ARTICLE 29 DATA PROTECTION WORKING PARTY

01037/12/EN
WP 196

Opinion 05/2012 on Cloud Computing

Adopted July 1st 2012

Executive Summary

In this Opinion the Article 29 Working Party analyses all relevant issues for cloud computing service providers operating in the European Economic Area (EEA) and their clients specifying all applicable principles from the EU Data Protection Directive (95/46/EC) and the e-privacy Directive 2002/58/EC (as revised by 2009/136/EC) where relevant.

Despite the acknowledged benefits of cloud computing in both economic and societal terms, this Opinion outlines how the wide scale deployment of cloud computing services can trigger a number of data protection risks, mainly a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed/sub-processed. These risks need to be carefully assessed by public bodies and private enterprises when they are considering engaging the services of a cloud provider. This Opinion examines issues associated with the sharing of resources with other parties, the lack of transparency of an outsourcing chain consisting of multiple processors and subcontractors, the unavailability of a common global data portability framework and uncertainty with regard to the admissibility of the transfer of personal data to cloud providers established outside of the EEA. Similarly, a lack of transparency in terms of the information a controller is able to provide to a data subject on how their personal data is processed is highlighted in the opinion as matter of serious concern. Data subjects must[1] be informed who processes their data for what purposes and to be able to exercise the rights afforded to them in this respect.

A key conclusion of this Opinion is that businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such a service. Security, transparency and legal certainty for the clients should be key drivers behind the offer of cloud computing services.

In terms of the recommendations contained in this Opinion, a cloud client's responsibilities as a controller is highlighted and it is thus recommended that the client should select a cloud provider that guarantees compliance with EU data protection legislation. Appropriate contractual safeguards are addressed in the opinion with the requirement that any contract between the cloud client and cloud provider should afford sufficient guarantees in terms of technical and organizational measures. Also of significance is the recommendation that the cloud client should verify whether the cloud provider can guarantee the lawfulness of any cross-border international data transfers.

Like any evolutionary process, the rise of cloud computing as a global technological paradigm represents a challenge. This Opinion, as it stands, can be deemed to be an important step in defining the tasks to be assumed in this regard by the data protection community in the upcoming years.

---

[1] The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in Request for Comments 2119. The document is available at http://www.ietf.org/rfc/rfc2119.txt. However, for readability, these words do not appear in all uppercase letters in this specification.

Table of Contents

1. Introduction

For some, cloud computing is one of the biggest technological revolutions to emerge in recent times. For others, it is just the natural evolution of a set of technologies aimed to achieve the long awaited dream of utility computing. In any case, large numbers of stakeholders have put cloud computing to the fore in the development of their technological strategies.

Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space. Cloud computing can generate important economic benefits, because on-demand resources can be configured, expanded and accessed on the Internet quite easily. Next to economic benefits, cloud computing may also bring security benefits; enterprises, especially small-to-medium sized ones, may acquire, at a marginal cost, top-class technologies, which would otherwise be out of their budget range.

There is a wide gamut of services offered by cloud providers ranging from virtual processing systems (which replace and/or work alongside conventional servers under the direct control of the controller) to services supporting application development and advanced hosting, up to web-based software solutions that can replace applications conventionally installed on the personal computers of end-users. This includes text processing applications, agendas and calendars, filing systems for online document storage and outsourced email solutions. Some of the most commonly used definitions for these different types of services are contained in the Annex to this Opinion.

In this Opinion the Article 29 Working Party (hereinafter: WP 29) analyses the applicable law and obligations for controllers in the European Economic Area (hereinafter: EEA) and for cloud service providers with clients in the EEA. This opinion focuses on the situation, where the relationship is assumed to be a controller-processor relationship, with the customer qualifying as controller and the cloud provider qualifying as processor. In cases where the cloud provider acts as a controller as well, they have to meet additional requirements. As a consequence, a precondition for relying on cloud computing arrangements is for the controller to perform an adequate risk assessment exercise, including the locations of the servers where the data are processed and the consideration of risks and benefits from a data protection perspective, pursuant to the criteria outlined in the paragraphs below.

This Opinion specifies the applicable principles for both controllers and processors from the general data protection directive (95/46/EC), such as purpose specification and limitation, erasure of data and technical and organizational measures. The opinion provides guidance on the security-requirements, both as a structural and a procedural safeguard. Special emphasis is laid on the contractual arrangements that should regulate the relationship between a controller and a processor in this connection. The classic goals of data security are availability, integrity and confidentiality. However, data protection is not limited to data security and therefore these goals are complemented with the specific data protection goals of transparency, isolation, intervenability and portability to substantiate the individual's right to data protection as enshrined in Article 8 of the EU Charter of Fundamental rights.

With regard to transfers of personal data outside of the EEA, instruments such as the standard contractual clauses adopted by the European Commission, adequacy-findings and a possible future processor-BCR are analysed, as well as data protection risks arising from international law enforcement requests.

This Opinion concludes with recommendations for cloud clients as controllers, cloud providers as processors and for the European Commission with regard to future changes in the European data protection framework.

The Berlin International Working Group on Data Protection in Telecommunications adopted the *Sopot Memorandum*[2] in April 2012. This memorandum examines privacy and data protection issues in cloud computing and emphasizes that cloud computing must not lead to a lowering of data protection standards as compared to conventional data processing.

2. Data protection risks of cloud computing

As this Opinion focuses on personal data processing operations deploying cloud computing services, only the specific risks related to this context are considered.[3] The majority of these risks fall within two broad categories namely lack of control over the data, and insufficient information regarding the processing operation itself (absence of transparency). Specific cloud computing risks considered in this opinion include:

Lack of control

By committing personal data to the systems managed by a cloud provider, cloud clients may no longer be in exclusive control of this data and cannot deploy the technical and organisational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation[4], intervenability and portability of the data. This lack of control may manifest itself in the following manner:

- Lack of availability due to lack of interoperability (vendor lock-in): If the cloud provider relies on proprietary technology it may prove difficult for a cloud client to shift data and documents between different cloud-based systems (data portability) or to exchange information with entities that use cloud services managed by different providers (interoperability).
- Lack of integrity caused by the sharing of resources: A cloud is made up of shared systems and infrastructures. Cloud providers process personal data emanating from a wide range of sources in terms of data subjects and organisations and it is a possibility that conflicting interests and/or different objectives might arise.
- Lack of confidentiality in terms of law enforcement requests made directly to a cloud provider: personal data being processed in the cloud may be subject to law enforcement requests from law enforcement agencies of the EU Member States and of third countries. There is a risk that personal data could be disclosed to (foreign) law enforcement agencies without a valid EU legal basis and thus a breach of EU data protection law would occur.
- Lack of intervenability due to the complexity and dynamics of the outsourcing chain: The cloud service offered by one provider might be produced by combining services from a range of other providers, which may be dynamically added or removed during the duration of the client's contract.

