EUROPEAN DATA
PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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[1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular Article 41 thereof[2],

HAS ADOPTED THE FOLLOWING OPINION:

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)[3], 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.

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.1.2001, p. 1.
[3] COM (2012) 529 final.

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')[4] 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[5] 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[6];

- On 1 July 2012, the Article 29 Working Party[7] adopted an opinion on Cloud Computing (hereafter the "WP29 Opinion")[8] 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[9];

- On 26 October 2012, a resolution on cloud computing was adopted by the Data Protection and Privacy Commissioners during their 34th International Conference[10].

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

[4] COM (2012) 11 final.

[5] COM (2010) 245 final.

[6] http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf.

[7] 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.

[8] 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.

[9] 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

[10] Resolution on cloud computing adopted during the 34th International Conference of Data Protection and Privacy Commissioners, Uruguay, 26 October 2012.

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[11] that the proposed Regulation addresses many of the concerns raised by cloud service providers and by cloud clients[12].

1.4. 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[13], 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')[14] 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[15] - 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

[11] See page 8 of the Communication, section on 'Digital Agenda Actions on Building Digital Confidence'.

[12] 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.

[13] 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.

[14] The Opinion is available at www.edps.europa.eu.

[15] See EDPS Opinion, in particular para. 140 to 158.

computing and ensuring effective means of international cooperation (to be developed in Chapter V).

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.

II. THE CLOUD COMPUTING ENVIRONMENT

II.1. Definitions

15. Cloud computing is evolving and includes a wide range of technological solutions and business practices. The term is used with different meanings in different contexts. The most widely used definition is that published by the US National Institute of Standards and Technology (NIST)[16] which states that "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*". The NIST document defines three service models (SaaS: Software as a Service, PaaS: Platform as a Service and IaaS Infrastructure as a Service) and four deployment models: public, private, community and hybrid cloud environments. In this Opinion, the terms and acronyms should be understood within the meaning of the NIST definition.

II.2. Impact of cloud computing on businesses and consumers

16. One of the major impacts expected from cloud computing is the reduction of costs for IT services, mainly based on economies of scale and more efficient use of information and communication infrastructures. Dynamic allocation and re-use of resources in larger pools allows reduction of capital expenditure for IT infrastructure and rationalizing of operations.

17. While cost saving effects are expected from all cloud deployment models, public (and to a lesser extent, community) cloud services could further reduce the cost for cloud clients when they would be charged only for the services that they actually used in terms of computing time, storage space and other resources, thus removing nearly all fixed costs for IT services. This pay-per-use model would allow a more

[16] US NIST SP 800-145, The NIST Definition of Cloud Computing, Sept. 2011, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

dynamic acquisition of services only when they are actually needed for business. Furthermore, it would make higher quality services accessible to small organisations, such as SMEs, that could not afford them under traditional models, due to the high entry costs for infrastructure, licenses and set-up costs and the lack of scalability[17]. These new opportunities are expected to open the way for innovative start-ups to offer a wide range of new services.

18. Third party applications on social media services can be seen as one example for such new opportunities in a SaaS environment. Any individual with sufficient technical knowledge, basic computing equipment and access to the Internet can develop and offer applications that operate in the environment provided by the social media service. The inherent multi-user capacity of cloud computing makes it the ideal model for new ways of social computing.

19. Mobile computing and cloud computing complement and reinforce each other and together build the basis for ambient intelligence[18] and the Internet of Things. Mobile devices offer ubiquitous access to cloud services, and cloud services allow mobile access to highly sophisticated services and huge data collections, beyond the physical limitations of mobile devices. Access to the cloud offers new opportunities to use smart phones and tablets, in the sense that browsers and apps can be used as the interface to cloud services.

II.3. Future consolidation of the cloud computing market

20. While the market for cloud computing services is still in a phase of strong growth, in the long term the market is likely to experience consolidation in the same way as other sectors, and it may evolve towards a limited number of providers offering services to a large number of customers.

21. Such concentration could reinforce the already existing imbalance in the cloud services market between the service providers and most of the users of their services. While governments and big companies may have the possibility to have private clouds established according to their requirements or to negotiate the service agreements with cloud providers at equal level, small and medium organisations from the public and private sectors and individual consumers will have to accept the terms and conditions as they are laid down by the service providers for public cloud services. This asymmetry could be exploited by service providers to set conditions for their services which are to the disadvantage of the clients by limiting providers' obligations and liability and restricting clients' rights, giving providers far reaching privileges and powers, even to unilaterally change terms and conditions of service to the disadvantage of the cloud client.

[17] Hosted web shops are one example that shows the potential of more dynamic and scalable models.

[18] Ambient Intelligence and Ubiquitous Computing refer to a vision where humans will be surrounded by intelligent interfaces everywhere, sometimes embedded in everyday objects, connected everywhere and always on, enabling people and devices to interact with each other and with the environment (A social and technological view of Ambient Intelligence in Everyday Life, EC IPTS, 2003).

II.4. Relevance of data protection in a cloud computing environment

22. Cloud computing facilitates the processing of big data collections[19] and the creation of new services and applications to monetize those data, such as social media applications or cloud services delivered through mobile devices. To the extent that these big data collections contain personal data, specific risks for privacy and data protection arise which require scrutiny and the development of appropriate safeguards.

23. Cloud computing raises a number of issues related to the protection of privacy and personal data that need to be properly addressed in service development and roll-out. Most of these concerns are relevant regardless of the service and deployment models. In addition, some cloud computing models include outsourcing, remote access and multi-tenant IT infrastructures and the data protection risks relating to these characteristics must also be taken into account.

24. First, in cloud environments the specific physical location of the data is usually not known by the client, and it is, in principle, not relevant for the service itself. From a service perspective, it is more relevant to consider from where the data can be accessed. However, the hosting location of data remains relevant with respect to the applicability of national law. This is even more obvious where (national) authorities would need physical access to data.

25. Second, the contractual asymmetry between service providers and clients described above may make it very difficult or even impossible for cloud clients acting as data controllers to comply with the requirements for personal data processing in a cloud computing environment. The asymmetry could also lead to an undesirable allocation of responsibility in relation to compliance with data protection law. If the qualification of data controller and processor does not appropriately reflect the level of control over the means of processing, the responsibility for the protection of personal data even risks to evaporate with the use of cloud computing.

26. Third, in cloud computing different players usually cooperate along the end-to-end value chain in order to deliver the service to the client. Also this leads to complex questions concerning the allocation of responsibilities, in particular when considering personal data processing requirements such as security of the data, access and auditing. This may be aggravated considerably when new providers can be added to the service dynamically during operation[20].

27. Fourth, cloud computing also leads to a considerable increase of transfers of personal data over networks, involving many different parties and crossing borders between countries, including outside the EU. Depending on the type of service offered, data can be replicated in multiple locations, in order to make them better accessible from anywhere in the world. Where personal data is processed in these

[19] 'Big data' is used to describe a massive volume of both structured and unstructured data that is so large that it is difficult to process with traditional database and software techniques. See "Big data: The next frontier for innovation, competition, and productivity" May 2011, McKinsey Global Institute, http://www.mckinsey.com/insights/mgi/research/technology_and_innovation/big_data_the_next_frontier_for_innovation.

