Overview of applicable legal framework and general legal requirements: Deliverable 3.1 for the SeCloud project

Konstantinou, Ioulia; Quinn, Paul; De Hert, Paul

Publication date:
2016

February 2016

SeCloud Deliverable 3.1

Overview of applicable legal framework and general legal requirements

Ioulia Konstantinou – Paul Quinn – Paul De Hert
LSTS – VRIJE UNIVERSITEIT BRUSSEL

Table of Contents

Executive Summary

This Deliverable provides an introduction and overview of the applicable legal framework on Cloud Computing relating to security, confidentiality of data and information and personal data protection and the resulting requirements. It is the first part of Task 3.1 on Security Requirements Engineering, which aims at mapping the legal requirements applicable for SaaS and Mobile Cloud applications with a focus on the above legal aspects.

The use of Cloud Computing models facilitates and accelerates the creation and processing of big data collections and the production of new services and applications in order to utilize those data as a source of profit. When these big data collections contain personal data, specific risks and challenges for privacy and data protection arise and appropriate safeguards is imperative to be implemented.

Cloud Computing is a new and alternative paradigm of data processing, compared to the traditional one. Privacy and personal data protection are in the core of this new status quo, as new impacts and risks have to be analysed, assessed and judged. What was best practice until now is not necessary the best practice from now on.

Privacy and data protection in the context of cloud computing must not, in any case, be inferior to the level of protection required in any other data processing context. The Cloud computing model can only be developed and applied legally if it guarantees that this level of data protection is respected and the data protection standards are not lowered compared to those applicable in conventional data processing operations.

The majority of the data protection challenges in cloud computing fall within two general and broad categories: first, the lack of control over the data and secondly, the absence of transparency, in terms of the provision of insufficient or no information regarding the processing operation itself.

The first step we take in our research is the presentation of the applicable EU legal framework in the context of Cloud Computing: Directive 95/46/EC, with some comments on its applicability, e-Privacy Directive 2002/58/EC and the e-commerce Directive 2000/31/EC. The proposed General Data Protection Regulation is also presented and the Belgian legislation is discussed.

In order to familiarize non-lawyer readers with data protection principles and terminology, we provide an overview of and introduction in the basic principles and rules of the EU Data Protection Law as legislated in the Directive 95/46/EC. This systematic and categorized approach includes basic data protection terminology, the key principles of EU Data Protection Law, presentation of the rules on lawful personal data processing, security of personal data processing and transparency of personal

data processing, data subject's rights and the conditions for international data transfers.

Having discussed the applicable legal framework and its principles, we move towards the role description of the Cloud players. The Cloud Client-Provider relationship is a data controller-processor relationship. Exceptional circumstances may occur, where the cloud provider may act as a controller as well. In this case, the cloud provider has full (joint) responsibility for the data processing and must comply with all relevant legal obligations derived from Directives 95/46/EC and 2002/58/EC (if applicable).

As the data controller, the Cloud Client is responsible to comply with data protection legislation and is subject to all legal obligations stemming from Directives 95/46/EC and 2002/58/EC. Furthermore, the cloud client is responsible for selecting a Cloud Provider that guarantees compliance with EU data protection legislation.

Contracts between the Cloud Provider and Cloud Clients should include provisions for subcontractors, specifying that sub-processors may only be delegated on the basis of the controller's consent with regards to the processor's obligation to inform the controller of any intended changes. The controller should be able to object at any time to such changes or to terminate the contract. Furthermore, the cloud provider should sign a contract with each subcontractor, clearly reflecting the provisions of his contract with the cloud client. The cloud client should also have contractual recourse possibilities in case of contractual breaches by the cloud provider's sub-contractors.

Having presented the applicable legal instruments and the roles of the various players, a more detailed analysis in connection with the specific Cloud Computing legal requirements follows. They are divided into two categories: (i) compliance with the basic data processing principles and (ii) technical and organizational measures implementation. The conditions for international data transfers are also discussed.

Regarding compliance with the fundamental data protection principles, we come up to the following outocomes:

- Transparency: cloud providers should inform cloud clients about all data protection relevant aspects of their services during contract negotiations (e.g. subcontractors involved, locations in which data may be stored or processed by the cloud provider and/or its subcontractors, technical and organisational measures implemented by the provider. Accordingly, the client should inform data subjects about these aspects.

- Purpose specification and limitation: the cloud client should act in compliance with this principle and ensure that the data is not processed for further purposes, other than the original, by the cloud provider or any subcontractors. Contractual commitments can also be agreed upon, including technical and organisational safeguards.

- Data erasure/Retention of data: the cloud client must ensure 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 they were collected and processed. Contracts should include provisions on secure erasure mechanisms (destruction, demagnetisation, overwriting).

- Accountability: the cloud client and the cloud provider must be able to ensure and demonstrate, through the adoption and implementation of appropriate data protection policies and technical and organizational measures that their processing activities comply with the requirements of the EU Data Protection Law.

As far as the technical and organisational measures are concerned, we conclude that:

- Technical and organizational measures should be guaranteed and included in the contract between the cloud client and the cloud provider, and also be reflected in the provider and sub-contractors relationship. They should be stipulated in written or another equivalent form.

- Technical measures must ensure availability of the data (timely and reliable access to personal data) and integrity of the data (the quality of the data to keep their authenticity and not been maliciously or accidentally altered during processing, storage or transmission).

- Confidentiality is very important. Only authorized persons should have access to data. Confidentiality clauses should be included in the contracts between the cloud provider and its employees.

- Isolation is a protective goal, which is meant to address the risk that data is used beyond its initial original purpose and to maintain confidentiality and integrity.

- The data subjects have the rights of access, rectification, erasure, blocking and objection. The cloud client must verify that the cloud provider does not impose technical and organisational obstacles to the exercise of these requirements, even in cases when data is further processed by subcontractors. The exercise of the data subject rights should be facilitated by the cloud provider.

- Interoperability and data portability are facilitated by the use of standard data formats and service interfaces by the cloud providers. If a cloud client decides to move to another cloud provider, any lack of interoperability may result in the impossibility or at least difficulties to transfer the client's (personal) data to the new cloud provider ("vendor lock-in").

- Accountability is also applicable in the context of technical and organizational measures. It expresses the ability of the cloud parties to demonstrate that they took appropriate steps to ensure the implementation of data protection principles. Cloud

providers, especially, should provide documentary evidence of appropriate and effective measures.

In case of cross-border transfers are concerned, the cloud client should verify that the cloud provider can guarantee the lawfulness of international 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 special arrangements (e.g. the former Safe Harbor – now Privacy Shield), standard contractual clauses (SCC) or binding corporate rules (BCR).

Finally, we highlight the role of Cloud standards. The adoption of privacy-oriented standards and certifications is of utmost importance for the establishment of trust between cloud providers, controllers and data subjects. These standards and certifications should address not only technical measures but also processes within cloud providers' organization/business that guarantee a high level of data protection.

1. Overview of the Deliverable

This Deliverable provides an introduction and overview of the applicable legal framework on Cloud Computing relating to security, confidentiality of data and information and personal data protection and the resulting requirements. It is the first part of Task 3.1 on Security Requirements Engineering, which aims at mapping the legal requirements applicable for SaaS and Mobile Cloud applications with a focus on the above legal aspects.

Chapter 2 offers general background information on the Cloud Computing model and introduces its deployment models and types of cloud services. Furthermore, it explains its importance in the digital era. Chapter 3 presents the legal issues and challenges of Cloud Computing, with regards to personal data protection. In Chapter 4, an overview of the applicable EU legal framework is provided, with some comments on the applicability of the Directive 95/46/EC. The proposed General Data Protection Regulation is also presented and, finally, the Belgian legislation is discussed. Chapter 5 aims at providing an overview and introduction in the basic principles and rules of the EU Data Protection Law as legislated in the Directive 95/46/EC. It also aims at familiarizing non-lawyer readers with data protection principles and terminology. A more detailed analysis in connection with the specific Cloud Computing legal requirements follows in Chapter 6, which discusses the legal responsibilities imposed on the Cloud Computing players by EU Data Protection Law. Basically, it transposes the legal overview of Chapter 5 into legal requirements and translates it in the context of Cloud Computing, after explaining the roles of the various cloud players. Finally, Chapter 7 discusses the role of Cloud Standards.

The methodology followed consists of a desk study analysis of both primary and secondary sources. The evaluated primary sources include legislative texts. Secondary sources include legal journals and research papers, policy papers and opinions and deliverables of other relevant projects.

2. Introduction to Cloud Computing

The Cloud computing model 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)[1] 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*

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

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.[2]

ICO defines the four deployment models as follows:[3]

- In private cloud, the cloud customer is the sole user of the cloud service. The underlying hardware may be managed and maintained by a cloud provider under an outsourcing contract. Access to the cloud service may be restricted to a local or wide area network.
- In community cloud, a group of cloud customers access the resources of the same cloud service. Typically the cloud customers will share specific requirements such as a need for legal compliance or high security which the cloud service provides. Access to the cloud service may be restricted to a wide area network.
- In public cloud, the infrastructure, platform or software is managed by the cloud provider and made available to the general public (cloud customers or cloud end-users). Access to the cloud service is likely to be over the public internet.
- Hybrid cloud describes a combination of private, community and public clouds. A cloud customer will segregate data and services across different cloud services, with access between them restricted depending on the type of data they contain.

ICO also describes the three main types of cloud service:[4]

- Infrastructure as a Service (IaaS): an IaaS cloud offers access to the raw computing resources of a cloud service. Rather than purchasing hardware itself, the cloud customer purchases access to the cloud provider's hardware according to the capacity required.
- Platform as a Service (PaaS): a PaaS cloud offers access to a computing platform which allows cloud customers to write applications to run within that platform, or another instance of it. The platform may in turn be hosted on a cloud IaaS.

---

[2] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf , p.4

[3] Information Commissioner's Office: "Guidance on the use of Cloud Computing" (2012) p.4-5, available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[4] Information Commissioner's Office: "Guidance on the use of Cloud Computing" (2012) p.5-6, available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

- Software as a Service (SaaS): a SaaS cloud offers access to a complete software application which the cloud user accesses through a web browser or other software. Accessing the software in this manner eliminates or reduces the need to install software on the client machine and allows the service to support a wider range of devices. The software may in turn be hosted on a cloud platform or infrastructure.