---

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

3 In addition to the risks related to personal data processed "in the cloud" explicitly mentioned in this opinion, all risks related to the outsourcing of the processing of personal data must also be taken into account.

4 In Germany the broader concept of "unlinkability" has been introduced. Cf. footnote 24 below.

- Lack of intervenability (data subjects' rights): A cloud provider may not provide the necessary measures and tools to assist the controller to manage the data in terms of, e.g., access, deletion or correction of data.
- Lack of isolation: A cloud provider may use its physical control over data from different clients to link personal data. If administrators are facilitated with sufficiently privileged access rights (high-risk roles), they could link information from different clients.

Lack of information on processing (transparency)

Insufficient information about a cloud service's processing operations poses a risk to controllers as well as to data subjects because they might not be aware of potential threats and risks and thus cannot take measures they deem appropriate.

Some potential threats may arise from the controller not knowing that

- Chain processing is taking place involving multiple processors and subcontractors.
- Personal data are processed in different geographic locations within the EEA. This impacts directly on the law applicable to any data protection disputes which may arise between user and provider.
- Personal data is transferred to third countries outside the EEA. Third countries may not provide an adequate level of data protection and transfers may not be safeguarded by appropriate measures (e.g., standard contractual clauses or binding corporate rules) and thus may be illegal.

It is a requirement that data subjects whose personal data are processed in the cloud are informed as to the identity of the data controller and the purpose of the processing (an existing requirement for all controllers under Data Protection Directive 95/46/EC). Given the potential complexity of processing chains in a cloud computing environment, in order to guarantee fair processing in respect of the data subject (Article 10 of Directive 95/46/EC), controllers should also as a matter of good practice provide further information relating to the (sub-)processors providing the cloud services.

3. Legal framework

3.1 Data protection framework

The relevant legal framework is the Data Protection Directive 95/46/EC. This Directive applies in every case where personal data are being processed as a result of the use of cloud computing services. The e-privacy Directive 2002/58/EC (as revised by 2009/136/EC) applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks (telecom operators) and thus is relevant if such services are provided by means of a cloud solution[5].

[5] Directive 2002/58/CE on e-privacy (as amended by Directive 2009/136/CE): Directive 2002/58/EC on privacy in telecommunications applies to providers of electronic communication services made available to the public, and requires them to ensure compliance with obligations relating to the secrecy of communications and personal data protection, as well as rights and obligations with regard to electronic communications networks and services. In cases where cloud computing providers act as providers of a publicly-available electronic communication service they will be subject to this regulation.

3.2 Applicable law

The criteria for establishing the applicability of legislation are contained in Article 4 of Directive 95/46/EC, which refers to the law applying to controllers[6] with one or more establishments within the EEA and also to the law applying to controllers who are outside the EEA but use equipment located within the EEA to process personal data. The Article 29 Working Party has analyzed this issue in its Opinion 8/2010 on applicable law[7].

In the first case, the factor that triggers the application of EU law to the controller is the location of his or her establishment and the activities it carries out, according to Article 4.1.a) of the Directive, with the type of cloud service model being irrelevant. The applicable legislation is the law of the country in which the controller contracting the cloud computing services is established, rather than the place in which the cloud computing providers are located.

Should the controller be established in various Member States, processing the data as part of its activities in these countries, the applicable law shall be that of each of the Member States in which this processing occurs.

Article 4.1.c)[8] refers to how data protection legislation applies to controllers who are not established in the EEA but use automated or non-automated equipment located in the territory of the Member State, except where these are used only for purposes of transit. This means that if a cloud client is established outside the EEA, but commissions a cloud provider located in the EEA, then the provider exports the data protection legislation to the client.

3.3 Duties and responsibilities of different players

As previously indicated, cloud computing involves a range of different players. It is important to assess and clarify the role of each of these players in order to establish their specific obligations with regard to current data protection legislation.

It should be recalled that the WP29 pointed out in its opinion 1/2010 on the concepts of "controller" and "processor" that "*the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice. In other words: to allocate responsibility.*" These two general criteria responsible for compliance and allocation of responsibility should be borne in mind by the parties involved throughout the analysis in question.

3.3.1 Cloud client and cloud provider

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. The cloud client therefore acts as a data controller. The Directive defines a controller as "*the natural or legal person, public authority, agency or any other body that alone or jointly with others determines the purposes and means of the processing of*

---

6 The concept of the controller can be found in Article 2.h) of the Directive and was analysed by the Article 29 WG in its Opinion 1/2010 on the concepts of controllers and processors.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf

8 Article 4(1)c states that the legislation of a Member State shall be applicable when "the controller is not established in Community territory and, for purposes of processing personal data, makes use of equipment, automated or otherwise, situated in the territory of said Member State, unless such equipment is used only for purposes of transit through the territory of the Community".

personal data". The cloud client, as controller, must accept responsibility for abiding by data protection legislation and is responsible and subject to all the legal duties that are addressed in Directive 95/46/EC. The cloud client may task the cloud provider with choosing the methods and the technical or organisational measures to be used to achieve the purposes of the controller.

The cloud provider is the entity that provides the cloud computing services in the various forms discussed above. When the cloud provider supplies the means and the platform, acting on behalf of the cloud client, the cloud provider is considered as a data processor i.e., according to Directive 95/46/EC "*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"*.[9][10]

As stated in the Opinion 1/2010, some criteria[11] can be used for assessing controllership of the processing. As a matter of fact, there may be situations in which a provider of cloud services may be considered either as a joint controller or as a controller in their own right depending on concrete circumstances. For instance, this could be the case where the provider processes data for its own purposes.

It should be emphasized that even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules must be clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and gaps arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties.

In the current cloud computing scenario, clients of cloud computing services may not have room for manoeuvre in negotiating the contractual terms of use of the cloud services as standardised offers are a feature of many cloud computing services. Nevertheless, it is ultimately the client who decides on the allocation of part or the totality of processing operations to cloud services for specific purposes; the cloud provider's role will be that of a contractor vis-à-vis the client, which is the key point in this case. As stated in the Article 29 Working Party Opinion 1/2010[12] on the concepts of controller and processor, "*the imbalance in the contractual power of a small controller with respect to large service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law"*. For this reason, the controller must choose a cloud provider that guarantees compliance with data protection legislation. Special emphasis must be placed on the features of the applicable contracts – these must include a set of standardised data protection safeguards including those outlined by the WP in paragraph 3.4.3 (Technical and Organisational Measures) and in paragraph 3.5 (cross-border data flows) – as well as on additional mechanisms that can prove suitable for facilitating due diligence and accountability (such as independent third-party audits and certifications of a provider's services – see paragraph 4.2).

