EUROPEAN DATA PROTECTION SUPERVISOR

Executive summary EDPS Opinion of 7 March 2012 on the data protection reform package

(The full text of this Opinion can be found in EN, FR and DE on the EDPS website http://www.edps.europa.eu)

(2012/C 192/05)

On 25 January 2012, the Commission adopted a package for reforming the EU rules on data protection, including a proposal for a Regulation containing the general rules on data protection and a proposal for a Directive on data protection in the law enforcement sector.

On 7 March 2012, the European Data Protection Supervisor (EDPS) adopted an Opinion which provides a detailed commentary on both legislative proposals. The full text of the Opinion can be found on the EDPS website: http://www.edps.europa.eu

In the Opinion, the EDPS briefly sketches the context of the proposals and provides his general assessment.

The EDPS welcomes the proposed Regulation as it constitutes a huge step forward for data protection in Europe. The proposed rules will strengthen the rights of individuals and make controllers more accountable for how they handle personal data. Furthermore, the role and powers of national supervisory authorities (alone and together) are effectively reinforced.

The EDPS is particularly pleased to see that the instrument of a *regulation* is proposed for the general rules on data protection. The proposed Regulation would be directly applicable in the Member States and would do away with many complexities and inconsistencies stemming from the different implementing laws of the Member States currently in place.

The EDPS is, however, seriously disappointed with the proposed Directive for data protection in the law enforcement area. The EDPS regrets that the Commission has chosen to regulate this matter in a self-standing legal instrument which provides for an inadequate level of protection, which is greatly inferior to the proposed Regulation.

A positive element of the proposed Directive is that it covers domestic processing, and thus has a wider scope than the current Framework Decision. However, this improvement only has added value if the Directive substantially increases the level of data protection in this area, which is not the case.

The main weakness of the package as a whole is that it does not remedy the lack of comprehensiveness of the EU data protection rules. It leaves many EU data protection instruments unaffected such as the data protection rules for the EU institutions and bodies, but also all specific instruments adopted in the area of police and judicial cooperation in criminal matters such as the Prüm Decision and the rules on Europol and Eurojust. Furthermore, the proposed instruments taken together do not fully address factual situations which fall under both policy areas, such as the use of PNR or telecommunication data for law enforcement purposes.

As regards the proposed Regulation, one horizontal issue is the relationship between EU and national law. The proposed Regulation goes a long way in creating a single applicable law for data protection in the EU, however there is still more space for coexistence and interaction between EU law and national law than one might assume at first sight. The EDPS takes the view that the legislator should better acknowledge this.

A second issue of general importance arises from the numerous provisions which empower the Commission to adopt delegated or implementing acts. The EDPS welcomes this approach in so far as it contributes to the consistent application of the Regulation, but has reservations about the extent to which essential legal provisions are left to delegated powers. Several of these empowerments should be reconsidered.

On a detailed level, the EDPS points to the main positive elements of the proposed Regulation, which are:

— the clarification of the scope of application of the proposed Regulation,

— the enhanced transparency requirements towards the data subject and the reinforcement of the right to object,

— the general obligation for controllers to ensure and be able to demonstrate compliance with the provisions of the Regulation,

— the reinforcement of the position and role of national supervisory authorities,

— the main lines of the consistency mechanism.

The main negative elements of the proposed Regulation are:

— the new ground for exceptions to the purpose limitation principle,

— the possibilities for restricting basic principles and rights,

— the obligation for controllers to maintain documentation of all processing operations,

— the transfer of data to third countries by way of derogation,

— the role of the Commission in the consistency mechanism,

— the mandatory nature of imposing administrative sanctions.

As regards the Directive, the EDPS takes the view that the proposal, in many aspects, does not meet the requirement of a consistent and high level of data protection. It leaves all existing instruments in the area unaffected, and in many instances there is no justification whatsoever for departing from the provisions of the rules in the proposed Regulation.

The EDPS underlines that whilst the law enforcement area requires some specific rules, every departure from the general data protection rules should be duly justified based on a proper balance between the public interest in law enforcement and citizens' fundamental rights.

The EDPS is concerned in particular with regard to:

— the lack of clarity in the drafting of the principle of purpose limitation,

— the absence of any obligation on competent authorities to be able to demonstrate compliance with the Directive,

— the weak conditions for transfers to third countries,

— the unduly limited powers of supervisory authorities.

