EUROPEAN DATA PROTECTION SUPERVISOR

Executive summary of the Opinion of the European Data Protection Supervisor on the Commission's Communication on 'Unleashing the potential of cloud computing in Europe'

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

(2013/C 253/03)

I. **Introduction**

I.1. *Aim of the Opinion*

1. In view of the importance of cloud computing in the evolving information society and of the ongoing policy debate within the EU on cloud computing, the EDPS has decided to issue this Opinion on his own initiative.

2. This Opinion responds to the Communication of the Commission 'Unleashing the potential of cloud computing in Europe' of 27 September 2012 (hereafter 'the Communication') ([1]), which sets forth key actions and policy steps to be taken to speed up the use of cloud computing services in Europe. The EDPS was consulted informally before the adoption of the Communication and provided informal comments. He welcomes that some of his comments have been taken into account in the Communication.

3. However, given the scope and importance of the ongoing debate on the relationship between cloud computing and the data protection legal framework, this Opinion is not limited to the subjects addressed in the Communication.

4. The Opinion focuses especially on the challenges that cloud computing poses for data protection and how the proposed data protection regulation (hereafter 'the proposed regulation') ([2]) would tackle them. It also comments on the areas for further action identified in the Communication.

I.2. *Background*

5. In the context of the general policy debate in the EU on cloud computing, the following activities and documents are of specific importance:

— following its 2010 Communication on the digital agenda for Europe ([3]) the Commission launched a public consultation on cloud computing in Europe from 16 May until 31 August 2011 and published the results on 5 December 2011 ([4]),

— on 1 July 2012, the Article 29 Working Party ([5]) adopted an opinion on cloud computing (hereafter 'the WP29 Opinion') ([6]) that analyses the application of the current data protection rules set forth in Directive 95/46/EC to cloud computing service providers operating in the European Economic Area (EEA) and their clients ([7]),

— on 26 October 2012, a resolution on cloud computing was adopted by the Data Protection and Privacy Commissioners during their 34th International Conference ([8]).

([1]) COM(2012) 529 final.
([2]) COM(2012) 11 final.
([3]) COM(2010) 245 final.
([4]) http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf
([5]) The Article 29 Working Party is an advisory body established pursuant to Article 29 of Directive 95/46/EC. It is composed of representatives of national supervisory authorities and the EDPS, and a representative of the Commission.
([6]) WP29 Opinion 05/2012 on cloud computing, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
([7]) In addition, at national level data protection authorities in several Member States have issued their own guidance on cloud computing, for example in Italy, Sweden, Denmark, Germany, France, and the UK.
([8]) Resolution on cloud computing adopted during the 34th International Conference of Data Protection and Privacy Commissioners, Uruguay, 26 October 2012.

I.3. *Communication on cloud computing*

6. The EDPS welcomes the Communication. It identifies three specific key actions required at EU level to accompany and promote the use of cloud computing in Europe, as follows:

— key action 1: cutting through the jungle of standards,

— key action 2: safe and fair contract terms and conditions,

— key action 3: establishing a European Cloud Partnership to drive innovation and growth from the public sector.

7. Additional policy steps are also foreseen such as measures to stimulate the use of cloud computing by fostering research and development or awareness-raising, as well as the need to address key themes related to cloud services — including amongst others data protection, access by law enforcement, security, liability of intermediary service providers — through a reinforced international dialogue.

8. Data protection is mentioned in the Communication as an essential element for ensuring the success of cloud computing deployment in Europe. The Communication notes ([1]) that the proposed regulation addresses many of the concerns raised by cloud service providers and by cloud clients ([2]).

I.4. *Focus and structure of the Opinion*

9. This Opinion has three goals.

10. The first goal is to highlight the relevance of privacy and data protection in the current discussions on cloud computing. More particularly, it underlines that the level of data protection in a cloud computing environment must not be inferior to that required in any other data processing context. cloud computing practices can only be developed and applied legally if they guarantee that this level of data protection is respected (see Chapter III.3). The Opinion takes into account the guidance provided in the WP29 Opinion.