[20] The difficulties in allocating responsibilities to the different actors, as controllers and processors (as mentioned in paragraphs 25-26), will be further developed in IV.2.

services, data controllers and processors must ensure compliance of these transfers with data protection rules.

28. Last but not least, cloud computing is still evolving. The technological characteristics and development of new trends in cloud computing will pose new challenges to data protection. One can not precisely predict how cloud computing will evolve. This Opinion therefore is based on the trends that can be currently observed in cloud computing[21].

III. OVERVIEW OF THE EU DATA PROTECTION LEGAL FRAMEWORK APPLICABLE TO CLOUD COMPUTING

III.1. The current EU legal framework

29. Data processing operations carried out in a cloud computing environment that fall within the territorial scope criteria of EU data protection law[22] must respect the EU data protection framework currently set forth in Directive 95/46/EC. The WP29 Opinion has provided guidance as to how the principles and rules established in the general data protection Directive must be applied to the cloud environment[23].

30. To the extent that processing in a cloud computing environment involves the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks (telecom operators), the processing must also comply with the ePrivacy Directive 2002/58/EC[24].

31. The e-commerce Directive 2000/31/EC[25] defines the rules applicable to certain aspects of information society services. Cloud computing services usually fall within the definition of information society services. The e-commerce Directive sets forth a limited regime of liability for intermediary service providers in respect of the legality of the content transmitted or hosted at the request of the recipient of the service. Article 1(5)(b) of the e-commerce Directive clarifies that its provisions are without prejudice to the rules on data protection of Directive 95/46/EC. In accordance with Directive 95/46/EC, the processing of personal data by Internet service providers falls within the scope of data protection law. Their level of

[21] Some of these issues are underlined in the Sopot Memorandum adopted on 2 April 2012 by the Berlin International Working Group on Data Protection in Telecommunications, http://www.datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf?1335513083.

[22] Processing operations fall within the scope of EU data protection law when they involve personal data processed automatically and such processing takes place in the context of the activities of an establishment of the controller located in the EU or by a controller located outside the EU that makes use of equipment located in the EU, in accordance with Articles 3 and 4 of Directive 95/46/EC.

[23] See footnote 8.

[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.07.2002 p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337, 18.12.2009, p. 11.

[25] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.07.2000, p. 1.

responsibility may vary depending on whether they act as a processor or as a controller. In the former case, their liability is focused on ensuring the confidentiality and security of the data, while in the latter they retain full responsibility for ensuring compliance with data protection requirements. In many cases where online intermediaries provide added value services (e.g. social networks and cloud based services), they may be considered to act as data controllers[26] (see detailed analysis in section IV.2 below).

III.2. The proposal for a Data Protection Regulation

32. The Proposal for a Data Protection Regulation adopted by the Commission on 25 January 2012 aims at providing a single set of rules within the EU for the processing of personal data by private companies and by the public sector[27]. As part of the review, the territorial scope of EU data protection law is redefined. The proposed rules build upon the general principles set forth in Directive 95/46/EC with the aim to update them to the digital environment, to simplify certain administrative burden (such as prior notifications) and to strengthen the rights of individuals, the responsibility of controllers and processors of personal data, and the powers of supervisory national authorities.

33. The proposed Regulation introduces a number of new obligations for data controllers, such as 'data protection by design' and 'data protection by default', accountability, data protection impact assessments, personal data breach notifications, as well as the right to be forgotten and the right to data portability. As these new proposals maintain the technologically neutral approach of EU data protection and do not focus on any specific technology, they also encompass and apply to the cloud computing environment.

III.3. Importance of ensuring a high level of data protection in cloud computing services

34. At an international level, data protection authorities have recently emphasised[28] that it is essential that the challenges raised by the use of cloud computing services do not lead to a lowering of data protection standards as compared to those applicable to conventional data processing operations.

35. The EDPS wishes to emphasize that all the data protection principles laid down in Article 6 of Directive 95/46/EC and in Article 5 of the proposed Regulation (such as fairness and lawfulness, purpose limitation, proportionality, accuracy, limited

[26] See in particular recital 47 of Directive 95/46/EC: "Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; *whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service.*" (emphasis added). See also for example the WP 29 Opinion 5/2009 on online social networking, 12 June 2009, page 5, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf.

[27] In accordance with Article 2(2)(e), the proposed Regulation would not apply to competent authorities that process personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties..

[28] See footnote 10.

data retention periods) must be fully taken into account for the processing of personal data by cloud computing service providers.

36. Overall, due to the diversity of available cloud computing offerings, and in the absence of well-recognised legal and contractual standards covering all layers of cloud computing architecture, the data protection impact of each cloud computing service must currently be assessed on an *ad hoc* basis, in order to define the most appropriate safeguards that must be implemented.

IV. ANALYSIS OF THE IMPACT OF THE PROPOSED DATA PROTECTION REGULATION ON CLOUD COMPUTING SERVICES

37. The proposed Regulation provides an updated framework for data protection that takes into account technological developments, while at the same time remaining technologically neutral. It contains provisions that have particular relevance to the cloud computing environment.

38. This chapter of the Opinion analyses how the proposed Regulation would help address issues raised by the use of cloud computing services and underlines other issues that need to be taken into consideration by the legislator during the legislative process. It also highlights good practices in respect of data processing through cloud computing services.

IV.1. Clarification of the applicability of EU data protection law to processing operations carried out through Cloud Computing services

39. Article 2 of the proposed Regulation deals with its material scope of application. It includes, *inter alia*, a clarification that the proposed Regulation would not apply to processing carried out by ‘a natural person without any gainful interest in the course of its own exclusively personal or household activity’ (the so-called "household exception"). However, recital 15[29] explains that the rules of the proposed Regulation would apply to controllers or processors that provide the means for processing personal data for such personal or domestic activities. This specification is important in relation to providers of cloud services for consumers: even though consumers use the services for personal purposes, the provider is nevertheless an entity which, on the one hand, provides the means for processing and, on the other hand, engages in such activity for commercial purposes. The "household exception" therefore would not apply to these providers.

40. As far as the users are concerned, the EDPS notes that the proposed Regulation does not specify in the "household exception" what constitutes a personal activity in relation to "other" users (for example, contacts or friends on social networks or third parties in general): this leaves open the issue of the application of the exception to cases in which a user - through cloud services - may process personal data which can be accessed by an indefinite number of persons. The EDPS has already

[29] See EDPS Opinion on the Data Protection Reform package, paragraph 93, on the wording of recital 15.

indicated[30] that the application of the exception to such cases would not be in line with the rulings of the Court of Justice in cases *Lindqvist* and *Satamedia*[31].

41. For instance, a public figure could post on his social networking page full names of his "friends" or supporters in order to promote a cultural initiative. In this scenario, the public figure does not seem to have a gainful interest in his processing activity. However the personal data may well be made public to an indefinite number of persons, not only on the social networking page[32] but also potentially through search engines. In this scenario, the household exception would not apply to the subscriber, so he would also be subject to the data protection legislation[33].

