fair processing, the WP29 recommends that competent institutions inform any re-user of their obligations related to data' subjects rights and how to comply.

Prior to collecting any personal data, the competent institutions shall inform the public sector subject whose personal data is being collected in accordance with Articles 10 and 11 of Directive 95/46/EC. The right to be informed may result from the relevant law stipulating which personal data should be made public and may therefore be published without prior consent of the public sector subject.

Furthermore, the data subject shall be able to obtain from the following information from the competent institutions, unless an exception in Directive 95/46/EC applies:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him, in an intelligible form, of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him, at least in the case of the automated decisions.

According to Article 14 of Directive 95/46/EC, the data subject in some cases[22] has the right to object at any time to the processing. It is recommended that the controller informs all re-user of such data about an objection[23].

This right to object may be dropped or limited by law depending on the purpose. For example, it may permit data subjects to object to online publication of some or all of the data

[22] In that regard, it should be mentioned that Article 14 of the Directive provides that the data subject can exercise the right to object, at least, inter alia, in the case of the ground referred to in paragraphs 7 (e) of the Directive. This means that where the processing is allowed further to a reasonable and objective assessment of the different rights and interests at stake, the data subject still has an additional possibility to object on grounds relating to his/her particular situation. See the WP 29 above-mentioned Opinion n. 06/2014, Section III, par. 3.6.

[23] In France, this is an obligation stated in the article 97 of the décret of the national data protection law.

concerning them based on compelling legitimate grounds relating to their particular situation but not to its internal processing operations (different from the dissemination of data concerning them).

Also, any data subject shall be able to obtain from the competent institutions the rectification, erasure or blocking of data, the processing of which does not comply with the provisions of Directive 95/46/EC. Furthermore, third parties to whom the data have been disclosed shall be notified of such rectification, erasure or blocking, unless this proves impossible or involves disproportionate effort.

Under the GDPR, the data subject will have a right to rectification, erasure and restriction, as well as a right to lodge a complaint with a Data Protection Authority.