---

9 This opinion focuses only on the regular controller – processor relationship.

10 The cloud computing environment can also be used by natural persons (users) to carry out exclusively personal or domestic activities. In such a case, it is to be analysed thoroughly whether the so called household exception applies which exempts users from qualifying as controller. However, this issue is beyond the scope of this opinion.

11 e.g. Level of instructions, monitoring by the cloud client, expertise of the parties

12 Opinion 1/2010 on the concepts of "controller" and "processor" - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Cloud providers (as processors) have a duty to ensure confidentiality. Directive 95/46 EC states that: *"Any persons acting under the authority of the controller or of the processor, including the processors themselves, who have access to personal data must not process them except on instructions from the controller, unless he is required to do so by law."* Access to data by the cloud provider during its provision of services is also fundamentally governed by the requirement to comply with the provisions of Article 17 of the Directive – see section 3.4.2.

Processors must take into account the type of cloud in question (public, private, community or hybrid / IaaS, SaaS or PaaS [see Annex a) Rollout models - b) Service Provision Models]) and the type of service contracted by the client. Processors are responsible for adopting security measures in line with those in EU legislation as applied in the controller's and the processor's jurisdictions. Processors must also support and assist the controller in complying with (exercised) data subjects' rights.

3.3.2 Subcontractors

Cloud computing services may entail the involvement of a number of contracted parties who act as processors. It is also common for processors to subcontract additional sub-processors which then gain access to personal data. If processors subcontract services out to sub-processors, they are obliged to make this information available to the client, detailing the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/EC.

All the relevant obligations must therefore apply also to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider. In its Opinion 1/2010 on the concepts of "controller" and "processor", the Article 29 Working Party referred to the multiplicity of processors in cases in which processors may have a direct relationship with the controller or operate as subcontractors where the processors outsource part of the processing work they had been tasked with. "*Nothing in the Directive prevents that on account of organisational requirements, several entities may be designated as processors or (sub-)processors also by subdividing the relevant tasks. However, all of them are to abide by the instructions given by the controller in carrying out the processing.*"[13].

In such scenarios, the obligations and responsibilities deriving from data protection legislation should be set out clearly and not dispersed throughout the chain of outsourcing or subcontracting, in order to ensure effective control over and allocate clear responsibility for processing activities.

A possible model of assurances that can be used to clarify the duties and obligations of processors when they subcontract data processing was first introduced by the Commission Decision of 5 February 2010 on the standard contractual clauses for the transfer of personal data to processors established in third countries[14]. In this model sub-processing is permitted only with the prior written consent of the controller and with a written agreement imposing the same obligations on the sub-processor as are imposed on the processor. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the

[13] Cf. WP169, p. 29, Opinion 1/2010 on the concepts of "controller" and "processor" (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf)

[14] See FAQ II.5 of WP176.

processor shall remain fully liable to the controller for the performance of the sub-processor's obligations under such agreement. A provision of this kind could be used in any contractual clauses between a controller and a cloud service provider, where the latter intends to provide services through subcontracting, to assure required guarantees for the sub-processing.

A similar solution regarding assurances in the course of sub-processing has been proposed recently by the Commission in the proposal for a General Data Protection Regulation[15]. The acts of a processor must be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that, among other requirements, the processor shall enlist another processor only with the prior permission of the controller (Article 26(2) of the proposal).

In the view of the WP29, the processor can subcontract its activities only on the basis of the consent of the controller, which may be generally given at the beginning of the service[16] with a clear duty for the processor to inform the controller of any intended changes concerning the addition or replacement of subcontractors with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. In addition, a contract should be signed between cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider. The controller should be able to avail of contractual recourse possibilities in case of breaches of contracts caused by the sub-processors. This could be arranged by ensuring that the processor is directly liable toward the controller for any breaches caused by any sub-processors he has enlisted, or through the creation of third party beneficiary right for the benefit of the controller in the contracts signed between the processor and the sub-processors or by the fact that those contracts will be signed on behalf of the data controller, making this later a party to the contract.

3.4 Data protection requirements in the client-provider relationship

3.4.1 Compliance with basic principles

The lawfulness of the processing of personal data in the cloud depends on the adherence to basic principles of EU data protection law: Namely, transparency vis-à-vis the data subject is to be guaranteed, the principle of purpose specification and limitation must be complied with and personal data must be erased as soon as their retention is not necessary any more. Moreover, appropriate technical and organisational measures must be implemented to ensure an adequate level of data protection and data security.

3.4.1.1 Transparency

Transparency is of key importance for a fair and legitimate processing of personal data. Directive 95/46/EC obliges the cloud client to provide a data subject from whom data relating to himself are collected with information on his identity and the purpose of the processing. The cloud client should also provide any further information such as on the recipients or categories of recipients of the data, which can also include processors and sub-processors in

[15] Proposal for a Regualtion of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 25.1.2012.

[16] See FAQ II, 1) of WP176, adopted on 12 July 2010.

so far as such further information is necessary to guarantee fair processing in respect of the data subject (cf. Article 10 of the Directive)[17].

Transparency must also be ensured in the relationship(s) between cloud client, cloud provider and subcontractors (if any). The cloud client is only capable of assessing the lawfulness of the processing of personal data in the cloud if the provider informs the client about all relevant issues. A controller contemplating engaging a cloud provider should carefully check the cloud provider's terms and conditions and assess them from a data protection point of view.

Transparency in the cloud means it is necessary for the cloud client to be made aware of all subcontractors contributing to the provision of the respective cloud service as well as of the locations of all data centres personal data may be processed at.[18]

If the provision of the service requires the installation of software on the cloud client's systems (e.g., browser plug-ins), the cloud provider should as a matter of good practice inform the client about this circumstance and in particular about its implications from a data protection and data security point of view. Vice versa, the cloud client should raise this matter ex ante, if it is not addressed sufficiently by the cloud provider.

3.4.1.2 Purpose specification and limitation

The principle of purpose specification and limitation requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes (cf. Article 6(b) of Directive 95/46/EC). The cloud client must determine the purpose(s) of the processing prior to the collection of personal data from the data subject and inform the data subject thereof. The cloud client must not process personal data for other purposes that are not compatible with the original ones.

Moreover, it must be ensured that personal data are not (illegally) processed for further purposes by the cloud provider or one of his subcontractors. As a typical cloud scenario may easily involve a larger number of subcontractors, the risk of processing of personal data for further, incompatible purposes must therefore be assessed as being quite high. To minimise this risk, the contract between cloud provider and cloud client should include technical and organisational measures to mitigate this risk and provide assurances for the logging and auditing of relevant processing operations on personal data that are performed by employees of the cloud provider or the subcontractors.[19] Penalties should be imposed in the contract against the provider or subcontractor if data protection legislation is breached.