The impact of cloud computing on business and consumers is huge. On the one hand it reduces the IT services cost, as it is mainly based on economies of scale and more efficient use of information and communication infrastructures. On the other hand, dynamic allocation and re-use of resources in larger pools allows reduction of capital expenditure for IT infrastructure and rationalizing of operations.[5] Cloud Computing is attracting increasing interest due to promises of greater economic efficiency, lower environmental impact, simpler operation, increased user-friendliness. The economic driving force behind Cloud Computing is **economics of scale**. Consolidating data processing in large centres improves the usage of expensive resources such as: human knowledge, tangible capital, communication bandwidth and energy. In addition, due to their size and volume, cloud service providers have significant bargaining power when purchasing resources. Cloud service providers can therefore reduce unit costs and offer attractive prices to customers. The prerequisite for achieving economics of scale is many customers in "the store". To achieve sufficient volume, Cloud Computing services are offered globally via the internet.[6]

Cloud computing is considered to provide important opportunities for small and medium enterprises to have access to affordable and scalable computing resources. Due to the large number of relatively small entities, it is expected that cloud service providers will develop standard terms and conditions for this market segment.[7]

While cost saving effects are expected from all cloud deployment models, public 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 dynamic acquisition of services only when they are actually needed for business. It would also make higher quality services accessible to small organizations that could not afford them under traditional models, due to the

[5] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.4

[6] International Working Group on Data Protection in Telecommunications "Working Paper on Cloud Computing - Privacy and data protection issues- "Sopot Memorandum" – " (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

[7] Ibid.

high entry costs for infrastructure, licenses and set-up costs and the lack of scalability. These new opportunities are expected to open the way for innovative start-ups to offer a wide range of new services.[8]

Mobile Computing and Cloud Computing complement and strengthen each other. Together they build the basis for ambient intelligence and the Internet of Things. Mobile devices offer constantly encountered 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.[9]

3. Cloud Computing and Data Protection: Salient Legal Issues

The use of Cloud Computing models facilitates and accelerates the creation and processing of big data collections and the production of new services and applications in order to utilize those data as a source of profit.[10] Social media applications or cloud services delivered through mobile devices are some relevant examples. When these big data collections contain personal data, specific risks and challenges for privacy and data protection arise and appropriate safeguards is imperative to be implemented.[11]

Cloud Computing is a new and alternative paradigm of data processing, compared to the traditional one. This practically leads us to a situation where basic assumptions, experiences, ideas, theories and models for personal data processing no longer correspond to the practice, and therefore must be critically reflected, reassessed and revised. Privacy and personal data protection are in the core of this new *status quo*,

---

[8] European Data Protection Supervisor: ”Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.5

[9] Ibid, p.5-6

[10] '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.
McAfee, A., Brynjolfsson, E., Davenport, T. H., Patil, D. J., & Barton, D. (2012). Big data. *The management revolution. Harvard Bus Rev*, *90*(10), 61-67, http://www.rosebt.com/uploads/8/1/8/1/8181762/big_data_the_management_revolution.pdf
Chen, H., Chiang, R. H., & Storey, V. C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. *MIS quarterly*, *36*(4), 1165-1188, http://hmchen.shidler.hawaii.edu/Chen_big_data_MISQ_2012.pdf

[11] European Data Protection Supervisor: ”Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.6

as new impacts and risks have to be analysed, assessed and judged. By processing data in the cloud an organization/company may encounter risks to data protection that they were previously unaware of. What was best practice until now is not necessary the best practice from now on.[12]

Privacy and data protection in the context of cloud computing must not, in any case, be inferior to the level of protection required in any other data processing context.[13] The Cloud computing model can only be developed and applied legally if it guarantees that this level of data protection is respected and the data protection standards are not lowered compared to those applicable in conventional data processing operations.[14] Therefore, all the data protection principles laid down in Article 6 of Directive 95/46/EC and in Article 5 of the proposed General Data Protection Regulation (fairness and lawfulness, purpose limitation, proportionality, accuracy, limited data retention periods) must be fully taken into account and respected during personal data processing by cloud computing service providers.

Cloud computing raises a number of issues related to the protection of privacy and personal data that need to be properly addressed not only in service and software development, but also in the rollout. Most of these concerns are relevant regardless of the service and deployment models.[15]

According to Article 29 Working Party, the majority of the data protection challenges in cloud computing fall within two general and broad categories: first, the lack of control over the data and secondly, the absence of transparency, in terms of the provision of insufficient or no information regarding the processing operation itself.[16]

---

[12] International Working Group on Data Protection in Telecommunications "Working Paper on Cloud Computing - Privacy and data protection issues- "Sopot Memorandum" – " (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

[13] International Working Group on Data Protection in Telecommunications "Working Paper on Cloud Computing - Privacy and data protection issues- "Sopot Memorandum" – " (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

[14] Resolution on cloud computing adopted during the 34th International Conference of Data Protection and Privacy Commissioners, Uruguay, 26 October 2012, available at: https://www.privacy.org.nz/further-resources/events-and-networks/closing-communique-28th-international-conference/

[15] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.6

[16] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.5
See also: International Working Group on Data Protection in Telecommunications "Working Paper on Cloud Computing - Privacy and data protection issues- "Sopot Memorandum" – " (24/04/2012)

Lack of control

Cloud clients entrust their personal data to the systems managed by a cloud provider. Therefore, they may no longer be in exclusive control of this data and cannot utilize and apply the technical and organisational measures necessary to ensure the availability, integrity, confidentiality, transparency, isolation, intervenability and portability of the data. More specifically:

- *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).[17]
- *Lack of integrity* caused by the sharing of resources: A cloud is made up of shared systems and infrastructures. Cloud providers process personal data deriving from a wide range of sources in terms of data subjects and organisations and it is possible that conflicting interests and/or different objectives might arise.[18]
- *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. In that case, there is a breach of EU data protection law.[19]
- *Lack of intervenability* due to the complexity and dynamics of the outsourcing chain: The cloud service offered by one provider might be the result of a combination of various services from a range of other providers, which may be dynamically added or removed during the duration of the client's contract.[20]
- *Lack of intervenability* regarding 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.[21]

---

https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Hon, W. Kuan, Christopher Millard, and Ian Walden. "The problem of 'personal data'in cloud computing: what information is regulated?—the cloud of unknowing." International Data Privacy Law 1.4 (2011): 211-228, p.213-214, available at: http://idpl.oxfordjournals.org/content/1/4/211.short

[17] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.5-7

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] Ibid.

- *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.[22]

Lack of 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.[23] More specifically, 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 European Economic Area. 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 European Economic Area. 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.[24]

In addition to the above challenges, the European Data Protection Supervisor further remarks the following challenges:

- In cloud computing environments, the client is usually unaware of the specific physical location of the data. This location is, in principle, not relevant for the service itself. It is more relevant to consider data accessibility and from where it can be performed. However, the hosting location of data is very important with respect to the applicability of national law. This is even more obvious where (national) authorities would need physical access to data.[25]
- There is a contractual asymmetry between service providers and clients, which renders compliance with personal data processing requirements in a cloud computing environment very difficult or even impossible for cloud clients acting as data controllers. This asymmetry could also lead to an undesirable allocation of responsibility in relation to compliance with data protection law. The qualification of data controller and processor must appropriately reflect

[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.6-7

the level of control over the means of processing, otherwise the responsibility for the protection of personal data in the cloud context risks to evaporate.[26]

- In cloud computing models, many different players are involved and cooperate in order to develop and deliver the service to the client. This fact questions and complexes the allocation of responsibilities, in particular when considering personal data processing requirements such as security of the data, access and auditing. This situation may be aggravated considerably with the addition of new providers to the service during operation.[27]
- Several issues are also raised in the context of personal data transfers. Cloud computing considerably increases transfers of personal data not only over networks, involving many different parties but also between countries, including these 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 services, data controllers and processors must ensure compliance of these transfers with data protection rules.[28]
- The evolutionary character of cloud computing itself poses challenges, as its technological characteristics and new trends development may have unpredictable impacts.[29]

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.[30]

We must not omit taking into account, however, the diversity of the available cloud computing offerings and schemes. 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 highlight and recognize the risks and define the most appropriate safeguards that must be implemented.[31]

[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid, p.7-8
[31] Ibid.

4. EU Data Protection Law in the Cloud: Overview of the Applicable Legal Framework

In this Chapter, an overview of the applicable EU legal framework is provided, with some comments on the applicability of the Directive 95/46/EC, and the implementation of this legal framework in Belgium. The proposed General Data Protection Regulation is also presented.

At this point, it is important to explain the difference between an EU Directive and an EU Regulation. An EU Directive is a legislative act that sets out a goal that all EU countries must achieve. However, it is up to the individual countries to devise their own laws on how to reach these goals. Therefore, it requires implementation by the Member States, as it is only a framework law. An EU Regulation, on the other hand, "regulation" is a binding legislative act, directly applicable in its entirety across the EU. No national implementation is required. As it is immediately applicable and enforceable by law in all Member States, it offers higher levels of law harmonization across the EU.[32]

4.1 The current EU Legal Framework

Personal data processing operations resulting from the use of cloud computing services and falling within the territorial scope criteria of EU data protection law (as explained in the next paragraphs) must respect the EU data protection provisions of Directive 95/46/EC.

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.[33]

Article 4 Directive 95/46/EC contains the criteria for establishing the applicability of national legislation. It refers to the law applying to controllers 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.[34]

---

[32] http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm and http://ec.europa.eu/legislation/index_en.htm

[33] European Data Protection Supervisor: ”Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.7

[34] Article 29 Working party Opinion 8/2010 on applicable law-WP 179 (16/12/2010), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf

According to Article 4 (1)(a) Directive 95/46/EC,[35] the factor that decides the application of EU law to the controller is the location of his or her establishment and the activities it carries out. In the context of cloud computing, therefore, the type of cloud service model remains 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.[36]

Therefore, Article 4(1)(a) Directive 95/46/EC sets forth a two-step test for its applicability: (i) does the data controller have an 'establishment' on the territory of an EU Member State, and (ii) does the controller process personal data in the context of activities of that establishment? If the answer to both questions is yes, then that Member State's implementation of the Directive 95/46/EC will apply to such personal data processing, wherever in the world it takes place – whether outside or inside the EEA. In other words, if a controller's EEA branch or office (or other 'establishment') wishes to process personal data in the cloud in the context of that branch or office's activities, it must comply with the local requirements of the EEA country in which the branch or office is established when processing personal data, wherever in the world the processing takes place.[37]

In case the controller is established in various Member States and processes 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.[38]

Article 4(1)(c) Directive 95/46/EC[39] regulates how data protection legislation applies to controllers who are not established in the EEA but use automated or non-

---

[35] *"1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:*
(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;"

[36] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.7
Hon, W. Kuan, Julia Hörnle, and Christopher Millard. "Data protection jurisdiction and cloud computing–when are cloud users and providers subject to EU data protection law? The cloud of unknowing." International Review of Law, Computers & Technology 26.2-3 (2012): 129-164, p.7, available at: http://www.tandfonline.com/doi/abs/10.1080/13600869.2012.698843

[37] Hon, W. Kuan, Julia Hörnle, and Christopher Millard. "Data protection jurisdiction and cloud computing–when are cloud users and providers subject to EU data protection law? The cloud of unknowing." International Review of Law, Computers & Technology 26.2-3 (2012): 129-164, p.8, available at: http://www.tandfonline.com/doi/abs/10.1080/13600869.2012.698843

[38] Ibid.

