ARTICLE 29 Data Protection Working Party

10936/03/EN
WP 83

Opinion 7/2003 on the re-use of public sector information and the protection of personal data

- Striking the balance -

Adopted on: 12 December 2003

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

Having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

Having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT OPINION:

I. Introduction

The European Commission has adopted in June 2002 a proposal for a Directive on the re-use of public sector documents[2]. The European Parliament voted this Directive in second reading on 25 September 2003, and the Council formally accepted the amendments voted by Parliament on 27 October[3]. The re-use Directive aims at a minimum harmonisation of the rules for the re-use of public sector information in the European Union in order to ensure a level playing field. Such information is considered an important economic asset in that it provides raw material for new digital products and services and is a key data input for e-commerce trading.

The data this Directive aims at being re-used are for instance geographical information, business information, tourist, traffic or educational information. Personal data are thus not the main target, but such data may of course also be requested to be re-used.
In this respect, the Directive is intended to be neutral, i.e. it does not affect the harmonised level of data protection rules as set out in Directive 95/46/EC which is explicitly stated in an article and recital of the proposed Directive[4]. From this follows that 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

---

1 Official Journal no. L 281 of 23/11/1995, p. 31, available at: *http://europa.eu.int/comm/internal_market/en/dataprot/index.htm*

2 Proposal for a Directive on the re-use and commercial exploitation of public sector documents, (COM (2002) 207 final)

3 The Directive is presently in the process of signature, and publication in the Official Journal is expected to take place this December.

4 Article 1 (4) reads: '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.'
Recital 19 reads: '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 the free movement of such data'.
State of play: common position adopted by the Council on 26 May 2003.

Community. It has already delivered Opinion 3/99 on the same subject and Opinion 5/2001 on a related topic[5].
The purpose of this document is to explain the meaning of full applicability of the data protection Directive in this context and to give guidance on how to strike the balance between data protection and the re-use of public sector information, further to the two opinions cited above.

II Relevant aspects of the data protection Directive

1. General

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.
Whereas the data protection Directive guarantees, as part of the fundamental right to data protection, the right of access for the data subject to his or her own personal data, the purpose of freedom of information laws is to ensure transparency, openness and accountability to the citizens that consequently need not give any justification for their information requests. They will in the normal case use the information for their own, non-commercial, purposes. The data protection Directive recognises that this principle of public access to documents may be taken into account in the implementation of the data protection principles[6]. The legislator has in this case determined that there is a general obligation for disclosure, subject to certain conditions and exceptions, such as usually exceptions on privacy grounds. In these cases, the purpose for which the data will be re-used will thus not be an issue that would need to be considered. It should be mentioned that the Directive on re-use of public sector information builds on the existing access regimes in the Member States and does not change the national rules for access to documents. It does not apply in cases in which citizens or companies can, under the relevant access regimes, only obtain a document if they can prove a particular interest[7].

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 distinction made, although sometimes difficult to draw in practice, may have consequences for the application of the principles set out in the data protection Directive.
The present document is meant to give guidance for this latter case only, as regards access to personal data for re-use purposes.

---

5 Opinion 3/99 on Public sector information and the protection of personal data- Contribution to the consultation initiated by the European Commission in its Green Paper entitled 'Public sector information: a key resource for Europe' COM (1998) 585; Opinion 5/2001 on the European Ombudsman special report to the European Parliament following the draft recommendation to the European Commission in complaint 713/98/IJH. Community institutions will equally have to strike the balance between their obligation to openness, as set out in Regulation 1049/2001, and the protection of personal data, in accordance with Regulation 45/2001.

6 See recital 72 of the data protection Directive.

7 See recital 9 of the Directive of the European Parliament and the Council on the re-use of public sector information.

2. The data protection framework

This section looks at the data protection framework that applies and that public sector bodies will have to observe once personal data are requested to be disclosed for re-use purposes.

The data protection Directive only applies in this context if information held by the public sector contains personal data. Given the broad definition in the Directive[8], many public sector documents will potentially involve personal data. The proposal Directive mentions as examples of documents which could be re-used geographical information, business information, traffic information or aggregated statistical data. Information held by the public sector that contains personal data might for example be found in population, company, vehicle or credit registers as well as information on medical, employment or social welfare data. With a view to avoiding the disclosure of personal data in the first place, such should be excluded where the purpose of the re-use can be fulfilled with the disclosure of personal data rendered anonymous in such a way that the data subject is no longer identifiable.