The following recommendations are made.

Recommendations on the entire reform process

— Announce publicly the time schedule on the second stage of the reform process as soon as possible.

— Incorporate the rules for EU institutions and bodies in the proposed Regulation or at least have aligned rules in force when the proposed Regulation applies.

— Present as soon as possible a proposal for common rules for the Common Foreign and Security Policy, based on Article 39 TEU.

Recommendations on the proposed Regulation

Horizontal issues

— Add a provision clarifying the territorial scope of application of national law under the Regulation.

— Reconsider the delegation of power in Articles 31(5) and (6), 32(5) and (6), 33(6) and (7), 34(2)(a) and 44(1)(d) and (7).

— Provide appropriate and specific measures for MSMEs in selected implementing acts only, and not in delegated acts of Articles 8(3), 14(7), 22(4) and 33(6).

— Refine the notion of 'public interest' in each provision in which it is used. Specific public interests should be explicitly identified in relation to the context of the intended processing in each relevant provision of the proposal (see in particular, recital 87, Articles 17(5), 44(1)(d) and 81(1)(b) and (c)). Additional requirements could include that the ground can only be invoked in specifically pressing circumstances or on imperative grounds laid down in law.

Chapter I — General provisions

— Article 2(2)(d): insert a criterion to differentiate public and domestic activities based on the *indefinite* number of individuals who can access the information.

— Article 2(2)(e): provide that the exception applies to competent *public* authorities. Recital 16 should be made consistent with Article 2(2)(e).

— Article 4(1)(2): add a clearer explanation in a recital insisting on the fact that as soon as there is a close relation between an identifier and a person this will trigger the application of the data protection principles.

— Article 4(13): refine the criteria to identify the main establishment of the relevant controller, taking into account the 'dominant influence' of one establishment over others in close connection to the power to implement personal data protection rules or rules relevant for data protection. Alternatively, the definition could focus on the main establishment of the group as a whole.

— Add new definitions on 'transfer' and 'restriction of processing'.

Chapter II — Main principles

— Article 6: Add a recital to further clarify what falls under a task carried out 'in the public interest or in the exercise of public authority' in Article 6(1)(e).

— Article 6(4): delete the provision or at the very least restrict it to further processing of data for incompatible purposes on the grounds contained in Article 6(1)(a) and 6(1)(d). This would also require an amendment of recital 40.

— Add a new provision on the representation of all individuals lacking sufficient (legal) capacity or who are otherwise unable to act.

— Article 9: include offences and matters which have not led to convictions in the special categories of data. Extend the requirement of control of official authority to all grounds indicated in Article 9(2)(j).

— Article 10: make it more explicit in recital 45 that the data controller should not be able to invoke a possible lack of information to refuse a request of access, when this information can be provided by the data subject to enable such access.

Chapter III — Rights of the data subject

— Article 14: include information on the existence of certain processing operations which have a particular impact on individuals, as well as the consequences of such processing on individuals.

— Article 17: develop the provision further to ensure its effectiveness in reality. Delete Article 17(3)(d).

— Article 18: clarify that the exercise of the right is without prejudice to the obligation in Article 5(e) to delete data when they are no longer necessary. Ensure that Article 18(2) is not limited only to data that has been provided by the data subject on the basis of consent or a contract.

— Article 19: clarify what the controller should do in case of disagreement with the data subject and align with Article 17(1)(c). Explain in a recital what may qualify as 'compelling legitimate grounds'.

— Article 20: include the right of individuals to submit their point of view in Article 20(2)(a), as in the current Article 15 of Directive 95/46/EC.

— Article 21: introduce detailed guarantees that national law should specify the objectives pursued by the processing, the categories of personal data to be processed, the specific purposes and means of processing, the controller, the categories of persons authorised to process the data, the procedure to be followed for the processing, and the safeguards against any arbitrary interferences by public authorities. Include as additional safeguards informing of data subjects of a restriction and of their right to refer the matter to the supervisory authority to obtain indirect access. Add in Article 21 that the possibility of applying restrictions to the processing performed by private controllers for law enforcement purposes should not force them to retain data in addition to those strictly necessary for the original purpose pursued nor to change their IT architecture. Delete the ground contained in Article 21(1)(e).