42. As regards territorial scope, Article 3 of the proposed Regulation goes beyond the existing rules on two fronts: by providing explicitly that the establishment[34] of a processor in the EU would trigger the applicability of the Regulation and by introducing the new criteria of "offering goods or services to" or "monitoring the behaviour of" data subjects in the Union. This development has been welcomed by the EDPS in his Opinion on the Data Protection Reform package[35], and is also particularly relevant in relation to cloud computing.

43. When looking at concrete possible examples of cloud service provider/cloud client relationships, different scenarios can be envisaged. The new rules allow a broad territorial applicability of the proposed Regulation in relation to cloud computing services, which may lead to complex situations; however, as explained below, a small clarification in the text of Article 3 could help removing some interpretative doubts.

Cloud service provider as processor

44. As discussed below, in some instances the provider of cloud services is considered as a processor rather than a data controller. In these cases, if the establishment of the cloud client (the data controller) is in the Union territory, the applicability of the proposed Regulation to the controller and by contract to the processor would be unquestionable.

45. Also, if the processor/provider is established in the EU and the client/data controller is not resident in the EU, the Regulation would apply to all the processing activities of the processor. This would mean that European based cloud providers would have to respect the obligations imposed on them by the proposed Regulation and, possibly, suffer the consequences of violations of such obligations. According to Article 27 of the proposed Regulation, the processor shall not process except on the basis of instructions of the data controller "unless required to do so by Union or Member State law". This means that a European based cloud provider/processor

[30] See EDPS Opinion on the Data Protection Reform package, paragraph 91.

[31] See CJEU 6 November 2003, *Lindqvist*, C-101/01, [2003] ECR I-12971 and CJEU 16 December 2008, *Satamedia*, C-73/07, [2008] ECR I-983.

[32] Provided that the individual's privacy settings allow it.

[33] The user should be considered as a data controller because he chooses the means of processing (the cloud service provider) and to a certain extent determines the purposes of the processing.

[34] See also EDPS Opinion on the Data Protection Reform package paragraphs 106-107 for a critical remark on the definition of "main establishment".

[35] See EDPS Opinion on the Data Protection Reform package, paragraph 99.

should always act in conformity with EU data protection law, even if this conflicts with instructions by the (non European) client/data controller[36]. As indicated above, it is essential that the challenges raised by the use of cloud computing services do not lead to a lowering of EU data protection standards. Article 27 of the proposed Regulation must therefore be welcomed as a safeguard for the cloud environment.

Cloud service provider as data controller

46. In the case that the cloud service provider is considered as the data controller and is established in the EU, no interpretative doubts would arise about the applicability of the proposed Regulation to its processing activities.

47. Another scenario is if the cloud service provider is considered as a data controller - or even the sole data controller - rather than just a processor[37] but is not established in the EU. Cloud service providers are often established outside the EU and offer their services in the EU through the Internet. Under the current rules, in the absence of equipment in the EU territory, the EU regime would not apply to the processing activities[38]. Under the proposed rules, the processing of the personal data of data subjects residing in the EU by a non-EU based cloud provider (who can be categorized as a data controller) could fall under the scope of the proposed Regulation if it targets data subjects in the Union. The trigger for the applicability of the proposed Regulation would be the new criterion of "offering goods or services to [such] data subjects in the Union" in Article 3(2)(a) thereof. Since the definition of Article 4 indicates that a data subject can only be a natural person, the wording of this Article might be read as meaning that only processing related to goods or services offered to *individuals* residing in the Union would fall within the scope of application of the Regulation.

48. However, in the area of cloud computing, the target of the service is often constituted by enterprises of any size, hence legal entities that cannot be considered data subjects under the EU law[39]. Although, from a commercial point of view, the service is offered to EU businesses (hence not "data subjects"), the EDPS considers that the rules of the proposed Regulation should also apply when the service involves the processing of personal data of individuals resident in the Union. In order to avoid interpretative doubts, the text of the proposal could be amended by amending Article 3(2)(a) to read "the offering of goods or services *involving processing of personal data of* such data subjects in the Union". Alternatively, a new recital could specify that the processing of personal data of data subjects in the

[36] The application of the EU rules should, however, not result in an excessive burden for European companies in relation to the responsibilities of the non-European data controller. In this respect, the text of the proposed Regulation includes the possibility to exempt the (controller or) processor from liability for damages suffered by any person as a result of unlawful processing if the processor proves that it is not responsible for the event giving rise to the damage (Article 77(3)). Furthermore, Article 75 explicitly clarifies that the amount of possible sanctions for breaches or infringements to be imposed by the supervisory authorities shall take into due account also the "degree of responsibility of the natural or legal person" (Article 79(2)).

[37] For instance, in cases when the service provider processes personal data for its own purposes.

[38] It should be noted, however, that if the provider places cookies on the device of the user/client, such cookies are considered under EU legislation as "equipment" in the EU territory.

[39] See definition of data subject in the text of the proposed Regulation, article 4(1).

Union by non-EU based controllers offering services to EU based legal persons also falls within the territorial scope of the proposed Regulation.

IV.2. Improving the allocation of roles and responsibilities (the notions of Controller and Processor)

49. The applicability of the notions of controller and processor to the cloud computing environment is one of the most important aspects of the data protection regime applicable to this business model. The crucial point is how to allocate responsibility for compliance with data protection rules[40].

50. The WP29 Opinion discusses how to qualify the cloud services provider/cloud client relationship on the basis of the currently applicable rules of Directive 95/46/EC. Essentially, the cloud client determines the ultimate purpose of the processing and decides on the outsourcing of this processing and the delegation of all or part of the processing activities to an external organisation. He should therefore be considered as a data controller. In consequence, the cloud client, as controller, should ensure - normally through appropriate contractual safeguards - that the processing operations carried out by the service provider abide by the applicable data protection laws. When the cloud service provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is usually considered as a data processor according to Directive 95/46/EC[41]. The suggested way to ensure compliance by the data processor is to strictly apply the requirements of Article 17 of the Directive.

51. The WP29 Opinion acknowledges that in some cases the provider of cloud services may be considered either as a joint controller or as a controller in its own right, depending on the circumstances. For instance, this could be the case where the provider processes data for its own purposes.

52. The EDPS supports the WP29´s position on the qualifications of the relationship between cloud service providers and clients on the basis of the currently applicable rules. He notes, however, that the complexity of the technical means used in the cloud environment has now reached such a stage that it is necessary to add that the cloud client/data controller may not be the only entity that can solely determine the "purposes and means" of the processing. More and more often, the determination of the essential elements of the means, which is a prerogative of the data controller, is not in the hands of the cloud client. In this respect, the cloud service provider typically designs, operates and maintains the cloud computing IT infrastructure (be it simply the basic hardware and software services as in IaaS, or the platform as in PaaS, or the overall service, including the application software, as in SaaS).

53. As recognized in the WP29 Opinion, often the cloud services provider is the party which, on the basis of its technical infrastructure and business type, elaborates standard contracts or SLAs to be offered to the cloud client. The latter therefore has no or very little leeway to modify the technical or contractual means of the service.