3.4.1.3 Erasure of data

According to Article 6(e) of Directive 95/46/EC, personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Personal data that are not necessary any more must be erased or truly anonymised. If this data cannot be erased due to legal retention rules (e.g., tax regulations), access to this personal data should be blocked. It

---

17 A corresponding duty to inform the data subject exists when data that have not been obtained from the data subject himself, but from different sources are recorded or disclosed to a third party (cf. Article 11).

18 Only then he will be able to assess whether personal data may be transferred to a so-called third country outside of the European Economic Area (EEA) which does not ensure an adequate level of protection within the meaning of Directive 95/46/EC. Cf. also section 3.4.6 below.

19 Cf. section 3.4.3 below.

is the cloud client's responsibility to ensure that personal data are erased as soon as they are not necessary in the aforementioned sense any more[20].

The principle of erasure of data applies to personal data regardless of whether they are stored on hard drives or on other storage media (e.g., backup tapes). Since personal data may be kept redundantly on different servers at different locations, it must be ensured that each instance of them is erased irretrievably (i.e., previous versions, temporary files and even file fragments are to be deleted as well).

Cloud clients must be aware of the fact that log data[21] facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.[22]

Secure erasure of personal data requires that either the storage media to be destroyed or demagnetised or the stored personal data is deleted effectively through overwriting. For the overwriting of personal data, special software tools that overwrite data multiple times in accordance with a recognised specification should be used.

The cloud client should make sure that the cloud provider ensures secure erasure in the abovementioned sense and that the contract between the provider and the client contains clear provision for the erasure of personal data[23]. The same holds true for contracts between cloud providers and subcontractors.

3.4.2 Contractual safeguards of the "controller"-"processor" relationship(s)

Where controllers decide to contract cloud computing services, they are required to choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures (Article 17(2) of Directive 95/46/EC). Furthermore, they are legally obliged to sign a formal contract with the cloud service provider, as stated in Article 17(3) of Directive 95/46/EC. This article establishes the requirement for there to be a contract or other binding legal act to govern the relationship between the controller and the processor. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the technical and organizational measures shall be in writing or in another equivalent form.

The contract must at a minimum establish the fact, in particular, that the processor is to follow the instructions of the controller and that the processor must implement technical and organizational measures to adequately protect personal data.

To ensure legal certainty the contract should also set forth the following issues:

1. Details on the (extent and modalities of the) client's instructions to be issued to the provider, with particular regard to the applicable SLAs (which should be objective and measurable) and the relevant penalties (financial or otherwise including the ability to sue the provider in case of non-compliance).
2. Specification of security measures that the cloud provider must comply with, depending on the risks represented by the processing and the nature of the data to be

[20] Erasure of data is an issue both throughout the duration of a cloud computing contract and upon its termination. It is also relevant in case of substitution or withdrawal of a subcontractor.

[21] Remarks on logging requirements are provided below at 4.3.4.2.

[22] This means that reasonable retention periods for log files are to be defined and that processes safeguarding the timely erasure or anonymisation of these data are to be in place.

[23] Cf. section 3.4.3 below.

protected. It is of great importance that concrete technical and organizational measures are specified such as those outlined in paragraph 3.4.3 below. This is without prejudice to the application of more stringent measures, if any, that may be envisaged under the client's national law.

3. Subject and time frame of the cloud service to be provided by the cloud provider, extent, manner and purpose of the processing of personal data by the cloud provider as well as the types of personal data processed.
4. Specification of the conditions for returning the (personal) data or destroying the data once the service is concluded. Furthermore, it must be ensured that personal data are erased securely at the request of the cloud client.
5. Inclusion of a confidentiality clause, binding both upon the cloud provider and any of its employees who may be able to access the data. Only authorized persons can have access to data.
6. Obligation on the provider's part to support the client in facilitating exercise of data subjects' rights to access, correct or delete their data.
7. The contract should expressly establish that the cloud provider may not communicate the data to third parties, even for preservation purposes unless it is provided for in the contract that there will be subcontractors. The contract should specify that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned (e.g., in a public digital register). It must be ensured that contracts between cloud provider and subcontractor reflect the stipulations of the contract between cloud client and cloud provider (i.e. that sub-processors are subject to the same contractual duties than the cloud provider). In particular, it must be guaranteed that both cloud provider and all subcontractors shall act only on instructions from the cloud client. As explained in the chapter on sub-processing the chain of liability should be clearly set in the contract. It should set out the obligation on the part of the processor to frame international transfers, for instance by signing contracts with sub-processors, based on the 2010/87/EU standard contractual clauses.
8. Clarification of the responsibilities of the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data.
9. Obligation of the cloud provider to provide a list of locations in which the data may be processed.
10. The controller's rights to monitor and the cloud provider's corresponding obligations to cooperate.
11. It should be contractually fixed that the cloud provider must inform the client about relevant changes concerning the respective cloud service such as the implementation of additional functions.
12. The contract should provide for logging and auditing of relevant processing operations on personal data that are performed by the cloud provider or the subcontractors.
13. Notification of cloud client about any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a

prohibition under criminal law to preserve the confidentiality of a law enforcement investigation.

14. A general obligation on the provider's part to give assurance that its internal organisation and data processing arrangements (and those of its sub-processors, if any) are compliant with the applicable national and international legal requirements and standards.

In the event of infringement by the controller, any person suffering damages as a result of unlawful processing shall have the right to receive compensation from the controller for the damages caused. Should the processors use the data for any other purpose, or communicate them or use them in a way that breaches the contract, they shall also be considered to be controllers, and shall be held liable for the infringements in which they were personally involved.

It should be noted that, in many cases, cloud service providers offer standard services and contracts to be signed by controllers, which set forth a standard format for processing personal data. This imbalance in the contractual power of a small controller with respect to large service providers should not be considered as justification for the controllers to accept clauses and terms of contracts which are not in compliance with data protection law.

3.4.3 Technical and organisational measures of data protection and data security

Article 17(2) of Directive 95/46/EC puts full responsibility on cloud clients (acting as data controllers) to choose cloud providers that implement adequate technical and organisational security measures to protect personal data and to be able to demonstrate accountability.

In addition to the core security objectives of availability, confidentiality and integrity, attention must also be drawn to the complementary data protection goals of transparency (see 3.4.1.1 above), isolation [24], intervenability, accountability and portability. This section highlights these central data protection goals, without prejudice to other complementary security oriented risk analysis[25].

3.4.3.1 Availability

Providing availability means ensuring timely and reliable access to personal data.

One severe threat to availability in the cloud is accidental loss of network connectivity between the client and the provider or of server performance caused by malicious actions such as (Distributed) Denial of Service (DoS)[26] attacks. Other availability risks include accidental hardware failures both on the network and in the cloud processing and data storage systems, power failures and other infrastructure problems.

