EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 6/2015

A further step towards comprehensive EU data protection

EDPS recommendations on the Directive for data protection in the police and justice sectors

28 October 2015

The European Data Protection Supervisor (EDPS) is an independent institution of the EU. The Supervisor is responsible under Article 41.2 of Regulation 45/2001 "With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies", *and* "…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data".

The Supervisor and Assistant Supervisor were appointed in December 2014 with the specific remit of being more constructive and proactive, and they published in March 2015 a five-year strategy setting out how they intended to implement this remit, and to be accountable for doing so [1].

This Opinion is another milestone in the EDPS strategy which underlines that the reform of the EU data protection rules is more urgent than ever. As highlighted in the recent Opinion 3/2015, the EDPS is together with fellow national data protection authorities an active partner in the discussions between the European Commission, Parliament and Council on the data protection reform, though he is not part of the final trilogue even on the Directive for data protection in the police and judicial sectors. We continue looking for robust, effective, practical and workable solutions. This Opinion is a further expression of our commitment. It will be followed in the following weeks by specific recommendations on the relevant text of the draft Directive, which will be also integrated in the EDPS Data Protection App for mobile devices.

This Opinion on the Directive for data protection in the police and justice sectors is in line with the EDPS's comprehensive Opinion on the Commission's proposed reform package adopted in March 2012. The views expressed in that Opinion remain valid. More than three and a half years on, however, we needed to update our advice to engage more directly with the positions of the co-legislators, and to offer specific recommendations [2]*. As with the 2012 Opinion, this Opinion is in line with the opinions and statements of the Article 29 Working Party.*

Table of Contents

I. This Directive is a significant step towards modern EU data protection

With the adoption of a general agreement on the Directive on data protection in the police and justice sectors[3], the Council has made a step towards a new framework for data protection in the EU.

One of the main shortcomings of the current EU data protection laws in these sectors is that it is a patchwork consisting of various rules for specific sectors and one instrument that is meant to be generally applicable, but is not. Indeed the Council Framework Decision on Data Protection of 2008[4] only applies where data are exchanged between Member States, not where data remains within the national domestic context. As a result of the present Directive, European citizens may finally benefit from an updated legislative instrument of the Union which will apply to the entire police and justice sectors.

The present proposal is also welcome because it confirms the need for comprehensive data protection. Where the General Data Protection Regulation aims at modernising the legislative regime for the private sector and most of the public sector, it would not be acceptable that the police and justice sectors, where so many sensitive personal data are processed, would not be brought up to date with the current legislative changes. A comprehensive system of protection is also needed, if only, because in our modern societies large amounts of personal data are exchanged between the various sectors.

This need for comprehensiveness is also a reason why the EDPS strongly recommends the simultaneous entry into force of the various instruments of the data protection reform. In this respect,

1. The transposition deadline of the Directive should remain two years, as proposed by the Commission, and not be extended to three years.
2. The Commission should present as soon as possible its proposal for a new instrument for data protection at the level of the EU institutions and bodies, replacing Regulation 45/2001.

II. The rules should ensure a high level of protection

Our call for comprehensiveness aims also at ensuring that the rules applicable to all sectors of society are consistent and ensure a high level of protection. This need for a high level of protection is the consequence of the embedding of the right to data protection in EU primary law, particularly in Article 16 TFEU and in Article 8 of the Charter of the Fundamental Rights of the Union. Data protection is closely related to the right to privacy, a fundamental value in our democratic societies which was already recognised in law in 1950 in the European Convention for Human Rights, and is now also included in Article 7 of the Charter.

The judgements of the Court of Justice in *Digital Rights Ireland*[5] and, recently, in *Schrems*[6] further confirm the importance of a high level of protection especially in connection with law enforcement and national security. In *Digital Rights Ireland*, the Court warns that the instrument of data retention was "*likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*"[7]. In *Schrems,* the Court considers that access of public authorities on a generalised basis to the content of electronic communications affects the very essence of the right to privacy[8].