[40] See WP29 Opinion 1/2010 on the concepts of "controller" and "processor", available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

[41] The natural or legal person, public authority, agency or any other body that alone or jointly with others, processes personal data on behalf of the controller, Directive 95/46/EC, Article 2(e).

This is all the more true in view of the consolidation of the cloud computing market, as mentioned above in part II.3. Hence, ensuring data protection compliance may be particularly challenging.

54. Furthermore, when looking at the definitions in the proposed Regulation, the controller would be the natural or legal person which "alone or jointly with others determines the purposes, *conditions* and means"[42] (emphasis added) of the personal data processing. The current provision (Article 2(d) of Directive 95/46/EC) does not include the term "conditions". This change would put even more emphasis on the responsibility of those determining how a data processing activity will be concretely organised.

55. In this scenario, qualifying the relationship between provider and client as a co-controllership would better reflect the underlying level of influence on the processing activities. Such a step would lead to a more realistic allocation of responsibilities between the parties, which would need to be taken into account in the negotiation of the service terms. This would mean, for instance, that the service terms should clearly identify which controller is responsible for which areas of the processing and/or for which obligations imposed by the relevant data protection legislation. As a consequence, the cloud client should be responsible for the parts of the processing on which he has effective control. However, the difference in bargaining power between the parties involved may still prevent a balanced negotiation. This problem could be overcome by the development and use of standard contractual terms and conditions[43].

56. The EDPS supports the provision of the proposed Regulation that envisages making an arrangement between co-controllers compulsory (Article 24). Such an arrangement should in all cases specify how responsibility between different actors is divided, in conformity with the real influence different actors have on the different types of activities.

57. In the case of IaaS solutions, the cloud client - which is usually an enterprise - could have a certain influence on the conditions and terms of the service, although he may not be in a position to negotiate security measures of the cloud service provider. The cloud client would however remain controller in relation to the processing activities of the personal data of its employees, because it would be choosing the means and conditions and determining the purpose of the processing by the cloud provider. The allocation of responsibilities between the two should therefore be explicitly clarified in the terms of service. When looking at SaaS solutions like cloud-based office productivity tools or business intelligence tools, the cloud client usually has no possibility to influence the type of service offered by the provider. In addition, the relationship between provider and client may not involve any direct negotiation and may amount to a simple registration process. As a consequence, the level of control over the means of the processing operations by the cloud client may be extremely limited. In this scenario, the EDPS considers that the qualification of the cloud service provider as co-controller might be more appropriate.

[42] Article 4(5).

[43] See Chapter V.3 below.

58. Furthermore, the proposed Regulation introduces in Article 26(4) a new provision according to which, if a processor processes personal data other than instructed by the controller, he will be considered a controller in relation to that processing and will be subject to the joint controlling principles of Article 24. This provision can be crucial in relation to cloud computing services: it could apply to cases where a provider of SaaS to business customers processes, for instance, addresses and contact lists of employees or clients of the cloud user, or even scans the content of emails to which it has access, for the purpose of promoting its value added services.

59. In conclusion, the complexity of the technical IT infrastructure underlying the cloud computing environment requires an expansion of the circumstances in which a cloud service provider may be qualified as the controller. The text of the proposed Regulation may introduce a new element of controllership ("conditions") which is in line with this developing trend. Therefore, in many instances, considering the cloud services provider as co-controller will better reflect the real level of influence on the purpose, conditions and means of processing operations.

IV.3. Responsibility and Accountability in the Cloud: ensuring more effective data protection

60. The proposed Regulation increases the responsibility and accountability of data controllers and processors in general (see mainly Article 22) and by introducing specific obligations such as data protection by design and by default, data security breach notifications and a data protection impact assessment. From a general perspective, the enhanced responsibilities of the data controller ensure a very welcome improvement of the protection of the data subjects[44]. Most innovations can also be considered as major improvements in the cloud computing environment.

61. On the other hand, certain types of new obligations[45] may be challenging to abide by if the data controller is considered to be the cloud services client. Although the processor, on the basis of Article 26, is required to cooperate with the controller in order to fulfil the latter's obligation to respond to data subjects´ rights and assist the data controller in ensuring compliance with the security requirements, data breach notifications, data protection impact assessment and prior consultation, the ultimate responsibility rests mainly on the controller.

62. In a cloud computing environment, this would mean that the client/controller should be able, for instance, to implement appropriate technical and organisational measures and procedures to ensure that the data processing carried out by the cloud service provider complies with the Regulation (Article 23, data protection by design). This might prove to be difficult. In the case of a basic IaaS service, it seems particularly difficult for a business customer (especially if an SME) to influence the technical and organisational structure of the service. It is not realistic to expect from a large provider with many customers to tailor its technical infrastructure or organisation to meet the specific compliance requirements of each customer on the basis of individually negotiated contracts.

[44] See EDPS Opinion on the Data Protection Reform Package, paragraph 166 et seqq.

[45] In particular, implementation of policies to ensure that the processing of personal data is compliant with the Regulation; data security requirements; data protection impact assessment; data protection by design; notification of data breaches in particular in relation to point 3(c) and (e) of Article 31.

63. In consequence, the appropriate qualification of data controller and processor as explained in the previous chapters is key to ensure that the enhanced responsibility and accountability obligations are effectively respected.

Data protection impact assessment of cloud computing services

64. Article 33 of the proposed Regulation contains the requirement for the controller or the processor acting on the controller's behalf to carry out a data protection impact assessment. It includes a non-exhaustive list of the processing operations where this data protection impact assessment should be mandatory. The EDPS has already expressed the view that he was not fully satisfied as the list omitted some types of relevant risks[46]. In the absence of clear provisions in the proposed Regulation or guidelines on how to carry out such data protection impact assessments, the implementation of this requirement is completely linked to the subjective assessment made by each controller, which can lead to different results.

65. The use of cloud computing services to process personal data could, in some cases, imply (as illustrated by this Opinion), specific risks for data protection that call for a data protection impact assessment, on the basis of which appropriate mitigation measures could be defined.

66. In particular, the EDPS would highlight the importance of carrying out data protection impact assessments as concerns the use of cloud computing services by the public sector, especially when the processing may involve sensitive data (such as health data, data revealing political opinions, etc).

67. The EDPS recommends that the criteria and conditions to determine when a data protection impact assessment is required and the elements to be analysed are set forth in a delegated act[47]. In the context of cloud computing services, the EDPS highlights that it would be useful for the Commission to develop templates that could be used by public administrations (and by individuals and companies) to evaluate and manage risks.

Audits and certifications

68. More generally, the application of the accountability requirements in a cloud environment can be complex as different players may interact along the end-to-end value chain in order to deliver the service to the end customer. Therefore, the interaction of multiple parties requires the different actors involved to trust the others to act responsibly and take appropriate measures to ensure that data processing operations are carried out in compliance with data protection rules.

69. In this respect, internal and trusted third party audits and subsequent certifications are helpful in verifying responsibility and accountability when multiple parties are involved. Such audits should themselves be based on appropriate certification and standardisation models (which will be discussed further below in section V.2).