[39] *"Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:*
(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member

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.[40]

Regarding territorial scope, Article 3 of the proposed General Data Protection Regulation advances the already existing rules in two ways: first, by providing explicitly that the establishment of a processor in the EU would trigger the applicability of the Regulation and secondly, by introducing the new criteria of "offering goods or services to" or "monitoring the behavior of" data subjects in the EU.[41]

When 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 e-Privacy Directive 2002/58/EC.[42]

The e-commerce Directive 2000/31/EC[43] is also relevant in the cloud computing context. It defines the rules applicable to certain aspects of the information society services and cloud computing services usually fall within this scope. The e-commerce Directive provides of 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 data protection rules of Directive 95/46/EC,

---

State, unless such equipment is used only for purposes of transit through the territory of the Community."

[40] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.7
Hon, W. Kuan, Julia Hörnle, and Christopher Millard. "Data protection jurisdiction and cloud computing–when are cloud users and providers subject to EU data protection law? The cloud of unknowing." International Review of Law, Computers & Technology 26.2-3 (2012): 129-164, p.13, available at: http://www.tandfonline.com/doi/abs/10.1080/13600869.2012.698843

[41] Hon, W. Kuan, Julia Hörnle, and Christopher Millard. "Data protection jurisdiction and cloud computing–when are cloud users and providers subject to EU data protection law? The cloud of unknowing." International Review of Law, Computers & Technology 26.2-3 (2012): 129-164, p.33, available at: http://www.tandfonline.com/doi/abs/10.1080/13600869.2012.698843

[42] 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
It 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.

[43] 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.

according with which the processing of personal data by Internet service providers falls within the scope of data protection law. Their level of responsibility may vary, though, depending on whether they act as a processor or as a controller. In the context of the e-commerce Directive, their liability is focused on ensuring the confidentiality and security of the data, while in the context of Directive 95/46/EC 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.[44]

4.1.1 Belgian Legislation

The Privacy Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (*Loi vie privée/ Privacywet*) aims at protecting individuals against abuse of their personal data.[45] It establishes the rights and obligations of the individuals whose data are processed, as well as the rights and obligations of those processing the data. It further established an independent supervisory authority, the Commission for the Protection of Privacy (also known as "the Privacy Commission", the Belgian Data Protection Authority). As an independent body, the Commission ensures that personal data are used and protected with due care, so that citizens' privacy remains safeguarded.[46]

---

[44] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.7
Recital 47 of Directive 95/46/EC is also relevant: *"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."*

[45] See: Keuleneer, Fernand, and Dirk Lontings. "Privacy Protection and Personal Data Processing in Belgium: Analysis of a New Law's Centralized Approach to Regulation." Int'L Company & Com. L. Rev. 4 (1993): 344-344, available at: https://www.anthologieprivacy.be/sites/anthology/files/Privacy_protection_and_personal_data_processing_in_Belgium:_analysis_of_a_new_law's_centralised_approach_to_regulation.pdf

[46] Information available on the Belgian Data Protection's Authority website: https://www.privacycommission.be/en/privacy-act
See also: "Protection of personal data in Belgium", a document of the Belgian Data Protection Authority, which summarizes the basic principles of Belgian Data Protection Law, available at: https://www.privacycommission.be/sites/privacycommission/files/documents/protection-of-personal-data-in-belgium.pdf
An unofficial translation of the Privacy Act is also available in the website of the Belgian Data Protection Authority: https://www.privacycommission.be/sites/privacycommission/files/documents/Privacy_Act_1992.pdf
An overview of data protection in Belgium is also available in: http://uk.practicallaw.com/2-502-2977 and http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2015/belgium and http://www.mondaq.com/x/230854/data+protection/Data+Protection+Laws+of+the+World+Handbook+Second+Edition+Belgium

The Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data has undergone several substantial modifications. The first modification was the result of the adoption of Directive 95/46/EC on the protection of individuals with regards to the protection of their personal data, aiming at harmonizing personal data protection rules in the European Union. Consequently, Belgium, like all other member states, had to transpose this directive into Belgian law. That is why the Act of 8 December 1992 was modified by the Act of 11 December 1998.[47]

The second modification of the Privacy Act was upon the initiative of the Belgian legislator and it was an essential step in order to modernize it due to the rapid evolution of our computerised society. With the Act of 26 February 2003 the Privacy Commission's statute, composition and competences were adapted and the Sector Committees were established.[48]

The first Royal Decree implementing the Privacy Act was adopted in 2001, on the occasion of the transposition of European Directive 95/46/EC into the Privacy Act. In 2003 a second implementing decree established the way the sector committees work.[49]

The Electronic Communications Act of June 13, 2005 (Wet betreffende de elektronische communicatie/Loi relative aux communications électroniques) contains provisions regarding the confidentiality of electronic communications and the use of cookies and similar technologies. In addition, the processing of personal data for electronic marketing purposes is regulated in the Belgian Code on Economic Law of February 28, 2013.[50] There is also sector-specific legislation that impacts data protection: the Electronic Communications Act imposes requirements on providers of telecommunication and internet services regarding data retention, the use of location data and the notification of data security breaches. There is also specific legislation on the processing of personal data in the financial sector.[51] The Electronic Communications Act basically transposes the EU Telecom Package which includes, among others, the amended e-Privacy Directive. The e-Privacy Directive was implemented in Belgian law by the Act of July 10, 2012 containing various provisions on electronic communications. This Act amended Article 129 of the Belgian Act on Electronic Communications of June 13, 2005 to implement the new requirements on which were provided in the e-Privacy Directive (it is also named as the “Cookie

[47] https://www.privacycommission.be/en/privacy-act
[48] https://www.privacycommission.be/en/privacy-act
[49] https://www.privacycommission.be/en/privacy-act-and-implementing-decrees
[50] http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2015/belgium
[51] http://www.iclg.co.uk/practice-areas/data-protection/data-protection-2015/belgium

Directive"). The amendments to the Belgian Act on Electronic Communications of June 13, 2005 stipulating the new requirements entered into force on August 4, 2012.[52]

On March 11 2003 the E-commerce Directive (2000/31) was implemented into Belgian law, through the E-Commerce Act. Among other things, the Belgian legislation introduced information requirements which are applicable, in principle, to all electronic contracts. The main purpose of these requirements is to ensure transparency in transactions concluded by electronic means.[53]

4.2 The proposed General Data Protection Regulation

The European Commission's Proposal for a Data Protection Regulation was adopted on 25 January 2012 and 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.[54] 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.[55]

As part of the review, the territorial scope of EU data protection law is redefined. The proposed Regulation also introduces some 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. These new proposals maintain the technologically neutral approach of EU data protection rules in Directive 95/46/EC and do not focus on any specific technology, although they take into account technological developments. Therefore, they will also be applicable to and enclose cloud computing services.[56]

---

[52] Implementation of the Cookie Directive in Belgium-a status update: https://www.nymity.com/~/media/Nymity/Files/Interviews/2013/2013-04-dhontdumont.aspx and http://www.linklaters.com/Insights/Publication1403Newsletter/PublicationIssue20050728/Pages/PublicationIssueItem545.aspx

[53] http://www.internationallawoffice.com/Newsletters/E-commerce/Belgium/NautaDutilh/Information-Requirements-of-the-E-commerce-Act and http://whoswholegal.com/news/features/article/18245/it-privacy-e-commerce-belgium-recent-developments/ and http://www.timelex.eu/en/blog/detail/new-rules-for-e-commerce

[54] Directive 95/46/EC needed to be implemented at a national level, requiring transposition into national law by the national legislature of each member state. The proposed General Data Protection Regulation is directly applicable in all Member States. It applies automatically in each Member State and does not require any national implementation by the Member States.

[55] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.8-9

[56] Ibid.

On 17 December 2015, after three years of drafting and negotiations, the European Parliament and the Council of the European Union reached an informal agreement on the final draft of the EU General Data Protection Regulation, which is backed by the Committee on Civil Liberties, Justice and Home Affairs. Once officially adopted by the European Parliament and the Council of the European Union, the GDPR will apply in EU Member States after a period of two years.[57]

5. Introduction to EU Data Protection Law

The purpose of this Chapter is two-fold: first, it aims at providing an overview and introduction in the basic principles and rules of the EU Data Protection Law as legislated in the Directive 95/46/EC and, secondly, aims at familiarizing non-lawyer readers with data protection principles and terminology. The systematic and categorized approach followed is mostly based on the Handbook on EU Data Protection Law issued by the European Union Agency for Fundamental Rights and the Council of Europe and the Directive 95/46/EC.[58] A more detailed analysis in connection with the specific Cloud Computing legal requirements follows in the next chapter.

5.1 Data Protection terminology

Under EU Law, ***'personal data'*** are defined as information relating to an identified or identifiable natural person.[59] It is information about a person whose identity is either manifestly clear or can at least be established by obtaining additional information. If data about such a person are being processed, this person is called the ***'data subject'***.

A piece of information contains data about a person if an individual is identified in this information or if an individual, while not identified, is described in this information in a way which makes it possible to find out who the data subject is by conducting further research.

Sensitive data is a special category of personal data which, by their nature, may pose a risk to the data subjects, when processed, and need enhanced protection.[60] The processing of sensitive data must therefore be allowed only with specific safeguards.