Data controllers should check whether the cloud provider has adopted reasonable measures to cope with the risk of disruptions, such as backup internet network links, redundant storage and effective data backup mechanisms.

---

[24] In Germany the broader concept of "unlinkability" has been introduced into legislation and is promoted by the Conference of Data Protection Commissioners.

[25] Cf. e.g. ENISA at http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[26] A DoS attack is a coordinated attempt to make a computer or network resource unavailable to its authorised users, either temporarily or indefinitely (e.g., by means of a large number of attacking systems paralysing their target with a multitude of external communication requests).

3.4.3.2 Integrity

Integrity may be defined as the property that data is authentic and has not been maliciously or accidentally altered during processing, storage or transmission. The notion of integrity can be extended to IT systems and requires that the processing of personal data on these systems remains unaltered.

Detecting alterations to personal data can be achieved by cryptographic authentication mechanisms such as message authentication codes or signatures.

Interference with the integrity of IT systems in the cloud can be prevented or detected by means of intrusion detection / prevention systems (IPS / IDS). This is particularly important in the type of open network environments in which clouds usually operate.

3.4.3.3 Confidentiality

In a cloud environment, encryption may significantly contribute to the confidentiality of personal data if implemented correctly, although it does not render personal data irreversibly anonymous[27]. Encryption of personal data should be used in all cases when "in transit" and when available to data "at rest".[28] In some cases (e.g., an IaaS storage service) a cloud client may not rely on an encryption solution offered by the cloud provider, but may choose to encrypt personal data prior to sending them to the cloud. Encrypting data at rest requires particular attention to cryptographic key management as data security then ultimately depends on the confidentiality of the encryption keys.

Communications between cloud provider and client as well as between data centres should be encrypted. Remote administration of the cloud platform should only take place via a secure communication channel. If a client plans to not only store, but also further process personal data in the cloud (e.g., searching databases for records), he must bear in mind that encryption cannot be maintained during processing of the data (except of very specific computations).

Further technical measures aiming at ensuring confidentiality include authorization mechanisms and strong authentication (e.g. two-factor authentication). Contractual clauses should also impose confidentiality obligations on employees of cloud clients, cloud providers and subcontractors.

3.4.3.4 Transparency

Technical and organisational measures must support transparency to allow review, cf. 3.4.1.1.

3.4.3.5 Isolation (purpose limitation)

In cloud infrastructures, resources such as storage, memory and networks are shared among many tenants. This creates new risks for data to be disclosed and processed for illegitimate purposes. The protection goal "isolation" is meant to address this issue and contribute to guarantying that data is not used beyond its initial purpose (Article 6(b) of Dir 95/46/EC) and to maintain confidentiality and integrity.[29]

---

[27] Directive 95/46/EC - Recital 26: "(...); whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; (...)". I n the same line, the technical data fragmentation processes that may be used in the framework of the provision of CC services will not lead to irreversible anonymisation and thus does not imply that data protection obligations do not apply.

[28] This holds true in particular for data controllers who plan to transfer sensitive data in the meaning of Article 8 of Directive 95/46/EC (e.g., health data) to the cloud or who are subject to specific legal obligations of professional secrecy.

[29] Cf. 3.4.1.2.

Achieving isolation first requires adequate governance of the rights and roles for accessing personal data, which is reviewed on a regular basis. The implementation of roles with excessive privileges should be avoided (e.g., no user or administrator should be authorised to access the entire cloud). More generally, administrators and users must only be able to access the information that is necessary for their legitimate purposes (least privilege principle).

Secondly, isolation also depends on technical measures such as the hardening of hypervisors and proper management of shared resources if virtual machines are used to share physical resources between different cloud customers. .

3.4.3.5 Intervenability

Directive 95/46/EC gives the data subject the rights of access, rectification, erasure, blocking and objection (cf. Article 12 and 14). The cloud client must verify that the cloud provider does not impose technical and organisational obstacles to these requirements, including in cases when data is further processed by subcontractors.

The contract between the client and the provider should stipulate that the cloud provider is obliged to support the client in facilitating exercise of data subjects' rights and to ensure that the same holds true for his relation to any subcontractor.[30]

3.4.3.6 Portability

Currently, most cloud providers do not make use of standard data formats and service interfaces facilitating interoperability and portability between different cloud providers. If a cloud client decides to migrate from one cloud provider to another, this lack of interoperability may result in the impossibility or at least difficulties to transfer the client's (personal) data to the new cloud provider (so-called vendor lock-in). The same holds true for services that the client developed on a platform offered by the original cloud provider (PaaS). The cloud client should check whether and how the provider guarantees the portability of data and services prior to ordering a cloud service.[31]

3.4.4.7 Accountability

In IT accountability can be defined as the ability to establish what an entity did at a certain point in time in the past and how. In the field of data protection it often takes a broader meaning and describes the ability of parties to demonstrate that they took appropriate steps to ensure that data protection principles have been implemented.

IT accountability is particularly important in order to investigate personal data breaches, where cloud clients, providers and sub-processor may each bear a degree of operational responsibility. The ability for the cloud platform to provide reliable monitoring and comprehensive logging mechanisms is of paramount importance in this regard.

Moreover, cloud providers should provide documentary evidence of appropriate and effective measures that deliver the outcomes of the data protection principles outlined in the previous sections. Procedures to ensure the identification of all data processing operations, to respond to access requests, the allocation of resources including the designation of data protection

---

[30] Cf. section 3.4.5 No. 7 above. The provider may even be instructed to answer requests on behalf of the client.

[31] Preferably, the provider should make use of standardised or open data formats and interfaces. In any event, contractual clauses stipulating assured formats, preservation of logical relations and any costs accruing from the migration to another cloud provider should be agreed on.

officers who are responsible for the organisation of data protection compliance, or independent certification procedures are examples of such measures. In addition, data controllers should ensure that they are prepared to demonstrate the setting up of the necessary measures to the competent supervisory authority upon request.[32]

3.5 International transfers

Article 25 and 26 of the Directive 95/46/EC provide for free flow of personal data to countries located outside the EEA only if that country or the recipient provides an adequate level of data protection. Otherwise specific safeguards must be put in place by the controller and its co-controllers and/or processors. However, cloud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of the world at 4pm. The cloud client is therefore rarely in a position to be able to know in real time where the data are located or stored or transferred. In this context, the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations.

3.5.1 Safe Harbor and adequate countries

Adequacy findings, including Safe Harbor, are limited in respect of the geographical scope, and therefore do not cover all transfers within the Cloud.
Transfers to US organizations adhering to the principles can take place lawfully under EU law since the recipient organizations are deemed to provide an adequate level of protection to the transferred data.