These are just examples of an approach in the Treaty and confirmed by the highest EU Court, which emphasises the need for strong protection of individuals, as part of the values of the

European Union. This same approach should be reflected in the Directive, which must not only respect the legal obligations laid down in international law and EU law but should also reflect that privacy and data protection are essential values for individuals and for society as such.

The EDPS Opinion on the reform package of March 2012 particularl criticised the level of protection in the proposed Directive. We underlined that there was a very inadequate level of protection.

The main justification for a specific regime for data protection in the police and justice sectors relates to the specific nature of these sectors[9]. In other words, specific rules are needed, not rules that mainly contain exceptions to the principles of data protection laid down in the proposed General Data Protection Regulation. Data protection in the police and justice sectors should be fully consistent with the general rules and contain specifications only where necessary.

Furthermore, the general agreement of the Council aims at changing the nature of the Directive into an instrument providing minimum harmonisation, making it possible for Member States to provide for higher data protection safeguards under national law[10]. While we are not opposed to a discretionary power of Member States to further strengthen data protection safeguards at national level, we underline that it is the responsibility of the EU legislator, under Article 16 TFEU, to ensure high standards of data protection data and not to leave this to the Member States individually. Moreover, differentiation in standards between the Member States would hamper the free flow of information between the competent authorities and hence adversely affect the effectiveness of police and judicial cooperation. If too wide differences in standards exist amongst the Member States, this would also complicate the exchange of information with Europol, which has its own and, compared to the Directive, relatively strict data protection regime: Member States might chose to cooperate bilaterally, on the basis of the lowest common denominator.

In substance, the EU legislator should ensure that:

1. None of the provisions of the Directive decreases the level of protection that is currently offered by EU law -particularly the 2008 Council Framework Decision- and by the instruments of the Council of Europe[11].
2. The essential components of data protection, laid down in Article 8 of the Charter of the Fundamental Rights of the Union, are respected and that exceptions fulfil the strict test of proportionality, as specified in *Digital Rights Ireland*[12]. In this Opinion, we point particularly on the principle of purpose limitation, on the right to access of individuals to their personal data and on the control by independent data protection authorities[13].
3. The essential components of data protection are included in the Directive and not left to the discretion of the Member States[14].

III. The scope of the directive should be limited to the areas where specific rules are really necessary

We note that in the general agreement on the Directive in the Council, the scope is extended to the safeguarding against and the prevention of threats to public security[15], a domain outside criminal law that, under present law, is not covered by the current Council Framework Decision on Data Protection. Recital (11a) gives examples of what would be covered: police activities at demonstrations, major sporting events and riots, or, more in general, police activities maintaining law and order.

However, the definition of "*safeguarding against and the prevention of threats to public security*" remains unclear. This term can receive different interpretations and does not provide for a clear delimitation of the tasks of the police within the scope of the Directive [16]. We therefore recommend restricting the scope of the Directive to the activities of criminal law enforcement by police and judicial authorities, as was done in the original proposal of the Commission.

In the view of the EDPS, the notion of "competent authority", as defined under Article 3(13) should also remain as limited as possible: the performance of law enforcement tasks by non-public entities and organisations should be subject to the Regulation and not the Directive. These private entities and organisations do not need a specific regime. For example, airline companies or telecommunications operators, which are obliged by law to collect and hand over their data, should not become subject to the Directive as the main and original purpose of the collection of these data is totally different from the prevention, investigation, detection or prosecution of criminal offences. Recital (11) of the general agreement of the Council also refers to the retention of data by financial institutions and, in this specific case, to the obligation for these private entities, to be bound by a contract according to Article 21 of the Directive.