On challenges regarding jurisdictional applicability see also: Hon, W. Kuan, et al. "Cloud accountability: the likely impact of the proposed EU data protection regulation." Queen Mary School of Law Legal Studies Research Paper 172 (2014), available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2405971

[57] EU Data Protection Regulation Tracker: https://www.huntonregulationtracker.com/

[58] Available at: http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf

[59] Article 2(a) Directive 95/46/EC

[60] According to Article 8 Directive 95/46/EC, sensitive data are the personal data revealing racial or ethnic origin, personal data revealing political opinions, religious or other beliefs and personal data concerning health or sexual life.

According to the principle of limited retention of data, data must be kept *"in a form which permits 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."*[61] Consequently, data would have to be anonymised if a controller wanted to store them after they were outdated and no longer served their initial purpose. Data are anonymised if all identifying elements have been eliminated from a set of personal data.

Processing of personal data means any operation […] such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" performed upon personal data.[62]

A ***data controller*** is someone who *"alone or jointly with others determines the purposes and means of the processing of personal data".*[63] A controller's decision lays down why and how data shall be processed. There might also be several legally separate entities who together or jointly with others act as controller. This means that they decide together to process data for a shared purpose.[64] This is legally possible, however, only in cases where a special legal basis provides for processing the data jointly for a common purpose.

A ***data processor*** is someone who processes personal data on behalf of a controller.[65] The activities entrusted to a processor may be limited to a very specific task or context or may be quite general and comprehensive.

The most important consequence of being a controller or a processor is legal responsibility for complying with the respective obligations under data protection law. For the sake of clarity and transparency, the details of the relationship between a controller and a processor should be recorded in a written contract.[66]

A ***third party*** is *"any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data*".[67]

A ***recipient*** means *"a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not"*.[68] This recipient may either be a person outside the controller or processor – this would then be a third

[61] Article 6(1) Directive 95/46/EC
[62] Article 2(b) Directive 95/46/EC
[63] Article 2(d) Directive 95/46/EC
[64] Ibis
[65] Article 2(e) Directive 95/46/EC
[66] Article 17(3) and 17(4) Directive 95/46/EC
[67] Article 2(f) Directive 95/46/EC
[68] Article 2(g) Directive 95/46/EC

party – or someone inside the controller or processor, such as an employee or another division within the same company or authority.

Consent means *"any freely given specific and informed indication of the data subject's wishes"*.[69] In order for consent to be valid, the data subject must have been under no pressure when consenting, the data subject must have been duly informed about the object and consequences of consenting and the scope of consent must be reasonably concrete. The consent can be given either explicitly[70] or non-explicitly. The former leaves no doubt about the intentions of the data subject and can be made either orally or in writing; the latter is concluded from the circumstances. Every consent must be given in an unambiguous way.[71]

The ***European Data Protection Supervisor*** is the independent supervisory authority at EU level with responsibilities for monitoring the processing of personal data by the EU institutions and bodies, advising on policies and legislation that affect privacy and cooperating with similar authorities to ensure consistent data protection.[72]

The ***Article 29 Working Party*** is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States. The Working Party is composed of: (i) representatives of the national supervisory authorities in the Member States; (ii) a representative of the European Data Protection Supervisor (EDPS); (iii) a representative of the European Commission (the latter also provides the secretariat for the Working Party).[73] After the adoption and the implementation of the proposed General Data Protection Regulation, the Article 29 Working Party will be replaced by the "European Data Protection Board".

A ***Data Protection Authority*** (DPA) is an independent body which is in charge of: (i) monitoring the processing of personal data within its jurisdiction (country, region or international organization); (ii) providing advice to the competent bodies with regard to legislative and administrative measures relating to the processing of personal data; (iii) hearing complaints lodged by citizens with regard to the protection of their data protection rights.[74]

According to Article 28 of Directive 95/46/EC, each Member State shall establish in its territory at least one data protection authority, which shall be endowed with investigative powers (such as access to data, collection of information, etc.), effective

[69] Article 2(h) Directive 95/46/EC
[70] Article 8(2) Directive 95/46/EC
[71] Articles 8(2), 7(a) and 26(1) Directive 95/46/EC.
[72] More information can be found on the EDPS website: https://secure.edps.europa.eu/EDPSWEB/edps/EDPS
[73] More information can be found on the Article 29 Working Party website: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
[74] https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary/pid/74

powers of intervention (power to order the erasure of data, to impose a ban on a processing, etc.), and the power to start legal proceedings when data protection law has been violated. National data protection authorities have been established in almost all European countries, as well as in many other countries worldwide. (e.g. the Information Commissioner's Office (ICO) in the UK).

5.2 Key Principles of EU Data Protection Law

The ***principle of lawful processing*** is enshrined in Article 6 Directive 95/46/EC. It practically required that the personal data processing must be in accordance with the law, pursues a legitimate purpose and is necessary in a democratic society in order to achieve the specific legitimate purpose.

The ***principle of purpose specification and limitation*** means that the legitimacy of processing personal data will depend on the purpose of the processing.[75] The purpose must have been specified and made manifest by the controller before the processing of data starts. The processing of personal data for undefined and/or unlimited purposes is unlawful.

The ***principles of data quality*** must be implemented by the data controller in all processing operations. These are the following:

- The ***data relevancy principle***: Only such data shall be processed as are adequate, relevant and not excessive in relation to the purpose for which they are collected and/or further processed".[76] The categories of data chosen for processing must be necessary in order to achieve the declared overall aim of the processing operations, and a controller should strictly limit collection of data to such information as is directly relevant for the specific purpose pursued by the processing.
- The ***data accuracy principle***: a controller holding personal information shall not use that information without taking steps to ensure with reasonable certainty that the data are accurate and up to date. The obligation to ensure accuracy of data must be seen in the context of the purpose of data processing. The limited retention of data principle: personal data are "kept in a form which permits 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."[77] The data must therefore be erased when those purposes have been served. The time limitation for storing personal data applies, however, only to data kept in a form which permits identification of data subjects. Lawful

[75] Article 6(1)(b) Directive 95/46/EC.
[76] Article 6(1)(c) Directive 95/46/EC
[77] Article 6(1)(e) Directive 95/46/EC

storage of data which are no longer needed, could, therefore, be achieved by anonymisation of the data or pseudonymisation.

- The ***fair processing principle***: the principle of fair processing governs primarily the relationship between the controller and the data subject, in the context of transparency. Transparency establishes an obligation for the controller to keep the data subjects informed about how their data are being used. Processing operations must be explained to the data subjects in an easily accessible way which ensures that they understand what will happen to their data. A data subject also has the right to be told by a controller on request if his or her data are being processed, and, if so, which ones.
- The ***principle of accountability***: it requires the active implementation of measures by controllers to promote and safeguard data protection in their processing activities. Controllers are responsible for the compliance of their processing operations with data protection law. Controllers should be able at any time to demonstrate compliance with data protection provisions to data subjects, to the general public and to supervisory authorities. Article 6 (2) of the Data Protection Directive states that the controller should ensure compliance with the principles relating to data quality included in paragraph 1. In the context of the accountability principle, the Data Protection Directive mentions several instruments for promoting compliance, such as: prior checking of intended processing operations by the national supervisory authority;[78] personal data protection officials who shall provide the controller with special expertise in the field of data protection;[79] codes of conduct specifying the existing data protection rules for application in a branch of society, especially of business.[80]

5.3 Rules on lawful personal data processing

Personal data may be lawfully processed if the processing is based on one of the following legal bases:[81] (i) the consent of the data subject or (ii) vital interests of data subjects requiring the processing of their data or (iii) legitimate interests of others as a reason for processing, but only as long as they are not overridden by interests in protecting the fundamental rights of the data subjects.[82]

[78] Article 20 Directive 95/46/EC
[79] Article 18(2) Directive 95/46/EC
[80] Article 27(1) Directive 95/46/EC
[81] All processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the Data Protection Directive and, secondly, with one of the criteria for making data processing legitimate.
[82] Article 7 Directive 95/46/EC

Lawful processing of sensitive personal data is subject to a special, stricter regime.[83] The processing of sensitive data is prohibited in principle. There is, however, an exhaustive list of enumerated exemptions to this prohibition, which can be found in Article 8 (2) and (3) of the Directive. These exemptions include explicit consent of the data subject, vital interests of the data subject, legitimate interests of others and public interest.

5.4 Rules on security of personal data processing

The rules on security of processing imply an obligation of the controller and the processor to implement appropriate technical and organisational measures in order to prevent any unauthorised interference with data processing operations.[84] The necessary level of data security is determined by the security features available in the market for any particular type of processing and the costs and the sensitivity of the data processed.

The secure processing of data is further safeguarded by the general duty on all persons, controllers or processors, to ensure that data remain confidential. Article 16 of the Data Protection Directive concerns confidentiality only within a controller–processor relationship. Whether or not controllers have to keep data confidential, in the sense that they may not disclose them to third parties, is dealt with under Articles 7 and 8 of the directive.

Data security is not just achieved by having the right equipment – hardware and software – in place. It also requires appropriate internal organisational rules.

5.5 Rules on transparency of personal data processing

Transparency is secured for the data subject by way of the controller's obligation to inform the data subject about the identity of the controller and the purpose of the data processing, and for the general public by way of notification.

Provision of information: controllers of processing operations are obliged to inform the data subject in advance about their intended processing.[85] This obligation does not depend on a request from the data subject but must be complied with proactively by the controller, regardless of whether the data subject shows interest in the information or not. The information must include the purpose of processing, as well as the identity and contact details of the controller. The Data Protection Directive requires further information to be given where this "is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject".

[83] Article 8 Directive 95/46/EC
[84] Article 17(1) Directive 95/46/EC
[85] Articles 10, 11 Directive 95/46/EC

National law can oblige controllers to notify the competent supervisory authority of their processing operations so that these can be published. Alternatively, national law can provide that controllers may employ a personal data protection official, who is responsible in particular for keeping a register of processing operations carried out by the controller.[86]

5.6 Data Subject's Rights

Everyone shall have the right under national law to request from any controller information as to whether the controller is processing his or her data.

- ***Right of access***: article 12 of the Data Protection Directive contains the elements of the data subjects' right of access, including the right to obtain from the controller "confirmation as to whether or not data relating to them are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are isclosed", which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data".
- ***Right to rectification, erasure and blocking of data***: "Any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing."[87] In line with these principles, data subjects must have the right under national law to obtain from the controller the rectification, erasure or blocking of their data if they think that their processing does not comply with the provision of the directive, in particular because of the inaccurate or incomplete nature of the data.[88]
- ***Right to object***: includes the right to object to automated individual decisions,[89] the right to object due to the data subject's particular situation[90] and the right to object to further use of data for direct marketing purposes[91].

