ARTICLE 29 DATA PROTECTION WORKING PARTY

00379/13/EN
WP 201

Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive

Adopted on 26 February 2013

1. Introduction

On 25 January 2012 the European Commission adopted a proposal for a *Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* (hereafter: the Police and Criminal Justice Data Protection Directive or the Directive). The proposal was presented in parallel to the draft General Data Protection Regulation. Both the Council and the European Parliament have thereafter started their respective procedures in the legislative process for both instruments with the aim to reach an agreement on the full package before the European elections in 2014. Progress in the legislative debate on the Directive is however slow.

The Article 29 Working Party has provided its first general reaction to the Commission proposals in its opinion of 23 March 2012, highlighting areas of concern and making certain suggestions for improvement.

The Article 29 Working Party welcomes the so-called 'package approach' taken by the European Parliament rapporteurs in their draft reports to the LIBE committee and is confident all political groups will continue to take careful consideration of all elements of the package as well as the much needed consistency between the two proposals in order to further improve them. The Working Party also welcomes the intensified legislative debate in the Council instigated by both the Cypriot and Irish presidencies.

Following the first opinion providing further input into the discussions on the Regulation adopted by the Article 29 Working Party on 5 October 2012, the Working Party now presents further guidance on several specific elements of the proposed Police and Criminal Justice Data Protection Directive. Although there are more issues that could be further discussed, the Working Party has, given the stage of the negotiations, decided to focus on four issues which are currently considered to be the most important. These elements include the use of data of non-suspects, the rights of data subjects, the use of privacy impact assessments, and the powers of data protection authorities, especially concerning confidential or classified information.

2. On the use of data of non-suspects

Article 5 of the draft Directive obliges controllers to make a clear distinction between personal data of different categories of persons and defines five categories of data subjects. According to Recital 23, such a distinction is inherent to the processing of personal data in the areas of judicial co-operation in criminal matters and police co-operation. WP29 underlines that such distinction is also necessary to ensure a proper implementation of the principles relating to personal data processing as defined in Article 4.

Article 5 makes a distinction between various categories of persons that have a direct or (possible) indirect link with a specific crime or suspects (categories (a) to (d)) and other persons (category (e)). In view of the description of the relation to a crime or an investigation of the persons referred to in categories (a) to (d), it is clear that the persons falling under category (e) may be described as persons having no known relation to a crime or to suspects as referred to in the other categories.

It is precisely this group of persons for which the European data protection authorities already in 2005[1] stressed the need to distinguish between the processing of personal data of non-suspects with data of persons related to a specific crime. Processing of data of persons who are not suspected of having committed any crime (other than victims, witnesses, informants, contacts and associates) "should only be allowed under certain specific conditions and when absolutely necessary for a legitimate, well-defined and specific purpose." Furthermore, such processing should (in the view of the data protection authorities) "be restricted to a limited period and the further use of these data for other purposes should be prohibited." At the same time, the Directive should make clear that additional limitations and safeguards apply to victims or other third parties, as referred to in Article 5(1)(c) of the current Proposal. The law needs to recognise that differences must be made between the processing of personal data of convicted perpetrators and of victims of a crime, particularly in databases created for preventive purposes or the prosecution of future crime.

The evolution of law enforcement techniques and methods in the past decade clearly demonstrate that all these categories which fall under the broad category of "non-suspects" need specific protection. This is especially the case when the processing is not done in a specific criminal investigation or prosecution.It is the difference between information that the law enforcement authorities 'need to know' and the information that is 'nice to have'.

In order to protect "non-suspects", the Working Party strongly suggests to introduce a new Article 7a in addition to Article 5. The new Article 7a, as proposed below, would make sure that the differentiation of data categories is not an administrative burden and not an end in itself, as the current proposal could be interpreted. It is necessary in order to ensure that Member States may only process the data of "non-suspects" if specific requirements are fulfilled and that additional protection is required when the data of "non-suspects" is processed. Therefore, it makes better sense to place the new provision in the context of Article 7, which regulates the lawfulness of processing.