Furthermore[17], Article 2(3) of the Proposal excludes from its scope the processing of personal data in the course of an activity which falls outside the scope of Union law. The reference to national security was deleted from Article 2(3), but was reinserted in Recital (11b). As already stated by the EDPS, it is not always clear what this notion covers, as it depends on Member States national policy. We take note of the exception, but consider that it should not be used to legitimize the processing of personal data outside the scope of the Regulation and the Directive, for instance in the context of the fight against terrorism. As a consequence,

1. The Regulation should remain applicable to all activities which are not directly connected to the prevention, investigation, detection or prosecution or criminal offences or the execution of criminal penalties and where specific rules are proved to be necessary.
2. The performance of law enforcement tasks by non-public entities and organisations should be subject to the Regulation.

IV. Purpose limitation and special categories of data

We note that in the Council general agreement on the Directive, a second paragraph has been added in Article 4 that permits processing by the same or another controller for other purposes than for which the data are collected, in so far as the controller is authorised to process such data for such purpose according to applicable law provisions and the processing is necessary and proportionate to that other purpose. We would underline the importance of respect for the purpose limitation principle, which is a cornerstone of data protection law[18]. It must be ensured that data processed by competent authorities acting within the scope of the Directive are not further used for a totally different purpose, which will therefore be easily considered as incompatible (for instance, further use of data collected by the police for immigration purposes). We recommend that additional considerations are added to the text to delimit the notion of purpose limitation in the area of police and justice and to specify the notion of incompatible further processing. Similar considerations are currently being developed in the context of the Europol Regulation[19] and were mentioned in the recent Opinion of the EDPS on the General Data Protection Regulation (Article 6(2)).

We would also draw attention to the wording of the restriction on the processing of special categories of personal data in Article 8, which should be formulated as a prohibition to process those categories of data, except where a specific and express derogation applies (as proposed in the Parliament's text). The wording should not go below the current level of protection afforded on the basis of principle 2.4 of the Council of Europe Recommendation No. R(87)15. In substance,

1. It should be specified further what purpose limitation means in the areas of police and justice, and what incompatible further processing consists of.
2. The processing of special categories of personal data in the areas of police and justice should remain prohibited, except where a specific derogation of Article 8 of the Directive applies.

V. Data subjects rights

We recall that the rights of individuals in relation to the processing of their personal data are an essential component of the right to protection of personal data as guaranteed in Article 8 of the Charter. Such rights include the provision of information to individuals about the processing of their personal data and on the existence of their rights, so as to guarantee a fair processing, as well as the possibility to have access to their data and to ask for the rectification, erasure and/or restriction of the processing. We note that the provisions agreed in the Council General Approach do not fully guarantee the respect of individuals' rights, in particular in cases where a limitation to the individuals' rights is not, or no longer, applicable.

We therefore urge the co-legislators to ensure that the wording of Articles 10 to 16 respects the minimum requirements of those rights and does not go below the current level of data protection guaranteed in the Charter, the EU Treaties, and the international Treaties (particularly Convention 108).

It should be made clear in the text that limitations to individuals' rights, which are exceptions to a fundamental right, should be interpreted restrictively, as required by the Court’s case law. The result of those restrictions can be that, on a case-by-case basis and to the extent and for the period of time necessary, the communication of information to the individual may be refused. However, when the limitation ceases to apply, the individual should be able to exercise his or her rights fully. Furthermore, the individual concerned should always be informed of any refusal or restriction in writing; the communications of the reasoning may only be restricted, where this necessary for the interest of one of the legitimate grounds for refusal. In substance,

1. The original text of Article 10 of the Commission Proposal about the communication and modalities for exercising the rights of the data subject should be restored, as essential elements have been deleted in the Council’s general approach.
2. The notice to individuals should also include information about (i) the period for which data will be stored, (ii) the existence of a right to request access, rectification, erasure or restriction, and (iii) the category of recipients including third parties or international organisations, as provided in Article 11 of the Commission’s proposal.
3. The right of access should be established firmly in Article 12 and its exercise should not be made subject to the derogations provided in national legislation (as is foreseen in Article 12(1) in the Council’s general approach). It is the other way around: the right of access should be guaranteed as a matter of principle, which may only be derogated from

in given circumstances specifically provided for in the law and for as long as those limitations are valid.