The Working Party recalls that the data protection Directive applies to personal data which have been made publicly available[9].

From the point of view of the data protection Directive, the disclosure to third parties of personal data collected and held by public sector bodies is to be considered as processing of personal data, given that the definition of processing includes a *disclosure by transmission* with the consequence that the material conditions that govern the processing of personal data have to be observed.
It should be noted that re-use may be the consequence of either a specific request to a public sector authority to disclose certain information, or it may result of a contract, or it may result of the use of information that has been made publicly available or accessible through the internet, as for instance certain public registers. For this latter case, the Working Party emphasizes the need to provide for technical safeguards in order to ensure that access is limited or structured in such a way as to avoid unlawful processing, for instance massive downloads. In this respect, the data protection Directive indeed requires that the controller must implement appropriate measures to protect personal data against unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network (Article 17 of the Directive).

The material provisions that have to be complied with under the data protection Directive are articles 7, and in case sensitive data are involved, article 8, as well as the principles relating to data quality as set out in article 6. It is important to underline that articles 7, 8 and 6 are complementary requirements that both have to be fulfilled.

(a) Legitimacy of public disclosure (Article 7 of the data protection Directive)

---

[8] Article 2 (a) of the data protection Directive reads 'For the purposes of this Directive: '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;…'

[9] See Opinion 3/99, op cit footnote 2 supra.

The processing of personal data that would consist in disclosing these data upon request needs to be legitimate in accordance with one of the grounds set out in the closed list of Article 7 of the data protection Directive. The following grounds appear to be relevant in this context:

(aa) Where the data subject has unambiguously given his or her consent, the public sector body may disclose the personal data of this particular data subject. With a view to guaranteeing this informational self-determination of the data subject, it would be advisable to provide for the possibility to give or deny consent to re-use already at the time of the original collection of the data.

(bb) A further legitimacy ground may be that processing is necessary 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.

(cc) Personal data may be disclosed if such is necessary for compliance with a legal obligation. Unless there is a specific power for a public body to disclose the data, such disclosure is not permitted on these grounds.
It is important to underline that the re-use Directive cannot be invoked as such a legal obligation that has to be complied with, because this Directive does not create an obligation to disclose personal information: it states on the one hand that it leaves intact the data protection Directive and on the other recital 9 explicitly foresees that '(T)his Directive does not contain an obligation to allow re-use of documents. The decision on authorising re-use or not will remain with the Member States or the public sector body concerned.' Hence it is left to the Member States to determine in which cases they oblige public sector bodies to disclose personal data.

There is a further ground – processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed- that is difficult to distinguish from the 'legal obligation' ground and indeed will overlap[10]. The distinction is however relevant, given that in the case of a legal obligation, it is the legislator's responsibility to assess compatibility before stipulating such a legal obligation to disclose personal data. When the processing is considered necessary for the performance of a task carried out in the public interest, this places the obligation to make the assessment upon the public sector body and consequently leaves a certain margin of appreciation.

(dd) The general clause that allows processing if necessary for the purposes of a legitimate interest pursued by the controller, that is the public sector body, or the party to whom the data are disclosed requires that a balance be struck on a case-by-case basis between the right of the data subjects to privacy and such legitimate interests of the controller or third parties who wish to re-use personal data.

(b) Special protection for sensitive data (Article 8)

There are special provisions in the data protection Directive for sensitive personal data[11] that foresee a general prohibition for processing such data while providing for a closed

[10] For details see Opinion 5/2001, footnote 2 supra.

[11] Sensitive data are personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. (Art. 8 (1) of the data protection Directive).

list of justified exemptions. If sensitive personal data are to be disclosed, the public sector body will in addition to the assessment in particular of compatibility have to carefully examine whether one of these justified exemptions applies.
Exemptions that may be relevant in this context are the explicit consent of the data subject to the processing of such data or data which are manifestly made public by the data subject.