The Working Party is aware of the specific character of data processing in a law enforcement environment, and understands that the processing of data of "non-suspects" might be necessary in specific situations. The proposal also takes account of the different purposes for which law enforcement authorities may process the data of "non-suspects" and suggests particularly stringent rules for those situations in which the processing does not serve the purpose of a specific investigation or prosecution. It is in these situations where the processing of data of "non-suspects" may only be processed if indispensable for a legitimate, well-defined and specific purpose, limited to assess the relevance for one of the categories indicated in Article 7a paragraph 1 (a) - (d), restricted to a limited period of time and its further use is prohibited.

In order to avoid semantic discussions about the difference between 'necessary' (as is currently being used in the draft Directive) and 'absolutely necessary' (as is used in the Krakow position paper), the Working Party in its proposed amendment has used the word 'indispensable'. This wording intends to reflect the need for a more stringent condition for the processing of the data of a non-suspect, because of the lack of a direct or indirect relation between the non-suspect and a specific investigation or crime.

---

[1] Position paper on Law Enforcement & Information Exchange in the EU, adopted at the Spring Conference of European Data Protection Authorities - Krakow (Poland), 25-26 April 2005

Proposed Amendment for a new article

Article 7a - Different categories of data subjects

1. Member States shall provide that the competent authorities, for the purposes referred to in Article 1(1), may only process personal data of the following different categories of data subjects:

(a) persons with regard to whom there are reasonable grounds for believing that they have committed or are about to commit a criminal offence;

(b) persons convicted of a crime;

(c) victims of a criminal offence, or persons with regard to whom certain facts give reasons for believing that he or she could be the victim of a criminal offence;

(d) third parties to the criminal offence, such as persons who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings, or a person who can provide information on criminal offences, or a contact or associate to one of the persons mentioned in (a) and (b);

2. Personal data of other data subjects than those referred to under paragraph 1 may only be processed

(a) as long as necessary for the investigation or prosecution of a specific criminal offence in order to assess the relevance of the data for one of the categories indicated in paragraph 1, or

(b) when such processing is indispensable for targeted, preventive purposes or for the purposes of criminal analysis, if and as long as this purpose is legitimate, well-defined and specific and the processing is strictly limited to assess the relevance of the data for one of the categories indicated in paragraph 1. This is subject to regular reviews, to take place at least every six months. Any further use is prohibited.

3. Member States shall provide that additional limitations and safeguards, according to national law, apply to the further processing of personal data relating to data subjects referred to in paragraph 1 (c) and (d).

3. On the rights of data subjects

The various elements of data protection legislation are grouped around three main actors: the data controllers/ processors, the supervisory authorities and the data subjects. For the latter category, both the Regulation and the Directive foresee a number of rights that can be exercised upon request, including a right to information, a right of access and a right to rectify or delete wrong or illegally processed data. In the Regulation, such rights have been implemented rather liberally, with a limited number of possible exceptions. The situation for the Directive is different, also because of the nature of the law enforcement sector. It is very

understandable that the police and judicial authorities cannot always be transparent about the ways they process data and which personal data is held in their files since this could jeopardise ongoing investigations.

At the same time the Working Party stresses that the current exemptions and limitations to the data subjects' rights are too broad. Without further explanation, it is in particular not justifiable why Member States should be allowed to exempt entire categories of personal data from the right of access. Accordingly, Articles 11(5) and 13(2) should be deleted. The Working Party stresses that a limitation of the rights of a data subject should always be a decision on a case-by-case basis, keeping in mind the specific circumstances of the request. This could for instance also lead to a decision to only partially deny the request. Furthermore, the Working Party maintains the view that exceptions to a fundamental right should at all times be interpreted restrictively.

4. On the use of privacy impact assessments in the law enforcement sector

In its first response to the draft Directive, the Working Party has already urged the European legislator to insert in the Directive provisions requiring a data protection impact assessment (DPIAs), including in the legislative procedure. It is particularly important in the field of law enforcement processing of personal data that DPIAs are carried out, especially given the increased risks to individuals of this processing. WP29 fails to see what is the paramount difference between the law enforcement sector and those sectors covered by the Regulation, where DPIAs are required to assess the risks of intended new data processing operations. Thorough safeguards when dealing with personal data are of the highest importance in this field of law and should therefore be considered and implemented before the data processing is started.