[46] See EDPS Opinion on the Data Protection Reform package, para. 201.

[47] This is also supported by the WP29 Opinion 08/2012 of 5 October 2012 providing further input on the data protection reform discussions, pages 31-32, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf.

70. In terms of substance, Article 22 of the proposed Regulation specifies the data protection measures that controllers are required to take[48]. In particular, Article 22(3) requires the controller to implement mechanisms to ensure that the effectiveness of those data protection measures can be verified. If proportionate, this can be done by independent internal or external auditors.

71. The EDPS welcomes the provision but also highlights that, especially in the context of cloud computing, more specific guidance is required to clarify which mechanisms should be put in place to ensure verification of the effectiveness of data protection measures in practice. Unless this happens, these verification exercises risk measuring compliance only on "paper" but not in "reality". The EDPS takes note that the current text of the proposed Regulation (Article 22(4)) provides for the Commission to adopt delegated acts to specify, *inter alia*, the conditions for the verification and auditing mechanisms referred to in Article 22(3). Irrespective of whether such provision on delegated acts will be maintained in the final text[49], cloud computing specific codes of conduct drawn up by the industry and approved by the relevant data protection authorities could be a useful tool to enhance compliance as well as trust among the various players[50].

IV.4. Adapting international data transfers mechanisms to the Cloud Computing environment

Challenges in applying EU data transfer rules to the Cloud Computing environment

72. Cloud computing services rely upon the continuous flows of data of cloud clients across cloud service providers' infrastructure. Data are being conveyed from the cloud clients to cloud providers' servers and data centres located in various parts of the world. Cloud computing therefore often involves massive and continuous transfers of data worldwide.

73. The EU rules on international data transfers both in the current law and in the proposed Regulation impose conditions on the transfers of personal data: in particular, the country of the recipient should assure an adequate level of protection, or in the absence thereof[51], adequate safeguards should be adduced. However, the application of the EU data transfer rules to processing operations taking place through cloud computing services is often perceived as being particularly challenging.

[48] And indirectly for processors under Article 26.

[49] In its Opinion 8/2012 of 5 October 2012 providing further input on the data protection reform discussions, the WP 29 suggests the removal of paragraph 4 in Article 22, as there "seems to be no need to specify any further the criteria and requirements for appropriate measures other than those already provided in paragraph 2 and the conditions for the verification and auditing mechanism".

[50] See Article 38 of the proposed Regulation.

[51] Under the current legal framework, the Commission has adopted several adequacy decisions with respect to Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, US PNR, and the US Safe Harbor. Under Article 41 of the proposed Regulation, the Commission will have the power to adopt adequacy decisions, as well as negative adequacy decisions, not only in respect of a third country, but also in respect of a territory or a processing sector within that third country or an international organisation.

74. First, there is no clear definition in the proposed Regulation of the notion of 'transfer' of personal data. This is problematic with respect to network environments such as cloud computing, where data are not only being actively transferred but are also being made available to a number of recipients located in various countries (often unknown to the cloud customer/end user). The EDPS has called for a clear definition of the notion of 'transfer' in his Opinion on the Data Protection Reform package[52].

75. Secondly, the application of international data transfer rules is usually based on an assessment of whether there is an adequate level of protection in the country/ies where the data are to be transferred. However, cloud computing services most frequently do not have any stable location of the data and personal data may not remain permanently in a given location. Furthermore, some service providers may refuse to inform where the cloud servers are located[53].

76. Thirdly, in cases where the cloud client is deemed to be the controller - and in particular the sole controller - of the data, it is very difficult for him to adduce adequate safeguards for the international transfer of his data since he has little knowledge and/or control over the design of the cloud architecture of his cloud services provider and the places where the latter and any other processors or sub-processors are processing the data. This derives from the asymmetry of control over the processing activities between the cloud customer and the cloud services provider discussed above in section II.3.

Significant improvements in the proposed Regulation facilitating international data transfers

77. The proposed Regulation introduces greater flexibility into the application of the data transfer rules, with the aim of facilitating international transfers while at the same time maintaining a high level of protection for these data. In particular, it sets forth a broader range of mechanisms for international data transfers. Furthermore, Article 42(1) of the proposed Regulation requires that not only controllers but also processors adduce appropriate safeguards for international data transfers. This constitutes a significant step forward which is particularly relevant to the cloud computing environment.

78. For instance, Article 42 of the proposed Regulation facilitates the use of several types of contractual clauses - from standard to *ad hoc* - by clarifying that only *ad hoc* clauses would require authorisation from a supervisory authority. Cloud computing providers may wish to use this flexibility by entering into the standard contractual clauses adopted by the Commission or by a supervisory authority in accordance with Article 42(2)(c). They may also wish to enter into *ad hoc* clauses that are specifically tailored to their specific environment, provided they obtain the necessary approval from the competent supervisory authority. Whatever the clauses chosen by cloud service providers, they should all contain minimum guarantees on essential aspects, e.g. the requirement to enter into written agreement with sub-processors by which they commit to the same data protection obligations (including

[52] See EDPS Opinion pages 18-19.

[53] See for example the referral for a preliminary ruling pending before the Court of Justice of the EU in the case C-131/12 Google v Spain.

security measures), prior information/notices of the cloud customer on the use of sub-processors, audit clause, third party beneficiary rights, rules on liability and damages, supervision, etc. Supervisory authorities, when developing standard clauses or reviewing *ad hoc* clauses submitted to their approval, will pay particular attention to these essential aspects.

79. Furthermore, Article 43 of the proposed Regulation sets forth a detailed mechanism for the use of Binding Corporate Rules (hereafter 'BCRs')[54], which may be more adapted to multilateral schemes. BCRs are a mechanism that is particularly well suited to the cloud computing environment, as it allows the flexibility of transferring data across all entities of an organisation while at the same time commanding legally enforceable obligations upon that organisation as concerns the protection of personal data everywhere such data are processed within that organisation. The extension of their use to processors is welcome, particularly as processors that have an establishment in the EU will be able to benefit from this mechanism to facilitate their intra-group data transfers to entities located outside the EU.

Opportunities in the proposed Regulation to further tailor the data transfer mechanisms to the cloud computing environment

80. The cloud computing environment is based on certain specificities, as explained earlier, not all of which are fully taken into account in the data transfer mechanisms that have been developed until now. The proposed Regulation offers the possibility to further tailor these mechanisms to a specific sector, such as the cloud computing environment. The European Data Protection Board could play a role in providing further guidance in this context[55].

(i) Standard contractual clauses

81. Standard contractual clauses[56] are particularly well suited for 'point to point' data transfers from a controller to identified recipients (whether controller(s), processor(s) and/or sub-processor(s)) in identified locations. Such clauses may however be difficult to use in most cloud computing environments, where data may be continuously transferred across a long chain of recipients.