11. The second goal is to further analyse the main challenges that cloud computing brings for data protection in the context of the proposed data protection regulation, in particular the difficulty to establish unambiguously the responsibilities of the different actors and the notions of controller and processor. The Opinion (mainly, Chapter IV) analyses how the proposed regulation would, as it is currently put forward ([3]), help ensure a high level of data protection in cloud computing services. It therefore builds upon the views developed by the EDPS in his Opinion on the data protection reform package (hereafter 'the EDPS Opinion on the data protection reform package') ([4]) and complements it by considering specifically the cloud computing environment. The EDPS underlines that his Opinion on the data protection reform package fully applies in relation to cloud computing services and must be considered as a basis for the present Opinion. Moreover, some of the issues mentioned there — such as his analysis of the new provisions on data subjects' rights ([5]) — are sufficiently clear and will therefore not be developed further in this Opinion.

12. The third goal is to identify areas that require further action at EU level from a data protection and privacy perspective, in view of the cloud strategy put forward by the Commission in the Communication. They include, amongst others, providing further guidance, standardisation efforts, carrying out further risks assessments for specific sectors (such as public sector), developing standard contract terms and conditions, engaging into international dialogue on issues related to cloud computing and ensuring effective means of international cooperation (to be developed in Chapter V).

([1]) See page 8 of the Communication, section on 'Digital agenda actions on building digital confidence'.
([2]) The term 'cloud clients' is generally used in this Opinion to refer to customers, acting in their capacity as businesses, and to consumers, acting in their capacity of individual end users.
([3]) Account should be taken of the fact that the proposal for a regulation is currently being discussed by the Council and the European Parliament following the ordinary legislative procedure.
([4]) The Opinion is available at: http://www.edps.europa.eu
([5]) See EDPS Opinion, in particular paragraphs 140 to 158.

13. The Opinion is structured as follows: Section II provides an overview of the main characteristics of cloud computing and the related data protection challenges. Section III reviews the most relevant elements of the existing EU legal framework and of the proposed regulation. Section IV analyses how the proposed regulation would help address the data protection challenges raised by the use of cloud computing services. Section V analyses the Commission's suggestions for further policy developments and identifies the areas where further work might be needed. Section VI contains the conclusions.

14. While many of the considerations of this Opinion apply to all environments in which cloud computing is used, this Opinion does not address the use of cloud computing services specifically by EU institutions and bodies subject to the supervision of the EDPS under Regulation (EC) No 45/2001. The EDPS will issue guidelines to these institutions and bodies on this subject separately.

VI. **Conclusions**

121. As described in the Communication, cloud computing offers many new opportunities to businesses, consumers, and the public sector for the management of data through the use of remote external IT resources. At the same time, it presents many challenges in particular as to the appropriate level of data protection offered to data processed therein.

122. The use of cloud computing services raises a major risk of seeing responsibility evaporating in relation to processing operations carried out by cloud service providers, if the criteria for applicability of EU data protection law are not sufficiently clear and if the role and the responsibility of cloud service providers are defined or understood too narrowly, or are not implemented effectively. The EDPS emphasises that the use of cloud computing services cannot justify a lowering of data protection standards as compared to those applicable to conventional data processing operations.

123. In this respect, the proposed data protection regulation, as it has been put forward, would provide many clarifications and tools that would help ensure that a satisfactory level of data protection is complied with by cloud service providers offering their services to clients based in Europe, in particular:

— Article 3 would clarify the territorial scope of the EU data protection rules and broaden its scope so that cloud computing services would be covered,

— Article 4(5) would introduce a new element of controllership, that is 'conditions'. This would be in line with the developing trend according to which, in view of the technical IT complexity underlying the provision of cloud computing services, it is necessary to expand the circumstances in which a cloud service provider may be qualified as the controller. This would better reflect the real level of influence on the processing operations;