Remedies and sanctions: national law must set out appropriate remedies and sanctions against infringements of the right to data protection. Before turning to the courts, one must first approach a controller.[92] Whether or not it is also mandatory to approach a supervisory authority before applying to a court, is left to regulation by

[86] Article 18(2) Directive 95/46/EC
[87] Recital 41, Directive 95/46/EC
[88] Article 12(b) Directive 95/46/EC
[89] Article 15(1) Directive 95/46/EC
[90] Article 14(a) Directive 95/46/EC
[91] Article 14(b) Directive 95/46/EC
[92] Approaching the national supervisory authority or a court directly would not help, as the authority could only advise that the controller must be addressed first, and the court would find an application inadmissible. The formal requirements for a legally relevant request to a controller, especially whether not it must be a written request, ought to be regulated by national law.

national law.[93] Rights under data protection law can be exercised only by the person whose rights are at stake; this will be someone who is, or at least claims to be, the data subject.

5.7 Transborder Data Flows

The Data Protection Directive not only provides for the free flow of data between the Member States but also contains provisions on the requirements for the transfer of personal data to third countries outside the EU. Transborder data flow is a transfer of personal data to a recipient who or which is subject to a foreign jurisdiction. Under EU law, restrictions or prohibitions on the free flow of data between Member States for reasons of data protection are forbidden by Article 1(2) of the Data Protection Directive.[94]

Transfer of personal data to third countries shall be free from restrictions under national data protection law, if: adequacy of data protection at the recipient has been ascertained or it is necessary in the specific interests of the data subject or legitimate prevailing interests of others, especially important public interests.

Adequacy of data protection in a third country means that the main principles of data protection have been effectively implemented in the national law of this country. The free flow of data to third countries with an adequate level of data protection is provided for in Article 25(1) of the Data Protection Directive. The requirement of adequacy rather than equivalence makes it possible to honour different ways of implementing data protection. According to Article 25 (6) of the directive, the European Commission is competent to assess the level of data protection in foreign countries through adequacy findings and consults on the assessment with the Article 29 Working Party which has substantially contributed to the interpretation of Articles 25 and 26.[95]

---

[93] Where a person, having made a request for access or having put in an objection with a controller, does not receive an answer which is timely and satisfactory, this person can approach the national data protection supervisory authority with a claim for assistance.
According to Article 22 Directive 95/46/EC, if the person, having made a request under data protection law to a controller, is not satisfied with the controller's response, this person must be entitled to bring a complaint before a national court.

[94] The area of free data flow has been extended by the Agreement on the European Economic Area (EEA), which brings Iceland, Liechtenstein and Norway into the internal market. (Decision of the Council and the Commission of 13 December 1993 on the conclusion of the Agreement on the European Economic Area between the European Communities, their Member States and the Republic of Austria, the Republic of Finland, the Republic of Iceland, the Principality of Liechtenstein, the Kingdom of Norway, the Kingdom of Sweden and the Swiss Confederation, OJ 1994 L 1.)

[95] For a continually updated list of countries that have received a finding of adequacy, see the homepage of the European Commission, Directorate-General for Justice, available at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
An adequacy decision by the European Commission has a binding effect.

Under Article 26(1) of the Data Protection Directive, interests of the data subject may justify the free flow of data to a third country if: the unambiguous consent of the data subject to the export of the data is given or the data subject enters – or prepares to enter – into a contractual relationship which clearly requires that the data be transferred to a recipient abroad or a contract between a data controller and a third party was closed in the interests of the data subject; or transfer is necessary in order to protect the vital interests of the data subject or for the transfer of data from public registers; this is an instance of prevailing interests in the general public to be able to access information stored in public registers.

The legitimate interests of others may justify free transborder flow of data owing to an important public interest, other than matters of national or public security, as they are not covered by the Data Protection Directive; or to establish, exercise or defend legal claims.

The Data Protection Directive also permits domestic law to establish regimes for transborder data flows to third countries not ensuring an adequate level of data protection, so long as the controller has made special arrangements to ensure adequate data protection safeguards at the recipient and so long as the controller can prove this to a competent authority.

The controller who wants to export data must demonstrate two issues during this examination: that a legal basis exists for the data transfer to the recipient and that measures are in place to safeguard adequate protection of the data at the recipient. Measures for establishing adequate data protection at the recipient may include: contractual stipulations between the data-exporting controller and the foreign data recipient[96] or binding corporate rules,[97] usually applicable for data transfers within a multinational group of companies.

Data transfers to foreign authorities can also be governed by a special international agreement.

[96] Article 26(4)
The European Commission with the assistance of the Article 29 Working Party developed standard contractual clauses which were officially certified by a Commission Decision as proof of adequate data protection. The existence of standard contractual clauses in the EU legal framework does not prohibit controllers from formulating other ad hoc contractual clauses. They would, however, have to produce the same level of protection as provided by the standard contractual clauses.

[97] Multilateral binding corporate rules (BCRs) very often involve several European data protection authorities at the same time.235 In order for BCRs to be approved, the draft of the BCRs must be sent together with the standardised application forms to the lead authority.236 The lead authority is identifiable from the standardised application form. This authority then informs all of the supervisory authorities in EEA member countries where affiliates of the group are established, although their participation in the evaluation process of the BCRs is voluntary. Although it is not binding, all data protection authorities concerned should incorporate the result of the evaluation into their formal licensing procedures.

6. EU Data Protection Law in the Cloud: Duties and responsibilities of the different players in Cloud Computing

This Chapter discusses the legal responsibilities imposed on the Cloud Computing players by EU Data Protection Law. Basically, it transposes the legal overview of Chapter 5 into legal requirements and translates it in the context of Cloud Computing, after explaining the roles of the various cloud players.

6.1 The different players in Cloud Computing

One of the most important and challenging aspects of the data protection legal framework in the cloud computing context is the applicability of the notions of "controller" and "processor". The crucial point is how to allocate responsibility for compliance with data protection rules.

Cloud computing involves a range of various and different players. In order to establish the specific obligations, duties and responsibilities of each player according to the data protection legal framework, it is, first of all, necessary to define, refine and assess the role of each of these players involved.

Article 29 Working Party, on Opinion 1/2010 on the concepts of "controller" and "processor" stressed out 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.*" Therefore, two general criteria can be extracted: allocation of responsibility and responsibility for compliance.[98]

6.1.1 Cloud Client and Cloud Provider

Article 2(d) Directive 95/46/EC 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 personal data".* 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.[99]

---

[98] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor"-WP 169 (16/02/2010), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

[99] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.10-11
Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.7-8

The cloud client, acting as controller, is responsible for complying with data protection legislation (usually through appropriate contractual safeguards) and is subject to all the relevant legal obligations defined in Directive 95/46/EC. The cloud client may assign the cloud provider to choose the methods and the technical or organisational measures to be used to achieve the purposes of the controller.[100]

Furthermore, Article 4(e) of the proposed General Data Protection Regulation defines the controller as the natural or legal person which "alone or jointly with others determines the purposes, conditions and means" of the personal data processing. The current provision (Article 2(d) of Directive 95/46/EC) does not include the term "conditions". As the EDPS observes, this change emphasizes even more the responsibility of those determining how a data processing activity will be concretely organised.[101]

The EDPS further comments: *"In this scenario, qualifying the relationship between provider and client as a 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."*[102]

The introduction, therefore, of controllership (by means of the word "conditions" in the legal text) considering the cloud services provider as co-controller will better

---

Information Commissioner's Office: "Guidance on the use of Cloud Computing" (2012), available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[100] Hon, W. Kuan, Christopher Millard, and Ian Walden. "Who is responsible for 'personal data'in cloud computing?—The cloud of unknowing, Part 2." International Data Privacy Law 2.1 (2012): 3-18, p.7-8, available at: http://idpl.oxfordjournals.org/content/2/1/3.short

[101] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.11-12

[102] Ibid;

Hon, W. Kuan, et al. "Cloud accountability: the likely impact of the proposed EU data protection regulation." Queen Mary School of Law Legal Studies Research Paper 172 (2014), p.15-16, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2405971

reflect the real level of influence on the purpose, conditions and means of processing operations.[103]

Article 2(d) Directive 95/46/ defines a processor as "*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*". The cloud provider is the entity that provides the various forms of cloud computing services. When the cloud provider supplies the means and the platform, acting on behalf of the cloud client ("data controller"), the cloud provider is considered as a data processor. (29WP) The suggested way to ensure compliance by the data processor is to strictly apply the requirements of Article 17 Directive 95/46/EC on the security of processing.[104]

The precise role of the cloud provider will have to be examined in a case by case basis, in order to assess whether or not it is processing personal data. If it is, it is important to determine whether the cloud provider is merely acting as a 'data processor' on behalf of the data controller or whether it is a data controller in its own right.[105]

---

[103] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.12

[104] Ibid;
Hon, W. Kuan, Christopher Millard, and Ian Walden. "Who is responsible for 'personal data'in cloud computing?—The cloud of unknowing, Part 2." International Data Privacy Law 2.1 (2012): 3-18, p.9, available at: http://idpl.oxfordjournals.org/content/2/1/3.short
See also: Article 29 Working Party Opinion 1/2010 on the notions of controller and processor for the criteria in order to assess controllership: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

[105] Information Commissioner's Office: "Guidance on the use of Cloud Computing" (2012), p.7. available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf
According to ICO, identifying the data controller in a private cloud should be quite straightforward because the cloud customer will exercise control over the purpose for which the personal data will be processed within the cloud service. If a cloud provider is contracted simply to maintain any underlying infrastructure then it is likely to be a data processor, ie it will only process the data on behalf of the data controller. This will include tasks such as allocating computing resources, performing and storing back-ups, providing support. In a community cloud, more than one data controller is likely to access the cloud service. They could act independently of each other or could work together, for example where they are involved in a joint enterprise. If one of the data controllers also maintains the cloud infrastructure, ie it is acting as a cloud provider, it will now also assume the role of a data processor in respect of the various data controllers that use the infrastructure. If the cloud customers intend to share data between themselves they must take the time to clarify their roles and be clear as to the extent to which they will be acting as data controllers in relation to the shared data. When using a public cloud, the ICO recognises that a cloud customer may find it difficult to exercise any meaningful control over the way a large (and perhaps global) cloud provider operates. However, simply because an organisation chooses to contract for cloud computing services on the basis of the cloud provider's standard terms and conditions, does not mean that the organisation is no longer responsible for determining the purposes for which and manner in which the personal data is to be processed. (p.7-9)
See also: Hon, W. Kuan, Christopher Millard, and Ian Walden. "Who is responsible for 'personal data'in cloud computing?—The cloud of unknowing, Part 2." International Data Privacy Law 2.1 (2012): 3-18, p.9, available at: http://idpl.oxfordjournals.org/content/2/1/3.short

Cloud providers as processors have a duty to ensure confidentiality. Article 16 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.