Chapter IV — Controller and processor

— Article 22: refer explicitly to the principle of accountability, in any event in recital 60. Merge Article 22(1) and (3) and mention explicitly that measures should be *appropriate* and *effective*. Include a general provision preceding the specific obligations in Article 22(2) developing the concept of 'management control', including the assignment of responsibilities, training of staff, and adequate instructions and requiring that the controller should at least have an overview and a general inventory of the processing operations within the scope of his responsibility. Add a new paragraph to provide that when the controller decides or is obliged to publish a regular report of its activities this report should also contain a description of the policies and measures referred to in Article 22(1).

— Article 23: refer in Article 23(2) and recital 61 to the fact that data subjects should in principle be left the choice to allow use of their personal data in a broader way.

— Article 25(2)(a): delete the exception for adequate third countries.

— Article 26: add the obligation of the processor to take account of the principle of data protection by design to the list of specifications contained in Article 26(2).

— Article 28: reconsider or delete the exemptions of Article 28(4).

— Article 30: clarify Article 30 to ensure the overall responsibility of the controller and add the obligation on the controller to adopt an information security management approach within the organisation, including where appropriate the implementation of an information security policy specific to the data processing performed. Include an explicit reference to the DPIA in Article 30.

— Articles 31 and 32: specify the criteria and requirements for establishing a data breach and the circumstances in which it should be notified. Change the time limit of 24 hours in Article 31 to no later than 72 hours.

— Article 33: the list of processing operations contained in Article 33(2)(b), (c) and (d) should not be limited to processing on a large scale basis. Align Article 33(5) with recital 73. Limit Article 33(6) to non essential elements. Clarify that the size of a company should never lift the obligation of performing a DPIA with regard to the processing operations which present specific risks.

— Article 34: move Article 34(1) to Chapter V of the proposed Regulation.

— Articles 35 to 37: lower the threshold of 250 employees in Article 35(1) and clarify the scope of Article 35(1)(c). Add guarantees, in particular stronger conditions for the DPO's dismissal and ensure in Article 36(1) that the DPO is given access to all information relevant, and to premises necessary to perform his duties. Include in Article 37(1)(a) the role of the DPO in raising awareness.

Chapter V — Transfer to third countries

— State in recital 79 that the non-applicability of the Regulation to international agreements is restricted in time only to already existing international agreements.

— Insert a transitional clause providing for the review of these international agreements within a set time in order to align them with the Regulation.

— Article 41 (and recital 82): clarify that in the case of a non-adequacy decision, transfers should be allowed only under appropriate safeguards or if such transfer falls under the derogations set forth in Article 44.

— Article 42: Ensure that the possibility of using non-legally binding instruments to provide appropriate safeguards should be clearly justified and limited only to cases where the necessity to rely on such instruments has been demonstrated.

— Article 44 (and recital 87): Add that the possibility to transfer data should only concern occasional transfers and be based on a careful assessment of all the circumstances of the transfer on a case by case basis. Replace or clarify the reference to 'appropriate safeguards' in Article 44(1)(h) and in Article 44(3).

— Recital 90: change the recital into a substantive provision. Put in place appropriate guarantees for these cases, involving judicial guarantees as well as data protection safeguards.

Chapters VI and VII — Independent supervisory authorities, cooperation and consistency

— Article 48: include a role for the national parliaments in the procedure of appointment of members of supervisory authorities.

— Article 52(1): include duty to develop guidelines on the use of the different enforcement powers, where necessary coordinated at EU level in the Board. This could possibly be included in Article 66 as well.

— Article 58: replace the word 'immediately' in Article 58(6) by 'without delay' and extend the deadline of one month in Article 58(7) to two months/eight weeks.

— Article 58: give more weight to the majority rule by ensuring that a request by one authority could be submitted to vote in case the issue at stake does not relate to one of the main measures described in Article 58(2).

— Articles 59 and 60: limit the power of the Commission by deleting the possibility to overrule a decision of a national supervisory authority in a specific matter through an implementing act. Ensure that the role of the Commission consists in an initial phase in triggering the seizure of the Board, as foreseen in Article 58(4), and in a subsequent phase in the power to adopt opinions. Insert a reference to a further procedure before the Court of Justice, in the context of an infringement procedure or of a request for interim measures such as a suspension order.

— Article 66: add that the Board shall be consulted in the context of adequacy assessments.

— Reconsider the current assessment of the impact of the secretariat of the European Data Protection Board in terms of financial and human resources (see the Annex to the present Opinion, available on the EDPS website).