The Working Party is therefore pleased with the proposed amendments 27, 28, 110 and 113 of the European Parliament's rapporteur which introduce DPIA requirements for the law enforcement sector, to a very large extent comparable to those already in place in the Regulation. This important step for a better protection of the individuals' basic rights, even in an information rich environment like the law enforcement sector, should also be included in the Council general approach on the draft Directive.

However, it is on one point that the view of the Working Party differs from that of the rapporteur. Both in the amended Consideration 41 as well as the Article 25(2), the rapporteur introduces an obligation for the data protection authorities to assess all DPIAs and to make 'appropriate proposals to remedy (…) non-compliance'. WP29 considers that the assessment of DPIAs by data protection authorities should be done where appropriate.

5. On the powers of data protection authorities

The currently applicable Third Pillar Framework Decision contains little provisions on the duties and powers of data protection authorities and their possibilities and/or obligations to co-operate when carrying out their supervisory and enforcement tasks. In that respect, the draft Directive is a big step forward. Not only are provisions included on the need to have an independent supervisory authority for all data processing operations that take place within the scope of the Directive, but also a specific chapter is introduced on the co-operation between data protection authorities. The Article 29 Working Party welcomes the basic idea of these provisions.

Unfortunately, the provisions in the Directive are much less specific than those in the draft Regulation. In its general opinion on the legislative package, the Article 29 Working Party has therefore already stated the need to allow access of supervisory authorities to all premises. Also, the need has been stressed to bring the provisions of both instruments closer together to ensure consistency within the data protection legal framework. This is especially important in relation to the required co-operation between data protection authorities. Where data protection authorities do not have similar powers across the European Union, it may prove very difficult to protect the rights of our citizens. It could lead to situations where one authority would be allowed, based on their national implementing legislation, to enter the premises of a law enforcement agency to carry out an inspection without the prior consent of the agency involved, whereas another data protection authority in a neighbouring country does not have this power and thus can be denied access to the law enforcement agency's premises.

Regarding the information position of data protection authorities, co-operation may prove even more difficult if the powers of the authorities are not harmonised as is the current situation. A survey carried out by the Article 29 Working Party shows that some data protection authorities following a specific provision under national law have access to all information and documents they require, whether publicly available, confidential or classified, to fulfil their supervisory tasks on data processing in the law enforcement area. For other data protection authorities, similar access is given to staff members once they have obtained a security clearance from the relevant intelligence services. Yet other data protection authorities have no access to confidential and/or classified information at all.

Therefore, if data protection authorities are required to co-operate under the Directive, it is very important that all authorities involved have access to the same information. If not, they may not have the full picture of what is going on in a specific case and may not reach the same conclusion, thus possibly harming the interests of the data subject. The Article 29 Working Party therefore proposes to identify in the Directive the information which is accessible to data protection authorities when that information is necessary for the performance of their supervisory duties. This proposal does not intend to lower access levels to classified information currently held by DPAs.

In more general terms, the Working Party welcomes the proposals made by the European Parliament rapporteur on the powers of DPAs and supports the more detailed description of powers he suggests. The following amendment is to be seen as an addition to these proposals.

Proposed Amendment

Article 46 – Powers (paragraphs to be added)

1. Member States shall ensure that each supervisory authority shall have the investigative power to obtain from the controller or the processor access to any of its premises, including to any data processing equipment and means.
2. Member States shall ensure that each supervisory authority shall be provided with any information and all documents necessary for the exercise of their investigative powers. No secrecy requirements may be opposed to the requests of the supervisory authorities, except for the professional secrecy requirements referred to in Article 43.
3. Member States may provide that additional security screening in line with national law is required for access to information classified at a level similar to EU CONFIDENTIAL or higher. If no additional security screening is required under the law of the Member State of the supervisory authority, this must be recognised by all other Member States.

Done at Brussels, on 26 February 2013

For the Working Party
The Chairman
Jacob KOHNSTAMM