Processors must take into account the type of cloud in question (public, private, community or hybrid / IaaS, SaaS or PaaS) 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.[106]

The Article 29 Working Party 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. The European Data Protection Supervisor in his Opinion builds on the same position and further adds 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, who happens to have the technical background, 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)."*[107]

Furthermore, it is often the cloud service provider the one who develops standard contracts or Service Level Agreements to be offered to the cloud client, based on its technical infrastructure and business type. The cloud client has, therefore, has no or very little leeway to modify the technical or contractual means of the service. Another challenge for ensuring data protection compliance.[108]

---

[106] Hon, W. Kuan, Christopher Millard, and Ian Walden. "Who is responsible for 'personal data'in cloud computing?—The cloud of unknowing, Part 2." International Data Privacy Law 2.1 (2012): 3-18, p.11-15, available at: http://idpl.oxfordjournals.org/content/2/1/3.short

[107] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.12-13

[108] Ibid.

6.1.2 Subcontractors

Cloud computing services may involve many contracted parties who act as processors. Processors may also subcontract additional sub-processors which, accordingly, gain access to personal data. In case a processor subcontracts services to other processors (sub-processors), he is obliged to provide the client with any relevant information, especially on the type of service subcontracted, the characteristics of current or potential sub-contractors and guarantees that these entities act/will act in compliance with Directive 95/46/EC. Therefore, all the relevant obligations must 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 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.[109]

According to Article 29 Working Party, the processor can subcontract its activities only on the basis of the consent of the controller, given at the beginning of the service and accompanied with an obligation on behalf of the processor to inform the controller on any intended changes concerning the addition or replacement of subcontractors. The controller reserved the right to object to such changes or terminate the contract at any time. The cloud provider should be obliged to name all the delegated subcontractors. Furthermore, the cloud provider and the subcontractor(s) should sign a contract In addition, highlighting the terms, conditions and requirements of the contract between the cloud client and the cloud provider. The controller should be able to make use of contractual recourse possibilities in case of breaches of contracts caused by the sub-processors. Article 29 Working Party proposes that *"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."*[110]

6.2 Duties and responsibilities of the Cloud players

This Section discusses the legal requirements for the Cloud Client and Cloud Provider, as emanate from the EU Data Protection Law. They are divided into two categories: (i)

[109] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.9-10

[110] Ibid.

compliance with the basic data processing principles and (ii) technical and organizational measures implementation.

6.2.1 Compliance with the basic personal data processing principles

Personal data processing in the context of Cloud Computing is deemed lawful if it is performed in compliance with the basic principles of EU data protection law, as analysed in Chapter 5. These basic principles include: transparency towards the data subject, purpose specification and limitation, erasure of personal data as soon as their retention is not necessary anymore. Additionally and in order to safeguard data protection and data security, appropriate technical and organizational measures must be implemented.

6.2.1.1 Transparency

The principle of transparency is very crucial in order to perform a fair and legitimate processing of personal data in the cloud computing context. According to Article 10 Directive 95/46/EC, the cloud client is obliged to provide a data subject whose personal data or data related to him are collected with his identity and the purpose of the processing and also with any further relevant information such as: the recipients or categories of recipients of the data, which can also include processors and sub-processors in so far as such further information is necessary to guarantee fair processing in respect of the data subject.[111]

Article 11 Directive 95/46/EC also sets out a similar duty to inform the data subject when data have not been obtained from the data subject himself, but from different sources are recorded or disclosed to a third party.

Apart from the above case, transparency must also be guaranteed in the relationship(s) between cloud client, cloud provider and subcontractors (if any). The cloud client can assess the lawfulness of the processing of personal data in the cloud only 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.[112]

Another aspect of transparency in the context of cloud computing is the necessary knowledge the cloud client must have regarding all the subcontractors involved in the provision of the respective cloud service and the locations of all data centers in which personal data may be processed. This is crucial, because only under this condition an

[111] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p. 10-11
Kamarinou, Dimitra, Christopher Millard, and W. Kuan Hon. "Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers." Queen Mary School of Law Legal Studies Research Paper 209 (2015), p.20, 26 available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2646447
[112] Ibid

assessment can be made on whether personal data may be transferred to a 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.[113]

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.[114]

6.2.1.2 Purpose specification and limitation

The principle of purpose specification and limitation, as defined in Article 6(b) Directive 96/46/EC, requires that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The cloud client, therefore, is competent to determine the purpose(s) of the processing prior to the collection of personal data from the data subject and inform the data subject accordingly. The cloud client must not process personal data for other purposes, inconsistent with the original ones. Based on this prohibition, we can further deduce that a cloud service provider cannot, unilaterally, decide or arrange for personal data (and its processing) to be transmitted more or less automatically to unknown cloud data centres. This applies irrespective of whether this transfer is deemed to be beneficial and justifiable for the cloud service provider, for example as a reduction of operating costs, management of peak loads (overflow), load balancing, copying to backup, etc. Furthermore, the cloud service provider cannot use personal data for his own purposes.[115]

---

[113] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf , p.10-11
European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.12-13

[114] Ibid.

[115] Information Commissioner's Office: "Guidance on the use of Cloud Computing" (2012) p.4-5, available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf, p.17
Kamarinou, Dimitra, Christopher Millard, and W. Kuan Hon. "Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers." Queen Mary School of Law Legal Studies Research Paper 209 (2015), p.30, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2646447
International Working Group on Data Protection in Telecommunications "Working Paper on Cloud Computing - Privacy and data protection issues- "Sopot Memorandum" – " (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Moreover, further processing, incompatible with the original purpose(s), is also prohibited for the cloud provider or one of his subcontractors. As a typical cloud scenario may easily involve a larger number of subcontractors, the risk of further processing personal data for incompatible purposes is considered to be quite high. In order to mitigate the risk of further processing, the contract between cloud provider and cloud client should include technical and organisational measures 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. In case data protection legislation is violated, penalties should be imposed in the contract against the provider or subcontractor.[116]

6.2.1.3 Erasure of data

Article 6(e) Directive 95/46/EC states that personal data must be kept in a form which permits the identification of data subjects for no longer than 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 anonymised. If the data cannot be erased due to legal retention rules (e.g., tax regulations), access to this personal data should be prohibited and blocked. The responsibility to ensure that personal data are erased as soon as they are not necessary in the aforementioned sense any more lies in the cloud client. Erasure of data is a crucial issue not only throughout the duration of a cloud computing contract but also upon its termination. It is also relevant in case of substitution or withdrawal of a subcontractor.[117]

The principle of data erasure is applicable to personal data irrespective of whether they are stored on hard drives or other storage media (e.g., backup tapes). Since personal data may be kept at the same time 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).[118]

---

[116] Information Commissioner's Office: "Guidance on the use of Cloud Computing" (2012) p.4-5, available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf , p.17

[117] Kamarinou, Dimitra, Christopher Millard, and W. Kuan Hon. "Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers." Queen Mary School of Law Legal Studies Research Paper 209 (2015), p.46-47, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2646447
Hon, W. Kuan, Christopher Millard, and Ian Walden. "The problem of 'personal data'in cloud computing: what information is regulated?—the cloud of unknowing." International Data Privacy Law 1.4 (2011): 211-228, p.214-215, available at: http://idpl.oxfordjournals.org/content/1/4/211.short

[118] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.11-12
International Working Group on Data Protection in Telecommunications "Working Paper on Cloud Computing - Privacy and data protection issues- "Sopot Memorandum" – " (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Cloud clients must be aware of the fact that log data 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. 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.[119]

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.[120]

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. The same holds true for contracts between cloud providers and subcontractors.[121]

6.2.1.4 Responsibility and Accountability in the Cloud

The notion of accountability is not explicitly addressed in Directive 95/46/EC. It expresses the direct compliance obligation that data controllers have under the Directive. In Article 22 of the proposed General Data Protection Regulation, though, the responsibility and accountability of data controllers and processors in general is increased: they must be able to ensure and demonstrate, through the adoption and implementation of appropriate data protection policies and notices that their processing activities comply with the requirements of the Regulation. Responsibility and accountability are also expressed by the introduction of specific obligations such as data protection by design and by default, data security breach notifications and data protection impact assessments. Apart from the general improvement of the data subject's protection, these enhanced responsibilities of the data controller are also considered a major improvement in the cloud computing environment.[122]

---

[119] Kamarinou, Dimitra, Christopher Millard, and W. Kuan Hon. "Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers." Queen Mary School of Law Legal Studies Research Paper 209 (2015), p.46-47, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2646447

[120] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.11-12

[121] Ibid.
See also: Hon, W. Kuan, Christopher Millard, and Ian Walden. "The problem of 'personal data'in cloud computing: what information is regulated?—the cloud of unknowing." International Data Privacy Law 1.4 (2011): 211-228, available at: http://idpl.oxfordjournals.org/content/1/4/211.short

[122] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.14
European Data Protection Supervisor: "Opinion of 7 March 2012 on the Data Protection reform package", available at:

However, the European Data Protection Supervisor observes that certain types of these new obligations (in particular: the 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) 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.[123]

As the EDPS further explains, in a cloud computing environment, this would mean that the client/controller should be able, for instance, to implement appropriate technical and organizational 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 to influence the technical and organisational structure of the service. It is unrealistic to expect from a large provider with many customers to tailor and adapt its technical infrastructure or organisation to meet the specific compliance requirements of each customer on the basis of individually negotiated contracts.[124]

In consequence, the need to appropriately qualify the data controller and processor as explained in previous sections is once more highlighted, as it is the key to ensure the respect of these enhanced responsibility and accountability obligations.

Data Protection Impact Assessment of Cloud Computing Services

The proposed General Data Protection Regulation, in Article 33, introduces an obligation for the data controller or the processor acting on the controller's behalf to carry out a data protection impact assessment.[125] No clear provisions or guidelines on how to carry out such data protection impact assessments are included in the proposed Regulation. Therefore, the implementation of this requirement is based on

---

https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, par.166
See also: Hon, W. Kuan, et al. "Cloud accountability: the likely impact of the proposed EU data protection regulation." Queen Mary School of Law Legal Studies Research Paper 172 (2014), http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2405971

[123] European Data Protection Supervisor: ”Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.14

[124] Ibid.