82. If one considers the cloud service provider as the processor under the standard contractual clauses approved by the Commission for transfer from controller to processor, it is up to him to inform and seek consent from the cloud client before any sub-processing and transfer to an external third party. However, in many cases, the cloud client will have little or no realistic power to authorise or prohibit such transfers. In contrast, if the cloud service provider were actually qualified as data

[54] Binding Corporate Rules have been developed by data protection authorities in the frame of the Article 29 Working Party to provide another appropriate mechanism that can be used for the international transfers of data. (See Article 29 Working Party documents at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm). The proposed Regulation builds upon the work done by the WP29 in this area.

[55] See WP29 Opinion 08/2012.

[56] See more information on existing standard contractual clauses at: http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm.

controller, it would be fully responsible for ensuring compliance of its data transfers to entities within its organisation and externally, being in full control and fully accountable regarding its decisions on its cloud computing services' architecture. In this respect, the EDPS has demonstrated in section IV.2 above that the cloud service provider would in many circumstances have to be considered as co-controller.

83. Furthermore, there are currently no standard contractual clauses developed for the purpose of governing the transfers of data from processors based in the EU to processors located outside the EU. This is a significant gap in particular in the context of cloud computing services, which would deserve undertaking additional work in order to put forward an appropriate new set of clauses.

84. It would therefore be useful for the Commission and/or supervisory authorities to make use of the possibilities foreseen in Articles 42(2)(b) and (c) of the proposed Regulation to adopt updated standard contractual clauses that are tailored to the cloud computing environment. Such clauses should notably address the issues of processor-to-processor transfers originating from the EU, constant multi-jurisdiction transfers and the lack of precise identification of where the data may be located at a given time, as well as information/notice and accountability mechanisms. They should also specify further the conditions for access by law enforcement, as will be described in section IV.7 below.

(ii) Binding Corporate Rules

85. Binding Corporate Rules (BCRs), which fully embed the accountability principle, appear particularly well suited for cloud computing services. Cloud service providers should therefore be encouraged to make use of this mechanism for the purpose of their international transfers.

86. As concerns the applicability of BCRs to external processors and/or sub-processors, the EDPS underlines that, even though BCRs have been developed to provide a legally binding mechanism for intra-group situations, Article 43(2)(c) of the proposed Regulation would require that they also indicate their legally binding nature upon external organisations. The current work undertaken by the WP29 in view of developing BCRs for processors will be particularly helpful to address, amongst others, their binding nature on external sub-processors.

87. Furthermore, Article 43(3) of the proposed Regulation provides for the adoption by the Commission of delegated acts to specify the application of Article 43(2) points (b), (d), (e) and f) to BCRs adhered to by processors. The WP29[57] has welcomed that further specifications be defined in a delegated act and has also recommended that the European Data Protection Board provide guidance on this issue.

88. Finally, it must be underlined that the further tailoring of international data transfer mechanisms would also greatly benefit from complementary work done on standardisation and certification schemes to help achieve the required level of data protection at all levels of the processing, which in turn will generate the necessary trust from cloud clients (as will be discussed in section V.2).

[57] See WP29 Opinion 08/2012, pages 37-38.

IV.5. Security of processing

89. Technical and organisational measures must be taken to protect confidentiality, integrity and availability of data by preventing inter alia unauthorised access, modification, erasure or removal. Under the proposed Regulation, both the controller and the processor would be obliged to perform an evaluation of the risks represented by the processing and the nature of the data processed, and select their measures accordingly.

90. In cloud computing environments, it is of particular importance that all parties involved, whether controller or processor, perform risk assessments for the processing under their control, also because - as mentioned before - cloud computing adds levels of complexity. Comprehensive risk assessment and security management in a cloud environment requires cooperation and coordination between the different parties involved, as the overall level of security is determined by the weakest link. For example, a personal computer or a client PC that has been compromised and allows access to user credentials for unauthorised persons can invalidate security measures at central locations. In a cloud environment used by multiple clients, security failures of one client could even affect the security of other clients, unless the service has provided very robust and secure measures to separate services and data between clients and make mutual interference impossible.[58]

91. In order to enable cloud users to take the necessary measures on their side, they would have to be informed about the risk assessment and the security measures of the cloud provider and understand their effectiveness and their limitations. However, in the alleged interest of security itself, there is typically no transparency about the IT security measures that are implemented. Details of security incidents are often not reported to clients. This makes it difficult for cloud clients to even evaluate the security of the processing operation.

92. Data controllers can only comply with their security obligations when they have comprehensive and reliable information allowing them to assess that the cloud provider fully complies with his security obligations as processor or controller. They must not entrust processing of personal data to cloud service providers that do not provide sufficient information and transparency on their security measures.

93. The proposed Regulation would create a comprehensive obligation for controllers to inform supervisory authorities and data subjects about personal data breaches. Cloud providers would have to report any personal data breaches that occur in their services, either directly to the supervisory authorities and the individuals, as required, if they act as controllers, or to the cloud client who is the data controller if they are only processors.

94. The proposed Regulation would allow the Commission to further specify, by adopting where necessary implementing acts, the applicable security requirements

[58] It is sometimes argued that cloud computing environments could be safer and more secure than some traditional processing situations. However, this assertion only holds in very limited contexts, e.g. when processing operations by a small organisation or an individual, where no systematic information security measures are implemented, are moved into cloud data centres with professional management of security.

and the criteria and circumstances for establishing data breaches as well as format and procedure of notifications. In particular in a complex cloud computing environment such implementing acts should aim to bring clarity regarding the responsibility of the different roles actors. They could benefit from the development of European standards for data protection and IT security in cloud computing environments and the development and recognition of metrics announced in the Communication, as will be further developed in chapter V.

IV.6. Reinforcing cooperation and coordinated supervision over cross-border processing operations

95. One of the challenges of processing personal data through cloud computing services is the difficulty for supervisory authorities in the EU to supervise all aspects of the processing activities taking place in that environment. In particular, it can be challenging for the authorities to exercise effective supervision over data located in a foreign jurisdiction or available to and accessible by a processor or a controller located in a foreign jurisdiction.

96. As explained in section IV.1, the new provisions of the proposed Regulation on applicable law would help alleviate some of these concerns by making processing operations of cloud service providers having an establishment in the EU or certain processing operations carried out from outside the EU fall within the scope of EU data protection law and subject to the supervision of competent data protection authorities in the EU. Furthermore, the provisions of the proposed Regulation concerning reinforced cooperation (namely Articles 55 and 56) and the consistency mechanism (namely Articles 57 to 63) should help supervisory authorities in Europe work together and adopt a coordinated approach on topics which are transnational by nature, such as cloud computing services. Finally, the enforcement powers of supervisory authorities would be increased with the possibility to apply financial sanctions against those controllers or processors in breach of EU data protection law (as set forth in Article 79).

97. These cooperation and consistency mechanisms, as foreseen in chapter VII of the proposed Regulation, are particularly welcome; there is nonetheless a need to address the global context within which processing operations take place in cloud computing services. At the international level, there have been several developments with a view to address the need for cross-border cooperation in the field of privacy and data protection[59]. In 2011, the International Conference of Data Protection and Privacy Commissioners also called for more international enforcement coordination on issues related to privacy and data protection[60].