However, in the view of the Working Party, sole self-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment. In addition, Article 17 of the EU directive requires a contract to be signed from a controller to a processor for processing purposes, which is confirmed in FAQ 10 of the EU-US Safe Harbor Framework documents. This contract is not subject to prior authorization from the European DPAs. Such contract specifies the processing to be carried out and any measures necessary to ensure that the data are kept secure. Different national legislations and DPAs may have additional requirements.

The Working Party considers that companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification. On the contrary, the company exporting data should obtain evidence that the Safe Harbor self-certifications exists and request evidence demonstrating that their principles are complied with. This is important especially with regard to the information provided to data subjects affected by the data processing[33, 34].

The Working Party also considers that cloud client must verify if the standard contracts composed by cloud providers are compliant with national requirements regarding contractual data processing. National legislation may require sub-processing to be defined in the contract,

---

[32] The Working Party provided detailed remarks on the topic of accountability in its Opinion 3/2010 on the principle of accountability http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

[33] See German DPA: http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

[34] For requirements regarding contracting sub-processors, see 3.3.2.

which includes the locations and other data on sub-processors, and traceability of the data. Normally the cloud providers do not offer the client such information – their commitment to the Safe Harbor cannot substitute for the lack of the above guarantees when required by the national legislation. In such cases the exporter is encouraged to use other legal instruments available, such as standard contractual clauses or BCR.

Finally, the Working Party considers that the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC[35]. In terms of data security cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures[36], which are not sufficiently addressed by the existing Safe Harbor principles on data security[37]. Additional safeguards for data security may thus be deployed; such as by incorporating the expertise and resources of third parties that are capable of assessing the adequacy of cloud providers through different auditing, standardization and certification schemes[38]. For these reasons it might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud.

3.5.2 Exemptions

The exemptions provided by article 26 of the EU Directive 95/46 enable data exporters to transfer data out of the EU without providing additional guarantees. However, WP29 has adopted an opinion in which it considered that exemptions shall apply only where transfers are neither recurrent, nor massive or structural.[39]

Based on such interpretations, it is almost impossible to rely on exemptions in the context of cloud computing.

3.5.3 Standard contractual clauses

Standard contractual clauses as adopted by the EU Commission for the purpose of framing international data transfers between two controllers or one controller and a processor are based on a bilateral approach. When the cloud provider is considered to be the processor, model clauses 2010/87/EC are an instrument that can be used between the processor and the controller as a basis for the cloud computing environment to offer adequate safeguards in the context of international transfers.

In addition to the standard contractual clauses, the Working Party considers that cloud providers could offer customers provisions that build on their pragmatic experiences as long as they do not contradict, directly or indirectly the standard contractual clauses approved by

---

35 See an opinion by the Danish DPA: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Described in detail in ENISA paper Cloud Computing: Benefits, Risks and Recommendations for Information Security at: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 "Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction."

38 See section 4.2 below.

39 Working Document 12/1998: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive, Adopted by the Working Party on 24 July 1998 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf).

the Commission or prejudice fundamental rights or freedoms of the data subjects[40]. Nevertheless, the companies may not amend or change the standard contractual clauses without implying that the clauses will no longer be "standard"[41].

When the cloud provider acting as processor is established in the EU, the situation might be more complex since the model clauses applies, in general, only to the transfer of data from a EU controller to a non EU processor (see recital 23 of the Commission decision on the model Clauses 2010/87/EU and WP 176).

As regards the contractual relationship between the non EU processor and the sub-processors, a written agreement which imposes the same obligations on the subprocessor as are imposed on the processor in the Model clauses should be put in place.

3.5.4 BCR: towards a global approach

BCR constitute a code of conduct for companies which transfer data within their group. Such solution will be provided also for the context of cloud computing when the provider is a processor. Indeed, WP29 is currently working on BCRs for processors which will allow the transfer within the group for the benefit of the controllers without requiring the signature of contracts between processor and subprocessors per client.[42]

Such BCR for processors would enable the provider's client to entrust their personal data to the processor while being assured that the data transferred within the provider's business scope would receive an adequate level of protection.

4. Conclusions and recommendations

Businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. This analysis must address the risks related to processing of data in the cloud (lack of control and insufficient information – see section 2 above) by having regard to the type of data processed in the cloud.[43] Special attention should also be paid to assessing the legal risks regarding data protection, which concern mainly security obligations and international transfers. The processing of sensitive data via cloud computing raises additional concerns. Therefore without prejudice to national laws such processing requires additional safeguards.[44] The conclusions below are meant to provide a checklist for data protection compliance by cloud clients and cloud providers based on the current legal framework; some recommendations are also provided with a view to future developments in the regulatory framework at EU level and beyond.

---

40 See FAQ IV B1.9 9, Can companies include the standard contractual clauses in a wider contract and add specific clauses? published by the EC on http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

41 See FAQ IV B1.10, Can Companies amend and change the standard contractual clauses approved by the Commission?

42 See Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, adopted on 6th June 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

43 ENISA provides a list of the risks that must be taken into consideration http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

44 See Sopot Memorandum, cf. footnote 2 above.

4.1 Guidelines for clients and providers of cloud computing services

- Controller-processor relationship: This Opinion focuses on the client-provider relationship as controller-processor relationship; (see paragraph 3.3.1); Nevertheless based on concrete circumstances situations may exist where the cloud provider acts as a controller as well, e.g. when the provider re-processes some personal data for its own purposes. In such a case, the cloud provider has full (joint) responsibility for the processing and must fulfil all legal obligations that are stipulated by Directives 95/46/EC and 2002/58/EC (if applicable);
- Cloud client's responsibility as a controller: The client as the controller must accept responsibility for abiding by data protection legislation and is subject to all the legal obligations mentioned in Directive 95/46/EC and 2002/58/EC, where applicable, in particular vis-à-vis data subjects (see 3.3.1). The client should select a cloud provider that guarantees compliance with EU data protection legislation as reflected by the appropriate contractual safeguards summed up below;
- Subcontracting safeguards: Provisions for subcontractors should be provided for in any contract between the cloud provider and cloud clients. The contract should specify that sub-processors may only be commissioned on the basis of a consent that can be generally given by the controller in line with a clear duty for the processor to inform the controller of any intended changes in this regard with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. The cloud provider should sign a contract with each subcontractor reflecting the stipulations of his contract with the cloud client; the client should ensure that it has contractual recourse possibilities in case of contractual breaches by the provider's sub-contractors (see 3.3.2);
- Compliance with fundamental data protection principles:
    - Transparency (see 3.4.1.1): cloud providers should inform cloud clients about all (data protection) relevant aspects of their services during contract negotiations; in particular, clients should be informed about all subcontractors contributing to the provision of the respective cloud service and all locations in which data may be stored or processed by the cloud provider and/or its subcontractors (notably, if some or all locations are outside of the European Economic Area (EEA)); the client should be provided with meaningful information about technical and organisational measures implemented by the provider; the client should as a matter of good practice inform data subjects about the cloud provider and all subcontractors (if any) as well as about locations in which data may be stored or processed by the cloud provider and/or its subcontractors;
    - Purpose specification and limitation (3.4.1.2): the client should ensure compliance with purpose specification and limitation principles and ensure that no data is processed for further purposes by the provider or any subcontractors. Commitments in this respect should be captured in the appropriate contractual measures (including technical and organisational safeguards);
    - Data retention (3.4.1.3): the client is responsible for ensuring that personal data are erased (by the provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes; secure

erasure mechanisms (destruction, demagnetisation, overwriting) should be provided for contractually;