[125] The list of the processing operations where data protection impact assessments should be mandatory is non-exhaustive.

the subjective assessment made by each controller, which can lead to different results.

Since the use of cloud computing services for personal data processing could sometimes involve specific data protection risks, data protection impact assessments can be proven to be a very useful tool in order to identify these risks and define appropriate mitigation measures. The European Data Protection Supervisor highlights in particular the importance of carrying out data protection impact assessments regarding 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). The European Data Protection Supervisor and the Article 29 Working Party also recommend that the criteria and conditions to determine when a data protection impact assessment is required and the elements to be analysed should be set forth in a delegated act. In the context of cloud computing services, it would be very useful useful if the European Commission developed templates that could be used by public administrations, individuals and companies in order to evaluate and manage risks.[126]

Audits and Certifications

The European Data Protection Supervisor identifies another crucial aspect that directly affects the accountability principle and the application of its requirements in the Cloud Computing context: the interaction of various parties along the end-to-end value chain in order to deliver the service to the end customer. It is of utmost importance that these multiple actors trust each other in order to act responsibly and in coordination and take appropriate measures to ensure that data processing operations are carried out in compliance with data protection rules.[127]

In this respect, the European Data Protection Supervisor recognizes the value of internal and trusted third party audits and subsequent certifications in verifying

---

[126] European Data Protection Supervisor: ”Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf , p.14 and
Article 29 Working Party Opinion 08/2012 providing further input on the data protection reform discussions-WP 199 (05/10/2012), pages 31-32, available at: http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf

[127] European Data Protection Supervisor: ”Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.15-16
On third party audits, see also: International Working Group on Data Protection in Telecommunications “Working Paper on Cloud Computing - Privacy and data protection issues- “Sopot Memorandum” – “ (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

responsibility and accountability when multiple parties are involved. Such audits should themselves be based on appropriate certification and standardisation models.[128]

Article 22 of the proposed General Data Protection Regulation specifies the data protection measures that controllers are required to take. Among others, it requires for example that the controller should 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. Article 26 indirectly specifies the data protection measures that the processors must take. The EDPS welcomes this provision but also comments that in the context of cloud computing more specific guidance is necessary in order to clarify which mechanisms should be put in place to ensure verification of the effectiveness of data protection measures in practice. Otherwise, these verification exercises risk measuring compliance only on "paper" but not in "reality". The European Data Protection Supervisor also takes note that the proposed Regulation in Article 22 provides for the Commission to adopt delegated acts to specify, *inter alia*, the conditions for the verification and auditing mechanisms referred to in the same Article. Besides this provision, Cloud Computing specific codes of conduct drawn up by the industry and approved by the relevant data protection authorities could also be a useful tool to enhance compliance as well as trust among the various players. The codes of conduct model is present both in Directive 95/46/EC and the proposed General Data Protection Regulation (Articles 27 and 38 respectively).[129] Provided that they are fully respectful of data protection requirements, 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.[130]

6.2.2 Technical and organizational measures of data protection and data security

Article 17(2) Directive 95/46/EC obliges cloud clients (when acting as data controllers) to choose cloud providers that implement adequate technical and organizational security measures governing the personal data processing and to be able to demonstrate accountability and compliance with these measures. These technical and organizational measures must protect confidentiality, integrity and availability of data, by preventing inter alia unauthorized access, modification, erasure or removal.[131]

---

[128] Ibid.

[129] European Data Protection Supervisor: ”Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.16

[130] Ibid, par.110

[131] International Working Group on Data Protection in Telecommunications “Working Paper on Cloud Computing - Privacy and data protection issues- “Sopot Memorandum” – “ (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-

In addition to the core security objectives of availability, confidentiality and integrity, Article 29 Working Party also draws attention to the complementary data protection goals of transparency, isolation, intervenability, accountability and portability (as analysed above in Chapter 6.2.1).[132] This section highlights these central data protection goals, without prejudice to other complementary security oriented risk analysis.

Under the proposed General Data Protection 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. Regarding technical and organizational measures in Cloud Computing environments, the European Data Protection Supervisor highlights that all parties involved, whether controller or processor, should perform risk assessments for the processing under their control, due to the complexity that Cloud Computing adds. 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. 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.[133]

Informing cloud users on the risk assessment and security measures of the cloud provider and better understand their effectiveness and limitations would enable cloud users, accordingly, to also take necessary measures, as the European Data Protection Supervisor further observes. However, "*there is typically no transparency about the IT security measures that are implemented. Details of security incidents are often not*

protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Information Commissioner's Office "Guidance on the use of Cloud Computing" (2012), p.13, available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

Kamarinou, Dimitra, Christopher Millard, and W. Kuan Hon. "Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers." Queen Mary School of Law Legal Studies Research Paper 209 (2015), p.51-52, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2646447

[132] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.14

[133] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p. 20

See also: Hon, W. Kuan, et al. "Cloud accountability: the likely impact of the proposed EU data protection regulation." Queen Mary School of Law Legal Studies Research Paper 172 (2014), p.24, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2405971

reported to clients. Therefore, this makes it difficult for cloud clients to even evaluate the security of the processing operation."[134]

Compliance with security obligations is achievable for data controllers when they have extensive and accurate information allowing them to make the assessment that the cloud provider fully complies with his security obligations as processor or controller. Processing of personal data must not be assigned to cloud service providers that do not provide sufficient information and transparency regarding their security measures.[135]

The introduction of data breach notification in the proposed General Data Protection Regulation (Articles 31 and 32) imposes the obligation on data controllers to inform Data Protection Supervisory Authorities and data subjects about personal data breaches. Cloud providers, therefore, would have to report any personal data breaches that occur in their services, either directly (to the supervisory authorities and the individuals), in case they act as controllers, or indirectly (to the cloud client who is the data controller) if they are only processors.[136]

The proposed General Data Protection Regulation would make it possible for the European Commission to further specify, by the adoption of implementing acts where necessary, the applicable security requirements and the criteria and circumstances for establishing data breaches as well as format and procedure of notifications. These implementing acts could clarify the responsibilities of the different players in the complex Cloud Computing environment. The development of European standards for data protection and IT security in cloud computing environments and the development and recognition of metrics could be beneficial.[137]

---

[134] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p. 20

[135] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p. 20

[136] Ibid.

See also: International Working Group on Data Protection in Telecommunications "Working Paper on Cloud Computing - Privacy and data protection issues- "Sopot Memorandum" – " (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

Hon, W. Kuan, et al. "Cloud accountability: the likely impact of the proposed EU data protection regulation." Queen Mary School of Law Legal Studies Research Paper 172 (2014), available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2405971

[137] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf , p. 20

6.2.2.1 Availability

Providing availability, according to Article 29 Working Party, means ensuring timely and reliable access to personal data.[138]

Availability in the cloud can be threatened by 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) attacks.[139] 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.[140]

Data controllers should, therefore, check whether the cloud provider has adopted reasonable measures to cope with the risk of interferences, such as backup internet network links, redundant storage and effective data backup mechanisms.[141]

6.2.2.2 Integrity

Integrity could be defined as the quality of the data to keep their authenticity and 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 unmodified.[142]

Personal data modifications can be detected 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.[143]

6.2.2.3 Confidentiality

In a cloud environment, encryption may significantly contribute to the confidentiality of personal data if applied correctly, although it does not render personal data irreversibly anonymous. It is merely a tool for the cloud client to ensure that the personal data they are responsible for can only be accessed by authorized persons

---

[138] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.14

[139] A DoS attack is a coordinated attempt to make a computer or network resource unavailable to its authorized users, either temporarily or indefinitely (e.g., by means of a large number of attacking systems paralyzing their target with a multitude of external communication requests). (https://www.techopedia.com/definition/24841/denial-of-service-attack-dos)

[140] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.14

[141] Ibid.

[142] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.15

[143] Ibid.

who have the correct "key".[144] Recital 26 of Directive 95/46/EC states: *"(...); whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; (...)"*. The technical data fragmentation processes that may be used in the framework of the provision of Cloud Computing services, such as encryption, will not lead to irreversible anonymisation and thus does not imply that data protection obligations do not apply.[145] Encryption of personal data should be used in all cases when "in transit" and when available to data "at rest".[146] This applies particularly 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. 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.[147]

Communications between cloud provider and client as well as between data centres should also 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, he must bear in mind that encryption cannot be maintained during processing of the data (except of very specific computations).[148]

When encryption is chosen as a technical measure to secure data, it is also important to guarantee the security of the key. A robust key management arrangement is crucial to maintain the high level of protection encryption can offer. It is also important to

---

[144] Information Commissioner's Office "Guidance on the use of Cloud Computing" (2012), p.14, available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[145] Ibid.
See also: Hon, W. Kuan, Christopher Millard, and Ian Walden. "The problem of 'personal data'in cloud computing: what information is regulated?—the cloud of unknowing." International Data Privacy Law 1.4 (2011): 211-228, p.217-218, available at: http://idpl.oxfordjournals.org/content/1/4/211.short

[146] Information Commissioner's Office "Guidance on the use of Cloud Computing" (2012), available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[147] International Working Group on Data Protection in Telecommunications "Working Paper on Cloud Computing - Privacy and data protection issues- "Sopot Memorandum" – " (24/04/2012) https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group
Information Commissioner's Office "Guidance on the use of Cloud Computing" (2012), p.14-15, available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[148] Hon, W. Kuan, Christopher Millard, and Ian Walden. "The problem of 'personal data'in cloud computing: what information is regulated?—the cloud of unknowing." International Data Privacy Law 1.4 (2011): 211-228, p.219, available at: http://idpl.oxfordjournals.org/content/1/4/211.short

note that the loss of an encryption key could render the data useless. This could amount to the accidental destruction of personal data and therefore a breach of the security principle.[149]

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.[150]

6.2.2.4 Transparency

Technical and organisational measures must support transparency in order to allow review (see Section 6.2.1.1 for the Transparency analysis, which is also applicable in this context)[151]

6.2.2.5 Isolation (purpose limitation)

Isolation is an expression of the purpose limitation principle. In cloud infrastructures, resources such as storage, memory and networks are shared among many users. This creates new risks for data and renders the possibility of disclosure and further processing for illegitimate purposes quite high. Isolation as a protective goal, therefore, is meant to address this issue and ensure that data is not used beyond its initial original purpose and to maintain confidentiality and integrity.[152]