98. The EDPS therefore encourages the Commission and supervisory authorities to engage into more effective international cooperation (such as developing effective international cooperation mechanisms, providing international mutual assistance in the enforcement of legislation for the protection of personal data, etc), in order to

[59] For instance the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy adopted in 2007 and the recent creation of the Global Privacy Enforcement Network (GPEN), https://www.privacyenforcement.net/about_the_network.

[60] Resolution on Privacy Enforcement Co-ordination at the International Level, adopted at the 33rd International Conference of Data Protection and Privacy Commissioners, 1 November 2011, Mexico City.

engage in close cooperation in particular on issues related to the cloud computing environment. The EDPS reminds that the start of these activities does not depend on the entry into force of the proposed Regulation.

IV.7. Law enforcement access to personal data processed through Cloud Computing Services

99. Data stored through cloud computing services may be seized or accessed by local law enforcement bodies in the jurisdiction where the servers or the data centres are located or where the cloud services provider has an establishment. Such requests may originate not only from administrative and/or judicial bodies located within the EU but also from outside the EU. Within Europe, such requests must follow due process of law[61] and respect data protection requirements[62]. The members of the Council of Europe are bound by Convention No. 108 on data protection[63] and related documents. Access by law enforcement bodies is furthermore subject to *ex post* control by data protection supervisory authorities. However, access requests from foreign law enforcement bodies raise specific issues in terms of data protection, in particular in relation to ensuring that the protection afforded to individuals in Europe with respect to their data is not significantly weakened or ignored in such context.

100. For example, cloud service providers doing business in some countries have been compelled to reveal data to national law enforcement authorities, which has given rise to fears about access to data stored in cloud computing services abroad[64]. Furthermore, it has also been pointed out that there is an increasing likelihood that certain governments will require communication providers offering services in their country to '*maintain communications equipment there, in order to facilitate such access*'[65].

101. Cloud service providers may be caught between conflicting legal requirements, on the one hand an access request from a law enforcement body in a country that claims jurisdiction, and on the other hand ensuring compliance with EU data protection law. The terms of services of cloud providers often stipulate that they will preserve and disclose information to law enforcement when served with a legal request. However, the manner in which access requests are being dealt with should be reconciled with EU data protection requirements.

102. First, any such request to access to personal data of data subjects in the EU should only be granted following due process of law and there should be an appropriate

[61] In many instances, access requests are based on a legal request authorised by a judicial authority.

[62] The processing of data by law enforcement bodies must respect applicable data protection requirements. The Data Protection reform package contains a proposal for a Data Protection Directive, which will help harmonise the conditions for the processing of personal data by law enforcement bodies in the EU.

[63] Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, 28.01.1981).

[64] 'Lost in the Cloud', Jonathan Zittrain New York Times, 19 July 2009, http://www.nytimes.com/2009/07/20/opinion/20zittrain.html?_r=1.

[65] 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future', Christopher Kuner, Tilburg University, the Netherlands, Working Paper No. 016/2010, October 2010, page 40.

legal basis allowing for the transfer of data[66]. In this respect, the EDPS has called in his Opinion on the Data Protection Reform package[67] for the inclusion of a substantive provision in the proposed Regulation that would clarify the conditions for such requests for access. Appropriate guarantees should be in place in such cases, involving judicial guarantees as well as data protection safeguards, including the existence of international or bilateral cooperation agreements on specific issues (e.g. Mutual Legal Assistance Agreements). This issue would also benefit from being addressed in other types of international instruments, such as trade agreements with third countries. Furthermore, it should be assessed, as was previously underlined by the EDPS[68], how supervisory authorities could intervene in such cases, whether by giving an opinion or an authorisation on the transfer. This may require inserting a provision to that effect in the proposed Regulation.

103. Second, further work is needed to improve and standardise cloud service providers' contract terms on how they deal with law enforcement access requests (as will be described further in section V.3).

104. Finally, there is a clear need to address at an international level the issue of access to data by law enforcement bodies. In this respect, the conditions under which law enforcement bodies may seek access to data stored in cloud computing services would benefit from being further clarified, in particular by further developing common understandings and principles at an international level having regard to the following issues:

- These global standards should address the conditions of access, the security measures applicable for handing over the data to law enforcement bodies[69], the rights of the individuals, supervision and redress mechanisms.

- What the term 'access' entails in that context should be clarified to specify whether this consists in the retrieval or copy of data stored in particular equipment. In this view, account must be taken of the fact that access to data processed in cloud computing services often requires locating the relevant data and reassembling or converting them into an intelligible form.

- It should be considered further whether access to data stored in a private cloud infrastructure should be treated the same way as access to data stored in a public cloud infrastructure.

- The development of certification schemes for cloud computing services would also help to indicate if and how personal data are protected from such access.

105. In conclusion, the EDPS calls for the inclusion of a specific provision in the proposed Regulation to clarify the conditions under which access from non-EEA countries 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

[66] See recital 90 of the proposed Data Protection Regulation.
[67] See EDPS Opinion on the Data Protection Reform package, para. 229-232.
[68] See EDPS Opinion on the Data Protection Reform package, para. 231.
[69] Such as the use of encryption to protect the data and providing access to the decryption key in a secure manner.

the EU in specific cases. The issue of access to data by law enforcement bodies should be addressed at international level, and the Commission and the Member States should devote their efforts to developing common rules and principles at this level. Furthermore, they should systematically integrate specific provisions and safeguards on this issue into the various international agreements (including trade agreements) they enter into with non-EEA countries.

V. SPECIFIC COMMENTS ON THE COMMISSION'S COMMUNICATION

106. The Commission's Communication describes a number of actions to be taken or promoted by the Commission to help support the deployment of cloud computing services in Europe. Amongst others, the following actions are foreseen: providing guidance, fostering appropriate standardisation and certification schemes, developing model contract terms and a code of conduct, setting up a European Cloud Partnership, and pursuing its international dialogue with third countries and in multilateral fora.

107. The EDPS welcomes that data protection is a central element of the Communication and that the envisaged policy initiatives in relation to cloud computing services aim at maintaining a high level of data protection.

V.1. Providing further guidance

108. The EDPS also welcomes that the Commission envisages providing further guidance on the application of data protection law in respect of cloud computing services, in close cooperation with data protection authorities. He welcomes the account taken of the WP29 Opinion, and underlines that the present Opinion also provides further guidance in relation to the proposed data protection framework.

109. Further work still needs to be done to clarify best practice as regards specific 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. The WP29 Opinion providing further input on the data protection reform discussions[70] highlights many areas for which complementary guidance from the European Data Protection Board would be useful, in particular as concerns the security of the processing, the criteria for determining the high degree of specific risks referred to in Article 34(2)(a), as well as the application of some of the BCR requirements to processors.

110. Furthermore, the EDPS supports the development of codes of conduct for cloud computing, as foreseen in Article 38 of the proposed Regulation, provided that they are fully respectful of data protection requirements. In this respect, the EDPS underlines that only the endorsement of the codes of conduct by the supervisory authorities can give legal certainty to companies that they will comply with the legislation in force when following these codes.

V.2. Standardisation and Certification Schemes

[70] See footnote 47.