VI. Ensuring control by independent Data Protection Authorities

We take the position that there is no need to differentiate between the powers conferred on Data Protection Authorities (DPAs) under the Regulation and the Directive. Supervision is an essential component of the fundamental right to data protection[20], and the level and intensity of supervision should not be dependent on the sector where the personal data are processed.

We note that the powers of the supervisory authorities conferred by the Directive are not aligned with the powers listed in Article 53 of the proposed Regulation[21]. For example, the power to impose penalties is only included by the European Parliament, whereas the Regulation provides for such a possibility. Another example is the lack of specification of the investigation powers of the supervisory authorities, which should not be reduced compared to the investigation powers provided by the proposed Regulation.

The possibility to exclude the courts, acting in their judicial capacity, from supervision raises serious issues of interpretation and scope[22]. We, therefore, recommend –with a reference to recital 55 of the proposal of the Commission– to keep the term "**genuine**" judicial activities which was deleted by the Council. The *rationale* for the Article 44(2) exemption seems to be, as emphasized by the recital, "*to safeguard the independence of judges in the performance of their judicial tasks*"[23]. In this context, we also note that, particularly considering the important differences in judicial systems among Member States, it is not always clear when and if public prosecutors are "independent judicial authorities", as well as when and to what extent their activities constitute "judicial activities". Relevant clarifications are therefore needed.

The European Data Protection Board (EDPB) will be composed, under the proposed Regulation, of a supervisory authority of each Member State and the EDPS. However, according to Article 39(2) of the proposed Directive, the supervisory authority is not necessarily the supervisory authority designated under the proposed Regulation. Therefore, a member of the EDPB is not necessarily in charge of the supervision within the scope of the Directive. We recommend clarifying this point, for example by specifying in Article 39(3) that where different authorities are designated under the Regulation and the Directive, they should coordinate their action in order to represent the voice of both authorities in the EDPB. In substance,

1. There is no need to differentiate the powers conferred on DPAs under the Regulation and the Directive.
2. The exception of supervisory powers of DPAs in the judicial sector should be limited to genuine" judicial activities, by also clarifying the position of public prosecutors' offices.

VII. International transfers and transfers to private parties

The judgement in *Schrems*[24] confirms the strict conditions for transfer of personal data to third countries. We recommend that Chapter V of the Directive is reconsidered with due respect to the Schrems judgement. This means, for example, that any adequacy decision must be based on a full assessment of the law enforcement sector. An adequacy decision should not deprive the supervisory authority of the power to investigate on a specific transfer and to take enforcement action in case the transfer does not meet the standard required.

In addition, we recommend ensuring that the transfer of personal data without an adequacy decision will be limited to situations where there is a legally binding instrument, or where there is a need to protect the vital interest of the data subject or in case of immediate and serious threat to public security[25]. We recommend adapting Article 34(6) and 36 accordingly.

Finally, we take the view that transfer to a private party may only take place, subject to the conditions which are currently laid down in Council of Europe Recommendation No. R(87)15. This transfer should only occur where the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if the communication is necessary so as to prevent a serious and imminent danger. We recommend adapting Article 36(aa) as suggested by the Council accordingly. In substance,

1. We recommend that Chapter V of the Directive is reconsidered, also with due respect to the Schrems judgement.
2. Transfers to a private party may only take place subject to the conditions which are currently laid down in Council of Europe Recommendation No. R(87)15.

VIII. Final provisions

This Opinion has already mentioned that, in order to ensure that a comprehensive system of data protection is required in the Union, the Directive should enter into force at the same time as the General Data Protection Regulation. The same argument applies to the need for ensuring that existing instruments with provisions on data protection are in compliance with the Directive.

We note that under the Commission proposal, the Directive leaves existing internal EU instruments unaffected, but obliges the Commission to assess the need for aligning these instruments with the Directive, within two years of its adoption (Article 61 (2)). The Council proposes to extend this deadline to five years after the adoption, which unduly extends the period of legal uncertainty.