Chapter VIII — Remedies, liability and sanctions

— Articles 73 and 76: provide clarity about the mandate that the organisation must obtain from data subjects and the degree of formality required. Introduce a wider provision on collective actions.

— Article 74(4): limit the type of 'concern' of a data subject which could trigger the proceedings and restrict it to a more precise risk of impact on the data subject's rights.

— Article 75(2): specify that the derogation does not apply to a public authority of a third country.

— Article 76(3) and (4): insert a more systematic information procedure at the level of courts.

— Clarify the interaction with the Brussels I Regulation.

— Clarify the compatibility of the use of information obtained from a controller (on the basis of Article 53) with the general right against self-incrimination.

— Article 77: add that a data subject should always be able to address the controller, regardless of where and how the damage arose with regard to settlement of damage. Insert the subsequent settlement of the damage between the controller and the processor, once the distribution of liability among them has been clarified. Add that this should also apply to the compensation of immaterial damage or distress

— Introduce a provision using the concept of single economic entity or single undertaking to allow holding liable the group for the breach committed by a subsidiary.

— Article 79: insert a margin of appreciation for supervisory authorities with regard to administrative sanctions. Add specifications highlighting the circumstances in which an administrative sanction shall be imposed. Ensure that non-compliance with a specific order of a supervisory authority normally qualifies for a higher administrative sanction than a single breach of the same general provision.

Chapter IX — Specific data processing situations

— Article 80: rephrase Article 80 and state that Member States shall provide for exemptions or derogations from the provisions of the Regulation as indicated if such is *necessary* for reconciling the right to data protection with the right to freedom of expression. Add, in the provision or in a recital, that when reconciling the two fundamental rights the essence of both rights should not be impaired.

— Add a substantive provision on public access to documents stating that personal data in documents held by public authorities and bodies may be publicly disclosed if such is 1. provided for by EU or national law, 2. necessary for reconciling the right to data protection with the right of public access to official documents and 3. constitutes a fair balance of the various interests involved.

— Replace in Articles 81, 82, 83 and 84 the wording 'within the limits of this Regulation' by 'without prejudice to this Regulation'.

— Article 81: Align Articles 81(1)(3) and 9(3) and clarify the scope and nature of Article 81. Further direction should be given on the requirement of consent, the determination of responsibilities and the security requirements.

— Article 83: include additional safeguards if special categories of data are processed. Make clear in Article 83(1) that the point of departure for research purposes should be that such processing is done with use of anonymised data. Clarify what is meant by the word 'separately' and ensure that separate storage actually protects the data subjects. Refer in Article 83(1)(b) to 'data which enables to relate certain information to a data subject' instead of 'data enabling the attribution of information to an identified or identifiable data subject'. Exclude the limitation to rights of individuals via delegated acts.

Recommendations on the proposed Directive

Horizontal issues

— Article 59: specific acts in the area of police and judicial cooperation in criminal matters should be amended at the latest at the moment the Directive enters into force.

— Add a new provision introducing an evaluation mechanism for regular evidence based assessments of whether data processing activities of a certain scale do actually constitute a necessary and proportionate measure for the purposes of preventing, detecting, investigation and prosecuting criminal offences.

— Add a new provision to ensure that transfer of personal data from law enforcement authorities to other public bodies or to private parties is only permissible under specific and strict conditions.

— Add a new provision on specific safeguards in relation to the processing of data of children.

Chapters I and II — General provisions and principles

— Article 3(4): substantiate further in line with Article 17(5) of the proposed Regulation.

— Article 4(b): include clarification in a recital stating that the notion of 'compatible use' is to be interpreted restrictively.

— Article 4(f): align with Article 5(f) of the proposed Regulation and amend Articles 18 and 23 accordingly.

— Article 5: include non-suspected persons as a separate category. Delete 'as far as possible' and specify the consequences of the categorisation.

— Article 6: delete 'as far as possible' in paragraphs 1 and 2.

— Article 7(a): change into a self standing provision ensuring in a general manner that all data processing operations are provided for by law, thereby fulfilling the requirements of the EU Charter of Fundamental Rights and ECHR.

— Article 7(b) to (d): replace by an additional, separate provision which exhaustively lists the grounds of public interest for which a derogation to the purpose limitation principle can be allowed.