111. Under Key Action 1, the Communication proposes standardisation as a major step towards acceptance of cloud computing services. The Communication provides that, by 2013, a map of the necessary standards will be drawn. These standards should apply, inter alia, to security, interoperability, data portability and reversibility.

112. These standards could be a critical success factor to enable governance and supervision models at international level. Standards will help ensure that the whole chain of actors involved in the cloud computing architecture, including intermediaries, are all applying the same level of technical requirements. However, in order to be effective from a data protection point of view, the EDPS underlines that these standards should fully embed data protection requirements, in particular the principle of data protection by design and by default set forth in Article 23 of the proposed Regulation. In this respect, the EDPS encourages the Commission to intensify its efforts to ensure that the standards and metrics defined at international level cover EU requirements appropriately.

113. Special attention should be paid to ensure that standards in the field of cloud computing services effectively lead to a high level of security and data protection. This applies in particular to:

- interoperability, which can be defined as the ability of diverse systems to function together and exchange information. From a technical and economic perspective, interoperability allows to integrate different data sources which can bring processing of those data to a new level. The potential risk of personal data being used for purposes incompatible with what they were collected for should be addressed by taking the principle of purpose limitation into account where interoperability applies to personal data.

- data portability, which is defined in Article 18 of the proposed Regulation as the ability for a data subject to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used. In order to implement this right, it is important that, once the data have been transferred, no trace is left in the original system[71]. In technical terms, it should become possible to verify the secure erasure of data.

114. These standards should help cloud service providers to be accountable in practice. The combination of standards with certification by independent parties may enhance trust in cloud services and help controllers and processors achieve compliance with regulatory frameworks.

V.3. Developing model Contract Terms and Conditions

115. The EDPS fully acknowledges the need to assist stakeholders in the definition of standard contract terms and conditions in view of the usual significant imbalance of negotiating powers between cloud service providers and cloud clients. As discussed above, cloud service providers are often in a position to impose non negotiable contractual terms and conditions upon their clients. The EDPS therefore welcomes

[71] See EDPS Opinion on the Data Protection Reform package para. 150-152 and WP29 Opinion on cloud computing, page 16.

that, under Key Action 2 of the Communication, model contract terms and conditions will be developed by the Commission, which will help enhance the appropriate consideration of data protection obligations and data subjects' rights in the cloud service providers' commercial offers to customers (in service level agreements) and to consumers (in contract terms and conditions).

116. These model contract terms and conditions aim at providing standard terms to be included in the commercial offer to cloud clients. They are distinct from the standard contractual clauses used for the purpose of providing adequate safeguards for the international transfer(s) of data. Although Key Action 2 does not deal with standard contractual clauses for international transfers as its main area for action, the EDPS welcomes that the Communication foresees that standard clauses for international transfers will also be reviewed and adapted to the cloud computing environment, as suggested in section IV.4 above.

117. The Communication points out several data protection issues that must be addressed in model contract terms and conditions, such as data preservation upon termination, data disclosure and integrity, data location and transfers, change of service by cloud providers and subcontracting. The WP29 has also provided suggestions regarding the issues that should be specifically addressed in the contract[72]. In addition to the issues listed in the Communication and by the WP29, the EDPS underlines that it is particularly important that model contracts and model terms and conditions also contain appropriate terms on the following aspects:

- Eliminating unfair terms by which cloud service providers disclaim responsibility for keeping the clients' data confidential and secure or by which they exclude liability for loss or corruption of the data. Further, they should also provide for appropriate terms in respect of applicable law and dispute resolution that allow data subjects to have redress before a data protection authority and/or a EU Member State's national court in cases involving a breach of EU data protection law (e.g. concerning a data breach or a data loss).

- Informing cloud clients whether there is an option to keep data within a national or regional cloud, and the conditions thereof.

- As concerns subsequent contractual amendments, ensuring that appropriate information is provided and consent is sought from cloud clients before any term or condition is amended or revoked.

- Setting forth appropriate terms as regards data retention upon the termination of contract, in particular defining good practices regarding data retention time limits and erasure of the data thereafter.

- Ensuring that appropriate information is provided to cloud clients concerning the processing of personal data, in accordance with data protection

[72] See WP29 Opinion 05/2012 pages 12 to 14. These recommendations deal, amongst others, with the issues of security measures, confidentiality, sub-contracting, conditions for returning or destroying the data once the service is concluded, data breach notification, auditing, and the handling of requests from law enforcement authorities.

requirements. Additional information that is essential in the context of the use of cloud computing services should also be considered for inclusion in these model contract terms and conditions (e.g. applicable law, location(s) where the data may be processed, compliance with certification scheme/standards, guarantees that there are appropriate safeguards in place at all levels of the infrastructure and wherever the data are transmitted or stored, specific safeguards for sensitive data, identification of the relevant supervisory body, etc).

- Ensuring that data subjects are informed about their rights, in accordance with data protection requirements, and that the standard terms and conditions provide effective means to exercise such rights. In the cloud computing environment, it is particularly crucial to ensure that individuals have an effective right of access to their data and the right to data portability.

- As concerns access by law enforcement bodies in third countries, it should be ensured that, at a minimum, cloud clients are informed of the legal implications associated with the jurisdictions to which the processing are/may be subject and to ensure that they are, as a general rule, informed of any such request made by law enforcement bodies. Such information should be included in the cloud service providers' contractual terms as well as in the safeguards adduced for transferring personal data outside the EU/EEA (e.g. standard contractual clauses, BCRs).

118. Furthermore, in the context of the European Cloud Partnership, the Commission will work on developing specific procurement terms for the public sector by defining common procurement requirements for their use of cloud computing services. The EDPS underlines that these common procurement requirements should include data protection requirements, including appropriate security measures, which should be defined in a manner appropriate to the specific risks of processing public sector data in a cloud computing environment. This should be done on the basis of a careful data protection impact assessment according to the type and sensitivity of the processing carried out (e.g. differentiate between public sector processing of health data, criminal offences, confidential data, etc). As a result, the requirements contained in procurement terms will need to be differentiated according to the sensitivity of the data processed, which should lead to defining several sets of common requirements.

V.4. International dialogue

119. The EDPS has underlined in this Opinion the need for more global cooperation between supervisory authorities (section IV.6) and the importance of addressing specific issues relating to cloud computing at an international level (sections IV.5 and IV.7). He therefore welcomes the fact that the cloud computing Communication takes due account of the global nature of cloud computing services and that it foresees actions aimed at fostering the development of global governance standards and the implementation of more effective cooperation practices.

120. It is important that data protection is an essential part of the international dialogue pursued in relation to cloud computing issues. Such dialogue must be addressed: at a technological level, to create solutions and standards that ensure adequate level of data protection (for instance, by embedding data protection by default and by

design, and in terms of security); at a business level, with solutions based on accountability and governance mechanisms; and at a political level, to explore how the Commission together with third countries can work on facilitating global interoperability of the various legal frameworks on essential issues, such as jurisdiction and law enforcement access requests.

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 emphasizes 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 particular 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 in Brussels, 16 November 2012

(**signed**)

Peter HUSTINX
European Data Protection Supervisor