(c) Transfers to third countries (Articles 25 and 26)

If the recipient of personal data is established in a third country, the provisions of the data protection Directive on international transfers apply[12]. Accordingly, personal data may only be disclosed and transferred if the third country in question ensures an adequate level of protection, or if one of the derogations foreseen in the closed list of Article 26 of the Directive applies.
A provision that deserves particular attention in this context is article 26 (1) f that determines that transfers may take place, on certain conditions, if they are made from certain public registers. The logic behind is that those who are located in third countries should not be in a less favourable position as regards access to certain publicly available information. This does however not mean that such transfer is legitimate per se, just because it is made from a public register. Rather, in each case of processing of personal data –like a transfer from a register- the underlying conditions for this processing, in particular compatibility (see below under d), have to be fulfilled.

(d) Principles relating to data quality, in particular the finality principle (Article 6)

This provision sets up several principles relating to data quality as fundamental requirements that public sector bodies will have to comply with when disclosing personal data.
In this context, apart from the general 'fair and lawful processing' principle, the principle according to which personal data should be adequate, relevant and not excessive is of importance, especially when a disclosure serves a specific purpose. Thus, with a view to avoiding the disclosure of personal data in the first place, such should be excluded where the purpose of the re-use can be fulfilled with the disclosure of personal data rendered anonymous in such a way that the data subject is no longer identifiable.

Purpose limitation principle

Further to that, the purpose limitation principle deserves particular attention in this context. According to the purpose or finality principle set out in Article 6 of the data protection Directive, personal data must be *collected for specified…purposes and not processed further in a way incompatible with those purposes.* Thus, the Directive does not prohibit the re-use for different, but for incompatible purposes.

An exception to this principle exists for further processing for historical, statistical or scientific purposes: such processing shall not be considered incompatible if Member States provide appropriate safeguards. The underlying rationale is that processing of personal data for these purposes will, under normal circumstances, not imply their use in relation to a particular data subject. Consequently, recital 29 of the data protection

[12] Articles 25 and 26 of the Directive.

Directive states that the existence of safeguards should rule out the use of the data regarding any particular individual[13].

(aa) General

In the context of re-use of public sector information, the purpose principle obviously is of crucial importance. Some examples of possible interpretation of this principle in Member States include the use of the criterion of reasonable expectations of individuals to assess compatibility, or to accept compatibility if a legal obligation is at stake, or to stress all the circumstances surrounding the processing to evaluate the compatibility of the re-use which amounts to a kind of balance of interest test, including the nature of the data, the manner in which they have been collected and the existing safeguards for the data subject. Some Member States have adopted a restrictive position for constitutional reasons.

As outlined above, public sector bodies may only act within the competences that the law attributes to them. Thus, Member States' laws should clearly specify these competences as regards a possible disclosure of personal data for re-use purposes, taking account of the criteria set out below. It may however not be feasible to specify each and every situation by law, in which case the public sector body itself would have to assess the issue of compatibility. It should be mentioned in this respect that the data protection authorities in Member States, which are responsible for monitoring the application of the respective data protection laws, have already produced guidance on the issue and, in case of doubts, are in a position to provide for assistance in concrete cases.

The distinction has to be made between a specific request to have information disclosed and the use of information that was already publicly accessible, as for instance in certain public registers. Evidently, only in cases a specific request is made, an assessment by the public sector body of the purpose of the specific re-use will have to be made.
It should be noted in this respect that not only the public sector authorities bear the responsibility for this assessment when they are requested to disclose personal data. Likewise, the third party who requested disclosure and who intends to re-use such data would be a controller in the sense of the Directive and as such has to comply with its requirements. This is particularly relevant for information that is already publicly accessible.

(bb) Specified purposes

A major element in the assessment of compatibility is linked to the way in which the purpose is determined in the first place. A purpose that has been defined in a rather vague way is more likely to be compatible with another, secondary purpose. However, such a wide definition is neither likely to fulfil the determination requirement foreseen by the Directive nor likely to pass the quality and foreseeability test that the European Court of Human Rights requires when public authorities restrict fundamental rights and freedoms.

In the public sector, the original purpose will however usually be determined by the rules that govern the functioning of the sector. Public bodies vested with certain powers are thus only able to process personal data for such purposes that are within their

[13] The full text of the recital reads: Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

competences, or are reasonably necessary to carry out the primary functions attributed to them.