— the proposed regulation would increase the responsibility and accountability of data controllers and processors, by introducing specific obligations such as data protection by design and by default (Article 23), data security breach notifications (Articles 31 and 32), and data protection impact assessments (Article 33). Furthermore, it would require controllers and processors to implement mechanisms to demonstrate the effectiveness of the data protection measures implemented (Article 22),

— Articles 42 and 43 of the proposed regulation would allow a more flexible use of international data transfer mechanisms, to help cloud clients and cloud service providers adduce appropriate data protection safeguards for the transfers of personal data to data centres or servers located in third countries,

— Articles 30, 31 and 32 of the proposed regulation would clarify the obligations of controllers and processors regarding the security of processing and information requirements in case of data breaches, laying the basis for a comprehensive and cooperative approach to the management of security between the different actors in a cloud environment,

— Articles 55 to 63 of the proposed regulation would reinforce cooperation of supervisory authorities and their coordinated supervision over cross-border processing operations, which is particularly crucial in an environment such as cloud computing.

124. The EDPS nonetheless suggests that, after having taken into account the specificities of cloud computing services, further clarifications be made in the proposed regulation on the following aspects:

— as concerns the territorial scope of the proposed regulation, to amend Article 3(2)(a) to read 'the offering of goods or services *involving processing of personal data of* such data subjects in the Union', or alternatively to add a new recital specifying that the processing of personal data of data subjects in the Union by non-EU based controllers offering services to EU based legal persons also falls within the territorial scope of the proposed regulation,

— to add a clear definition of the notion of 'transfer', as stated in his Opinion on the data protection reform package,

— to add a specific provision to clarify the conditions under which access to data stored in cloud computing services by non-EEA countries law enforcement bodies could be allowed. Such provision may also include the obligation for the recipient of the request to inform and consult the competent supervisory authority in the EU in specific cases.

125. The EDPS also underlines that further guidance will be necessary from the Commission and/or from supervisory authorities (in particular through the future European Data Protection Board) on the following aspects:

— to clarify which mechanisms should be put in place to ensure verification of the effectiveness of the data protection measures in practice,

— to assist processors with the use of BCRs and how they can comply with applicable requirements,

— to provide best practices on issues such as controller/processor's responsibility, the appropriate retention of data in the cloud environment, data portability, and the exercise of data subjects' rights.

126. Furthermore, the EDPS acknowledges that codes of conduct drawn up by the industry and approved by the relevant supervisory authorities could be a useful tool to enhance compliance as well as trust among the various players.

127. The EDPS supports the development by the Commission, in consultation with supervisory authorities, of standard contractual terms for the provision of cloud computing services that respect data protection requirements, in particular:

— to develop model contractual terms and conditions to be included in the commercial terms of cloud computing service offerings,

— to develop common procurement terms and requirements for the public sector, taking into account the sensitivity of the data processed,

— to further tailor international data transfer mechanisms to the cloud computing environment, in particular by updating the current standard contractual clauses and by putting forward standard contractual clauses for the transfer of data from processors based in the EU to processors located outside the EU.

128. The EDPS underlines that appropriate consideration must be given to data protection requirements in the development of standards and certification schemes, in particular:

— to apply the principles of privacy by design and privacy by default in the development of the standards,

— to integrate data protection requirements such as purpose limitation and storage limitation in the standards' design,

— the obligations of providers to provide their clients with the information necessary to perform a valid risk assessment and the security measures they implemented, as well as alerts about security incidents.

129. Finally, the EDPS stresses the need to address the challenges raised by cloud computing at an international level. He encourages the Commission to engage in an international dialogue on the issues raised by cloud computing, including jurisdiction and access by law enforcement, and suggests that many of these issues could be addressed in different international or bilateral agreements, such as mutual assistance agreements and also trade agreements. Global standards should be developed at international level to set forth minimum conditions and principles regarding the access to data by law enforcement bodies. He also supports the development by the supervisory authorities of effective international cooperation mechanisms, in particular as relates to cloud computing issues.

Done at Brussels, 16 November 2012.

Peter HUSTINX

European Data Protection Supervisor