Moreover, the Council removes the obligation to amend, where necessary, existing agreements involving the transfer of personal data concluded by the Member States. By contrast, the general agreement of the Council stipulates that all agreements concluded before the entry into force of the Directive remain unaffected. This might not only mean that provisions in those agreements which do not comply with the Directive remain in force for an unlimited period of time, but also that the Member States are empowered to conclude agreements with third countries during the period of transposition of the Directive, without considering its substantive content[26]. In substance,

1. It should be ensured that the need for aligning existing internal EU instruments with the Directive is reviewed as soon as possible and, in any event, no longer than two years after its entry into force.
2. Where necessary, existing agreements involving the transfer of personal data concluded by the Member States should be amended within a fixed time limit. Member States should be precluded from concluding agreements with third countries, during the period of transposition of the Directive.

Done in Brussels, 28 October 2015

Giovanni BUTTARELLI
European Data Protection Supervisor

Notes

[1] Vacancy notice for the European Data Protection Supervisor COM/2014/10354 (2014/C 163 A/02), OJ C 163 A/6 28.5.2014. The EDPS Strategy 2015-2019 promised to *"seek workable solutions that avoid red tape, remain flexible for technological innovation and cross-border data flows and enable individuals to enforce their rights more effectively on- and offline"*; Leading by example: The EDPS Strategy 2015-2019, March 2015.

[2] EDPS Opinion on the data protection reform package, 7.3.2015.

[3] 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, COM(2012)10 final; European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council 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, P7_TA(2014)0219.

[4] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60.

[5] Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), ECLI:EU:C:2014:238.

[6] Case C-362/14, Schrems, ECLI:EU:C:2015:650.

[7] Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), ECLI:EU:C:2014:238, at 37.

[8] Case C-362/14, Schrems, ECLI:EU:C:2015:650, at 94.

[9] See, e.g. Declaration (21) on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the Lisbon Treaty: *"The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields"*.

[10] Article 1a of the general agreement.

[11] This is also constantly underlined by the Rapporteur on the GDPR. See, e.g., Jan Philipp Albrecht, No EU Data Protection Standard Below the Level of 1995, EDPL 2015, 1, at 3-4.

[12] Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), ECLI:EU:C:2014:238.

[13] Control is an essential component of the protection of the individual: Recital (62) of 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, OJ L 281/31, and case law of the Court of Justice, most recently, Case C-362/14, Schrems, EU:C:2015:650, at 42.

[14] This would not be in line with the case law of the Court of Justice, particularly Joined cases C-293/12 and C-594/12, Digital Rights Ireland (C-293/12) and Seitlinger (C-594/12), ECLI:EU:C:2014:238, at 54-62.

[15] Article 1(1) of the general agreement.

[16] For instance, would the follow up of a suicide attempt or an administrative arrest fall within the scope?

[17] As underlined in EDPS Opinion on the data protection reform package, 7.3.2015, at 323.

[18] See Opinion 03/2013 of the Article 29 Data Protection Working Party on Purpose limitation, adopted on 2 April 2013.

[19] Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA.

[20] As most recently confirmed in Case C-362/14, Schrems, ECLI:EU:C:2015:650.

[21] See also EDPS Opinion on the data protection reform package, 7.3.2015, at III.8.

[22] See also EDPS Opinion on the data protection reform package, 7.3.2015, at III.8.

[23] The EDPS considers that the criterion for exempting from or including in the supervision by DPAs the data processing activity should be, respectively, whether the processing of personal data takes place in the context of the judicial activity ("trial", judicial proceeding, judicial activities in court cases) or in the context of other activities where judges might be involved in accordance with national law, rather than being based on the distinction tout court between categories of data controllers, namely the court, on the one side, and the public prosecutor -as example of "other judicial authority"- on the other side.
[24]Case C-362/14, Schrems, ECLI:EU:C:2015:650.
[25] See also EDPS Opinion on the data protection reform package, 7.3.2015, at III.7.
[26] The power may, under certain conditions, be limited by the principle of sincere cooperation (Article 4(3) TEU).