— Add a new provision on the processing of personal data for historical, statistical and scientific purposes.

— Add an obligation for the competent authority to put mechanisms in place to ensure that time limits are established for the erasure of personal data and for a periodic review of the need for the storage of the data, including fixing storage periods for the different categories of personal data as well as regular checks on their quality.

— Article 8: include the strict wording of recital 26 in Article 8. Include what is envisaged by suitable measures going beyond regular safeguards.

Chapter III — Rights of the data subject

— Article 10: delete the reference to 'all reasonable steps' in Article 10(1) and (2). Include an explicit time limit in Article 10(4) and state that information should be given to the data subject at the latest within one month of receipt of the request. Replace the wording 'vexatious' in Article 10(5) by 'manifestly excessive' and provide further guidance on this notion in a recital.

— Add a new provision requiring the controller to communicate to each recipient to whom the data have been disclosed, any rectification, erasure or change of the data either or not carried out in accordance with Articles 15 or 16, unless this proves impossible or involves a disproportionate effort.

— Articles 11 and 13: add a sentence in Article 11(4) and Article 13(1) stating that the controller should be required to assess in each specific case by way of a concrete and individual examination whether partial or complete restrictions for one of the grounds applies. Ensure a limited interpretation of the scope of Article 11(5) and Article 13(2). Delete the word 'omitting' in Article 11(4) and Recital 33.

— Articles 15 and 16: add grounds and conditions for restricting the right to rectification and the right to erasure.

— Article 16: use the wording 'shall restrict processing' instead of 'shall mark' in Article 16(3). Include in Article 16 the obligation for the controller to inform the data subject before lifting any restriction on processing.

Chapter IV — Controller and processor

— Article 18: state, also in Article 4(f), that the documentation requirement stems from the general obligation to be able to *demonstrate* compliance with the Directive. Include a requirement to keep information on the legal ground on which the data is transferred, with a substantive explanation especially if a transfer is based on Articles 35 or 36.

— Article 19: substantiate the notion of data protection 'by default'.

— Article 23(2): align with Article 28(2) of the proposed Regulation.

— Article 24: include the identity of the recipients of the data.

— Insert a new provision, requiring the competent authorities to carry out a DPIA, unless a specific assessment, equal to a DPIA, has already been made during the legislative process.

— Article 26: align more closely with the procedures developed in Article 34(2) of the proposed Regulation.

— Article 30: deal with the issue of conflict of interest and lay down a minimum term of office of two years.

— Article 31: provide for an appropriate administrative attachment with due regard for the independent role of the DPO and with a view in particular to avoiding possible uneven relations or influence by high rank controllers.

Chapter V — Transfer to third countries

— Article 33: add the requirement that the transfer may only take place if the controller in the third country or the international organisation is a competent authority within the meaning of the proposed Directive.

— Article 35: delete Article 35(1)(b) or as a minimum include the requirement of a prior authorisation of the supervisory authority.

— Article 36: clarify in a recital that any derogation used to justify a transfer needs to be interpreted restrictively and should not allow the frequent, massive and structural transfer of personal data; even an individual case should not allow wholesale transfers of data and should be limited to data strictly necessary. Add additional safeguards such as the obligation to specifically document the transfers.

— Articles 35 and 36: add that in case of a negative decision on adequacy, transfers should be based (i) on Article 35(1)(a) if there is a legally binding international agreement allowing for the transfer under specific conditions guaranteeing an adequate protection, or (ii) on the derogations of Article 36(a) or (c).

Chapters VI and VII — Oversight mechanisms

— Article 44: provide more guidance in a recital on what is meant to be covered by 'judicial capacity'.

— Article 46: align the powers of the supervisory authorities vis-à-vis national police authorities with the powers under the proposal for a Regulation. Align Article 46(a) with Article 53 of the proposed Regulation and change the wording 'such as' in Article 46(a) and (b) into 'including'.

— Article 47: include that the annual activities report of the supervisory authorities must be presented to the national parliament and made public.

— Article 48: include the provisions of Article 55(2) to (7) of the proposed Regulation in Article 48.

— Consider the need for an enhanced cooperation mechanism also in the scope of application of the proposed Directive.

(Abridged version. The full text of this Opinion can be found in EN, FR and DE on the EDPS website http://www.edps.europa.eu)

Done at Brussels, 7 March 2012.

Peter HUSTINX

European Data Protection Supervisor