- Contractual safeguards (see 3.4.2, 3.4.3 and 3.5):
    - In general: the contract with the provider (and the ones to be stipulated between provider and sub-contractors) should afford sufficient guarantees in terms of technical security and organizational measures (under Article 17(2) of the directive) and should be in writing or in another equivalent form. The contract should detail the client's instructions to the provider including subject and time frame of the service, objective and measurable service levels and the relevant penalties (financial or otherwise); it should specify the security measures to be complied with as a function of the risks of the processing and the nature of the data, in line with the requirements made below and subject to more stringent measures as envisaged under the client's national law; if cloud providers aim at making use of standard contractual terms, they should ensure that these terms comply with data protection requirements (see 3.4.2); in particular technical and organisational measures that have been implemented by the provider should be specified in the respective terms;
    - Access to data: only authorised persons should have access to the data; a confidentiality clause should be included in the contract vis-à-vis the provider and its employees;
    - Disclosure of data to third parties: this should be regulated only via the contract, which should include an obligation for the provider to name all its sub-contractors – e.g. in a public digital register – and ensure access to information for the client of any changes in order to enable him to object to those changes or terminate the contract; the contract should also require the provider to notify any legally binding request for disclosure of the personal data by a law enforcement authority, unless such disclosure is otherwise prohibited; the client should warrant that the provider will reject any non-legally binding requests for disclosure;
    - Obligations to co-operate: client should ensure that the provider is obliged to co-operate with regard to the client's right to monitor processing operations, facilitate the exercise of data subjects' rights to access/correct/erase their data, and (where applicable) notify the cloud client of any data breaches affecting client's data;
    - Cross-border data transfers: The cloud client should verify if the cloud provider can guarantee lawfulness of cross-border data transfers and limit the transfers to countries chosen by the client, if possible. Transfers of data to non-adequate third countries require specific safeguards via the use of Safe Harbor arrangements, standard contractual clauses (SCC) or binding corporate rules (BCR) as appropriate; the use of SCC for processors (under Commission's decision 2010/87/EC) requires certain adaptations to the cloud environment (to prevent having separate per-client contracts between a provider and its sub-processors) which might imply the need for prior authorisation from the competent DPA; a list of the locations in which the service may be provided should be included in the contract;
    - Logging and auditing of processing: the client should request logging of processing operations performed by the provider and its sub-contractors; the client should be empowered to audit such processing operations, however

third-party audits chosen by the controller and certification may also be acceptable providing full transparency is guaranteed (e.g. by providing for the possibility to obtain a copy of a third-party audit certificate or a copy of the audit report verifying certification);

- Technical and organisational measures: these should be aimed at remedying the risks entailed by lack of control and lack of information that feature most prominently in the cloud computing environment. The former include measures aimed at ensuring availability, integrity, confidentiality, isolation, intervenability and portability as defined in the paper whilst the latter focus on transparency (see 3.4.3 for full details).

4.2 Third Party Data Protection Certifications

- Independent verification or certification by a reputable third party can be a credible means for cloud providers to demonstrate their compliance with their obligations as specified in this Opinion. Such certification would, as a minimum, indicate that data protection controls have been subject to audit or review against a recognised standard meeting the requirements set out in this Opinion by a reputable third party organisation.[45] In the context of cloud computing, potential customers should look to see whether cloud services providers can provide a copy of this third party audit certificate or indeed a copy of the audit report verifying the certification including with respect to the requirements set out in this Opinion.
- Individual audits of data hosted in a multi-party, virtualised server environment may be impractical technically and can in some instances serve to increase risks to those physical and logical network security controls in place. In such cases, a relevant third party audit chosen by the controller may be deemed to satisfy in lieu of an individual controller's right to audit.
- The adoption of privacy-specific standards and certifications is central to the establishment of a trustworthy relationship between cloud providers, controllers and data subjects.
- These standards and certifications should address technical measures (such as localisation of data or encryption) as well as processes within cloud providers' organisation that guarantee data protection (such as access control policies, access control or backups).

4.3 Recommendations: Future Developments

The WP is fully aware that the complexities of cloud computing cannot be addressed completely via the safeguards and solutions outlined in this Opinion, which provide, however, a sound basis for securing the processing of personal data that EEA-based clients submit to cloud providers. This section is meant to highlight some issues that need to be tackled in the short to medium term to enhance the safeguards in place, assisting the cloud industry in terms of the issues highlighted whilst ensuring respect for the fundamental rights to privacy and data protection.

[45] Such standards would include those issued by the International Standards Organisation, the International Auditing and Assurance Standards Board and the Auditing Standards Board of the American Institute of Certified Public Accountants in so far as these organisations provide standards that meet the requirements set out in this opinion.

- Better balancing of responsibilities between controller and processor: The WP welcomes the provisions contained in Article 26 of the Commission's proposals (Draft EU General Data Protection Regulation) that are aimed at making processors more accountable towards controllers by assisting them in ensuring compliance in particular with security and related obligations. Article 30 of the proposal introduces a legal obligation for the processor to implement appropriate technical and organisational measures. The draft proposals clarify that a processor failing to comply with the controller's instructions qualifies as a controller and is subject to specific joint controllership rules. The Article 29 Working party considers that this proposal goes in the right direction to remedy the unbalance that is often a feature in the cloud computing environment, where the client (especially if it is a SME) may find it difficult to exercise the full control required by data protection legislation on how the provider delivers the requested services. Furthermore, in view of the asymmetric legal position of data subjects and small business users *vis á vis* big cloud computing providers, a more proactive role for consumer and business interest organisations is recommended in order to negotiate more balanced general terms and conditions of such companies.

- Access to personal data for national security and law enforcement purposes: It is of the utmost importance to add to the future Regulation that controllers operating in the EU must be prohibited from disclosing personal data to a third country if so requested by a third country's judicial or administrative authority, unless this is expressly authorized by an international agreement or provided for by mutual legal assistance treaties or approved by a supervisory authority. Council Regulation (EC) No 2271/96 is an appropriate example of legal ground for this.[46] The Working Party is concerned by this gap in the Commission proposal as it entails a considerable loss of legal certainty for the data subjects whose personal data are stored in data centres all over the world. For that reason, the Working Party would like to stress[47] the need to include in the Regulation the obligatory use of Mutual Legal Assistance Treaties (MLATs) in case of disclosures not authorised by Union or Member States law.