Often, the public sector bodies that deal with a request will not be aware of the purpose the information is going be re-used for, given that under the proposed Directive there is no such obligation to declare which purposes the obtained information is requested for. However, the data protection Directive will require such a declaration if the disclosure of personal data is requested in order that the authority is in a position to assess whether a re-use is compatible with the original purpose and lawful more generally.

(cc) Assessment of compatibility

There are several elements which may have to be taken into account in the evaluation of whether further processing would be compatible with the original purpose.

- *Grounds for original processing*

The ground for the original collection of personal data by the public sector body contained in article 7 of the Directive may influence the assessment of compatibility: as outlined above, such grounds will normally either be consent of the data subject, compliance with a legal obligation or performance of a task carried out in the public interest. A further ground may be the performance of a contract that requires the processing of personal data.

There are cases in which public administrations are obliged by law to not only collect but also disclose personal data to third parties. An example of this can be found in the laws regulating certain public registers such as for instance personal data on property contained in public property registers or registers established under family law. The Directive allows this on the basis that it has to be in the public interest to have these data publicly available.

In such cases of a legal obligation, the legislator should make the assessment of compatibility beforehand, taking account of the issues discussed under compatibility. As a consequence, when there is a legal obligation, compatibility would no longer be an issue at the moment of disclosure, provided the assessment has been made beforehand.

In other cases, for instance when a disclosure is necessary for the performance of a task carried out in the public interest, the public sector body will have to make the assessment itself.

If no public interest can be invoked, but a mere private one of a third party, the Directive allows personal data from such registers to be disclosed to third parties if certain conditions are met, for instance if the third party can demonstrate a legitimate interest.

This suggests that there are cases in which a disclosure would also be compatible with the original processing given that the law already determined the disclosure as one of the purposes for the original processing, in the public interest.

As to further grounds for original processing, the data subject's consent will be relevant if personal data are collected for the conduct of a survey, or the performance of a contract would be for instance when a public body sells or buys assets, or intends to sell personal data with the aim to generate revenue. Situations may for example arise in this respect when public bodies have collected personal data in the framework of selling ground to the public and subsequently consider using these date to offer mortgages, or personal data collected from university students upon inscription may be considered to be used for education related direct marketing purposes.

Judged against the criterion of reasonable expectations of the data subject, a person who communicated his or her data for a very specific and particular purpose will normally not expect that these data are used for a further purpose that is not directly connected with the original one, and in particular if the secondary purpose consists in commercialising these data (see also below under *'re-use for commercialisation'*).

- *Mandatory personal data*

Often personal data will have to be submitted by citizens, for example in a tax declaration, or to be supplied in order to obtain a public service, as will be the case for social welfare services.
If such mandatory data are requested for re-use, compatibility needs to be assessed in a particularly careful way, especially in Member States that apply the reasonable expectations criterion: a data subject that is under an obligation to supply his or her personal data will not expect a re-use for other purposes so that disclosure would be considered unfair in terms of the data protection Directive. This is even more the case when a disclosure of mandatory data is requested with a view to commercialising these, see below.

- *Re-use for the purpose of commercialisation*

For the purpose of this document, it is understood that commercialisation consists of elements such as the intention of the 're-users' to directly generate revenue or use personal data for their general marketing purposes. The draft Directive on re-use speaks of 'commercial exploitation' in this respect. Looking at the public sector, the risk of commercialisation of information lies in the possibility that public sector bodies may seek to utilise the information obtained for particular purposes for other unconnected purposes with the sole aim to generate revenue.

A balance needs to be struck in each case of request between the fundamental right to data protection and the commercial interests of private operators. If personal data are to be re-used for commercial purposes, this secondary purpose may be considered as incompatible and thus the information not be disclosed. Indeed, some Member States' laws explicitly foresee such a prohibition of commercialisation. Examples are the French law that prohibits the commercial usage of electoral registers, the Belgian law on openness of the administration that strictly prohibits re-use of personal data for commercial purposes, and the Berlin law on freedom of information which generally prohibits the commercial use of the information received on the basis of this law.