- Special precautions by the public sector: A special caveat is to be added as to the need for a public body to first assess whether the communication, processing and storage of data outside national territory may expose the security and privacy of citizens and national security and economy to unacceptable risks – in particular if sensitive databases (e.g. census data) and services (e.g. health care.) are involved.[48] This special consideration should be given, at any rate, whenever sensitive data are processed in the Cloud context. From this standpoint, consideration might be given by national governments and European Union institutions to further investigate the concept of a European Governmental cloud as a supra national virtual space where a consistent and harmonized set of rules could be applied.

---

[46] Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom, Official Journal L 309 , 29/11/1996 P. 0001 - 0006, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:EN:HTML

[47] Cf. WP 191 - Opinion 01/2012 on the data protection reform proposals, page 23.

[48] In this respect, ENISA makes the following recommendation in its paper on Security & Resilience in Governmental Clouds (http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/at_download/fullReport): "In terms of architecture, for sensitive applications private and community clouds appear to be the solution that currently best fits the needs of public administrations since they offer the highest level of governance, control and visibility, even though when planning a private or community cloud, special regard should be given to the scale of the infrastructure."

- European Cloud Partnership: The Working Party supports the European Cloud Partnership (ECP) strategy presented by Mrs Kroes, Vice-president of the European Commission, in January 2012 at Davos.[49] This strategy involves public IT procurement to stimulate a European cloud market. Transferring personal data to a European cloud provider, sovereignly governed by European data protection law, could bring great data protection advantages to customers, in particular by fostering the adoption of common standards (especially in terms of interoperability and data portability) as well as legal certainty.

[49] Neelie Kroes, Vice-President of the European Commission responsible for the Digital Agenda, Setting up the European Cloud Partnership World Economic Forum Davos, Switzerland, 26th January 2012, URL: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

ANNEX

a) Rollout models

Private cloud[50] describes an IT infrastructure that is dedicated to an individual organization; it is located at the organization's premises or else its management is outsourced to a third party (usually via server hosting) that is under the controller's strict authority. A private cloud can be compared to a conventional data centre – the difference being that technological arrangements are implemented to optimize use of the available resources and enhance those resources via small investments that are made in a stepwise fashion over time.

Public cloud, conversely, is an infrastructure owned by a provider specializing in the supply of services that makes available – and therefore shares – his systems to/among users, businesses and/or public administrative bodies. The services can be accessed via the Internet, which entails transferring data processing operations and/or the data to the service provider's systems. Therefore the service provider takes on a key role as regards to the effective protection of the data committed to his systems. Along with the data, a user is bound to transfer a major portion of his control over those data.

Alongside "public" and "private" clouds, there are so-called "intermediate" or "hybrid" clouds where services provided by private infrastructures co-exist with services purchased from public clouds. Reference should also be made to the "community clouds", where the IT infrastructure is shared by several organizations for the benefit of a specific user community.

Flexibility and simplicity in configuring cloud systems allow their "elastic" dimensioning, i.e. these systems can be adjusted to the specific requirements in accordance with a usage-based approach. Users do not have to manage any IT systems, which are relied upon on the basis of outsourcing agreements and therefore are handled in full by the third party in whose cloud the data are stored. It is often the case that large-sized providers with complex infrastructures come into play; this is why the cloud might span several locations and users might ignore where exactly their data are being stored.

b) Service provision models

Depending on user requirements, there are several cloud computing solutions available on the market; they can be grouped into three main categories or "service models". These models usually apply to both private and public cloud solutions:

---

[50] The NIST (National Institute of Standards and Technology) in the US, which has been working for some years on standardization of cloud-based technologies[50], and whose definitions are also referred to in ENISA's paper:
Private cloud.
The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. It should be pointed out that a "private cloud" relies on at least certain technologies that are also typical of "public clouds" – including, in particular, virtualization technologies that foster the re-organisation (or overhaul) of the data processing architecture as explained above.
Public cloud.
The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

- **IaaS (Cloud Infrastructure as a Service):** a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. Such providers are usually specialized market players and can rely actually on a physical, complex infrastructure that often spans over several geographic areas.
- **SaaS (Cloud Software as a Service):** a provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems; accordingly, users are ultimately meant to outsource their data to the individual provider. This is the case, for instance, of typical web-based office applications such as spreadsheets, text processing tools, computerized registries and agendas, shared calendars, etc.; however, the services in question also include cloud-based email applications.
- **PaaS (Cloud Platform as a Service):** a provider offers solutions for the advanced development and hosting of applications. These services are usually addressed to market players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties. Again, the services delivered by a PaaS provider makes it unnecessary for the user to rely on additional and/or specific hardware or software at internal level.

A full-fledged transition to a thoroughly public cloud system would appear not to be feasible in the short term on account of several reasons, in particular as regards large-sized entities like major companies or organizations that have to fulfil specific obligations – e.g. major banks, governmental bodies, large municipalities, etc. This can be accounted for mainly on two grounds: firstly, there is a momentum-like factor related to the investments required to achieve such transition; secondly, one has to take account of the especially valuable and/or sensitive information that is to be processed in the specific cases.

Another factor militating in favour of the reliance on private clouds (at least in the cases mentioned above) has to do with the circumstance that no public cloud provider can often ensure a quality of service (as based on SLAs, Service Level Agreements) such as to keep pace with the critical nature of the service the controller is to provide – maybe because bandwidth and reliability of the Net are not enough or appropriate in a given area, or else with regard to specific user-provider connections. On the other hand, one can reasonably assume that private clouds may be leased or rented in some of the above cases (because this may prove more cost-effective), or else hybrid cloud models (including both public and private components) can be deployed. The relevant implications would have to be considered carefully in all cases.

In the absence of internationally agreed standards, there is the risk of "do-it-yourself" cloud solutions, or else federated cloud solutions, which would entail increased lock-in dangers (as well as what have been termed "privacy monocultures")[51] and prevent full control over the data without ensuring interoperability. Both interoperability and data portability are indeed key factors for the development of cloud-based technology as well as in order to enable full exercise of the data protection rights vested in data subjects (such as access or rectification).

[51] See the European Parliament's study "Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy" published in December 2011.

From this standpoint, the current debate over cloud technologies provides a significant example of the tension existing between cost-oriented and rights-oriented approaches, as briefly outlined in Section 2 above. Whilst relying on private clouds may be feasible and indeed advisable in a data protection perspective by having regard to the specific circumstances of the processing, this may not be viable to organisations in the long run mainly in a cost-oriented perspective. A careful assessment of the interests at stake is necessary, as no one-size-fits-all solution can be currently pointed to in this area.