Public authorities may lawfully disclose personal data for commercial purposes if such specific powers are attributed to them. Such laws should contain specific guarantees for the data subject, such as an opt out provision. Such is the case, for example, in Sweden and Finland as regards the population registers, or the register on data systems for road traffic. The Swedish law explicitly states that personal data from one population register, the *Swedish Person and Address Register (SPAR)* may be used for direct marketing purposes so that in this case re-use is in accordance with the original purpose, and provides for the possibility of an opt-out.
The Dutch law allows commercial use for some specific purposes, for example for credit scoring and liability purposes. In the UK, there are presently few instances where there has been statutory provision to permit commercial exploitation.

- *Recipient of the data*

In assessing the compatibility it may be relevant to know the purpose of the re-use. In some cases, the recipient will benefit from own fundamental rights, such as freedom of opinion or freedom of press. If such is the case, the recipients' fundamental rights need to be taken into account and a balance needs to be struck between the two competing fundamental rights. The compatibility test might be easier to be satisfied in these cases.

- *Nature of the data*

The nature of the data will play a role in assessing compatibility as well. If for example sensitive data are requested to be re-used, the threshold for compatibility will be higher than for 'normal' personal data. The request for re-use of sensitive data could even be considered as incompatible as a matter of principle, although it seems that the special provisions for sensitive data outlined above will most likely provide for sufficient protection.
In the event that partly anonymous data are requested, the fact that in such cases a data subject can only be identified with a certain effort has to be included in the assessment[14].

- *Disclosure from a public register*

In the case of public registers, disclosure may be made for narrower purposes, given that all public registers have been established for a specific purpose. If disclosure serves such a specific re-use purpose, the (legislative) framework has to be such as to avoid, to the extent possible, other use of the information. Again, it has to be emphasized that the third party who requested disclosure and who intends to re-use such data is a controller in the sense of the Directive and as such has to comply with its requirements.
The Working Party emphasizes the need to provide for technical safeguards in order to ensure that access is limited or structured in such a way as to avoid unlawful processing, for instance massive downloads.

- *Further elements*

The consequences for the data subject of a disclosure and re-use of his or her personal data will have to be taken into account as well, as the extent to which adequate guarantees are offered. Such could be the information to the data subject, or the possibility for the data subject to opt-out (see below point 3 for both aspects).

(d) Conclusion of this section

As is clear from the above, the assessment will have to be made on a case-by-case basis the result of which will often not be a clear 'yes' or 'no', but rather some differentiation in the sense that access to certain data may be prohibited, certain use may be prohibited, a restricted circle of persons may be granted access, conditions may be imposed on access, for instance the need to justify a request, or only non-computerised access is granted, for instance a paper copy of a document.
There are a number of instances where information held in the public sector may be utilised in a way that does not involve the disclosure of information relating to particular individuals. This is primarily where this amount aggregated statistical data such as where this occurs with national census statistics or in relation to epidemiological research or scientific research. Also, an individual's details could be omitted from a public sector document before disclosure, or the details could be omitted from a public register which is available for open inspection, or the registration of individuals could be allowed to be made anonymously, for instance when paying community charges.

[14] In order to render the protection afforded by such partly anonymous personal data effective, their re-identification should be sanctioned.

3. The data subject's rights

The data protection Directive grants a number of rights to the data subject whose personal data are disclosed. The primary means of ensuring transparency in processing is the obligation to inform the data subject of such processing. This is the precondition for an effective exercise of the data subject's other rights, such as the right to have incorrect data rectified or the right to object to processing.

The Working Party recalls that[15]

- data subjects have to be informed about the disclosure of their personal data; if public authorities envisage this possibility, they should inform the data subject at the moment of collection of the data, in accordance with Article 10 (c) of the data protection Directive;

- regardless of whether or not personal data are published, data subjects have a right to access and, where necessary, a right to require that the data be rectified or erased if they have not been processed in accordance with the Directive, and in particular if they are incomplete or inaccurate;

- data subjects have a right to object to the processing of their personal data, in particular if these data are re-used for commercial and even more so direct marketing purposes. In this latter respect, article 14 (1)(b) of the data protection Directive explicitly determines this right to object, the exercise of which does not require any particular justification.
Where a law allows usage, it should thus provide for the possibility to object to a re-use already at the time of the original collection of the data.
The existence of the right to object should also be mentioned in the information that is provided to the data subject in order to guarantee fair processing.

III. Conclusions

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.

Done at Brussels, on 12 December 2003
For the Working Party
The Chairman
Stefano RODOTA

[15] See Opinion 3/99.