Isolation is achieved first by adequate governance of the rights and roles for accessing personal data: it should be 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).[153] 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.[154]

6.2.2.6 Intervenability

According to Articles 12 and 14 of Directive 95/46/EC, the data subjects have the rights of access, rectification, erasure, blocking and objection. The cloud client must verify

[149] Information Commissioner's Office "Guidance on the use of Cloud Computing" (2012), p.15, available at: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf
[150] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.16
[151] Ibid.
[152] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.15
[153] Ibid.
[154] Ibid.

that the cloud provider does not impose technical and organisational obstacles to these requirements, even in cases when data is further processed by subcontractors. The contract between the client and the provider should demand that the cloud provider is obliged to support the client in facilitating exercise of data subjects' rights and to ensure that the same is safeguarded for his relation to any subcontractor.[155]

6.2.2.7 Portability

The use of standard data formats and service interfaces by the cloud providers is very important, as it facilitates interoperability and portability between different cloud providers. Therefore, if a cloud client decides to move to another cloud provider, any lack of interoperability may result in the impossibility or at least difficulties to transfer the client's (personal) data to the new cloud provider ("vendor lock-in"). The same problem also appears 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. Preferably, the provider should make use of standardised or open data formats and interfaces. Agreement on contractual clauses stipulating assured formats, preservation of logical relations and any costs accruing from the migration to another cloud provider could be considered as guarantees.[156]

Data portability is also defined in Article 18 of the proposed General Data Protection 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. In technical terms, it should become possible to verify the secure erasure of data.[157]

6.2.2.8 Accountability

In Information Technology, accountability is defined as the ability to demonstrate what an entity did at a certain point in time in the past and how. In the field of data protection, as discussed in Section 6.2.1.4, it takes a broader meaning and describes

[155] Ibid, p.16
[156] Ibid, p.16
[157] Hon, W. Kuan, et al. "Cloud accountability: the likely impact of the proposed EU data protection regulation." Queen Mary School of Law Legal Studies Research Paper 172 (2014), p.44-45, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2405971
European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p. 25

the ability of parties to demonstrate that they took appropriate steps to ensure that data protection principles have been implemented.[158]

Article 29 Working Party qualifies IT accountability as *"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."*[159]

Furthermore, cloud providers should provide documentary evidence of appropriate and effective measures that ensure the application 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 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.[160]

6.2.3 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 under the condition that this country or the recipient adopts 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, applying EU Data Transfers rules in the Cloud Computing environment is very challenging. One of the particularities of Cloud Computing is the fact that it is structured on a complete lack of any stable location of data within the cloud provider's network. The cloud client is therefore rarely able to know in real time where the data are located or stored or transferred. Consequently, the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations.[161] Cloud computing services rely on

---

[158] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf , p.16-17

[159] Ibid.

[160] Ibid.
Hon, W. Kuan, et al. "Cloud accountability: the likely impact of the proposed EU data protection regulation." Queen Mary School of Law Legal Studies Research Paper 172 (2014), p.44-45, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2405971
See also: Article 29 Working Party Opinion 3/2010 on the principle of accountability-WP 173 (13/07/2010), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

[161] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.17

the continuous flows of data of cloud clients across cloud service providers' infrastructure. Data are being transferred 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.[162]

Furthermore, according to the European Data Protection Supervisor, *"in cases where the cloud client is deemed to be the data controller, 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."* [163]

6.2.3.1 Adequacy decisions[164]

The application of international data transfer rules is usually based on an assessment of whether there is an adequate level of protection in the countries where the data are going to be transferred. However, as stated above, 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.[165]

Adequacy decisions, including the EU-US Safe Harbor Agreement,[166] have limited geographical scope. Therefore, they do not cover all transfers within the Cloud.

Hon, W. Kuan, and Christopher Millard. "Data Export in Cloud Computing-How Can Personal Data Be Transferred Outside the EEA." The Cloud of Unknowing, Part 4 (2012), p.5-6, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2034286

[162] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.16-17

[163] Ibid.

[164] 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 General Data Protection 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. (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm)

[165] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.17

[166] The US and the EU have made arrangements by way of a self-regulatory regime which allows organisations in the US (including cloud service providers) that import personal data from the EU to demonstrate an adequate standard of protection for the purposes of art 25 by participating in a Safe Harbor programme. (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML)
On 6 October, the Court of Justice of the European Union invalidated the European Commission's Decision on the Safe Harbour arrangement was invalid. On 2 February 2016, the European

Transfers to US organizations abiding by the principles can take place lawfully under EU law since the recipient organizations are considered to provide an adequate level of protection to the transferred data.

The Article 29 Working Party has commented regarding the Safe Harbor Agreement, that 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. Furthermore, Article 17 of the Directive 95/46/EC requires a contract to be signed from a controller to a processor for processing purposes, which is confirmed in the EU-US Safe Harbor Framework documents. This contract is not subject to prior authorization from the European Data Protection Authorities. 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 Data Protection Authorities may have additional requirements.[167]

The Article 29 Working Party further considers the following, using the Safe Harbor Agreement as an example:

Companies exporting data should not merely rely on the data importer's statement claiming a Safe Harbor certification. The company exporting data should also obtain evidence that the Safe Harbor self-certifications exist and request evidence demonstrating that their principles are complied with. This is important for transparency reasons and especially with regard to the information provided to data subjects affected by the data processing.[168]

The Article 29 Working Party also considers that the cloud client must verify if the standard contracts composed by cloud providers are compliant with national requirements regarding contractual personal data processing. National legislation may require sub-processing to be defined in the contract, 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

---

Commission and the United States agreed on a new framework for transatlantic data flows: the EU-US Privacy Shield. (http://europa.eu/rapid/press-release_IP-16-216_en.htm)
See also: Larry Downes "The Business Implications of the EU-US Privacy Shield" (10/02/2016), in Harvard Business review, available at: https://hbr.org/2016/02/the-business-implications-of-the-eu-u-s-privacy-shield and "Privacy Shield data agreement dismissed as 'reheated Safe Harbour'" in Business Cloud News: http://www.businesscloudnews.com/2016/02/03/privacy-shield-data-agreement-dismissed-as-reheated-safe-harbour/

[167] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p. 17-18

[168] Ibid.
See also: German Data Protection Authority: http://www.datenschutzberlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

instruments available, such as standard contractual clauses or Binding Corporate Rules.[169]

The Safe Harbor principles as such, may also not guarantee 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.[170] As it has already been analysed in Section 6.2.2, cloud computing raises several cloud-specific data security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles on data security.[171] Additional safeguards for data security may thus be deployed, for instance 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. Therefore, apart from the commitment to the Safe Harbor principles, additional safeguards should also be applied, taking into account the specific nature of the cloud.[172]

6.2.3.2 Exemptions

Article 26 of the Directive 95/46/EC provides for some exemptions which enable data exporters to transfer data out of the EU without providing additional guarantees. According to an Article 29 Working Party Opinion,[173] though, exemptions shall apply only where transfers are neither recurrent, nor massive or structural. Based on such interpretations, it is almost impossible to rely on exemptions in the context of cloud computing.[174]

6.2.3.3 Standard Contractual Clauses

Standard contractual clauses are adopted by the EU Commission for the purpose of governing international data transfers between two controllers or one controller and a processor. They are, therefore, based on a bilateral approach. When the cloud provider is considered to be the processor, model clauses 2010/87/EC are an

---

[169] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p. 17-18

[170] opinion by the Danish DPA: http://www.datatilsynet.dk/english/processing-of-sensitive-personaldata-in-a-cloud-solution

[171] A detailed analysis of these risks is described in the ENISA paper Cloud Computing: Benefits, Risks and Recommendations for Information Security at: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloudcomputing-risk-assessment.

[172] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.17-18

[173] 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).

[174] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.18

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.[175]

In addition to the standard contractual clauses, 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 the Commission or prejudice fundamental rights or freedoms of the data subjects.[176] Nevertheless, the companies may not amend or change the standard contractual clauses without implying that the clauses will no longer be "standard"[177].[178]

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.[179] As far as the contractual relationship between the non EU processor and the sub-processors is concerned, 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.[180]

6.2.3.4 Binding Corporate Rules

The Binding Corporate Rules are considered to be a sort of 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. Article 29 Working Party has worked on BCRs for processors which will allow the transfer within

---

[175] Hon, W. Kuan, and Christopher Millard. "Data Export in Cloud Computing-How Can Personal Data Be Transferred Outside the EEA." The Cloud of Unknowing, Part 4 (2012), p.19-20, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2034286

[176] 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

[177] Can Companies amend and change the standard contractual clauses approved by the Commission? Published by the EC on http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

[178] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.18-19

[179] Recital 23 Commission Decision 2010/87 EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087
See also: Article 29 Working Party FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC-WP 176 (12/07/2010), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_en.pdf

[180] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, p.19

the group for the benefit of the controllers without requiring the signature of contracts between processor and subprocessors per client.[181] 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.[182]

6.2.3.5 International transfers and the proposed General Data Protection Regulation

The proposed General Data Protection Regulation aims at balancing international transfers with high level protection for the personal data transferred. In particular, it provides for 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.[183]

As the European Data Protection Supervisor specifies, "a*rticle 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. This flexibility might be useful for Cloud computing providers, 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. What is important, though, is the following: 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 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.*

---

[181] 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
Hon, W. Kuan, and Christopher Millard. "Data Export in Cloud Computing-How Can Personal Data Be Transferred Outside the EEA." The Cloud of Unknowing, Part 4 (2012), p.20, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2034286

[182] Article 29 Working Party Opinion 05/2012 on Cloud Computing-WP 196 (01/07/2012), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf , p.19

[183] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p. 17
See also: Hon, W. Kuan, et al. "Cloud accountability: the likely impact of the proposed EU data protection regulation." Queen Mary School of Law Legal Studies Research Paper 172 (2014), p.31-36, available at: http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2405971

Supervisory authorities, when developing standard clauses or reviewing ad hoc clauses submitted to their approval, will pay particular attention to these essential aspects."[184]

Furthermore, Article 43 of the proposed Regulation sets forth a detailed and flexible mechanism for the use of Binding Corporate Rules. The European Data Protection Supervisor remarks that BCRs are a mechanism that is suitable for 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."*[185] 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.[186]

7. The role of Cloud Standards

In order to unleash the potential of cloud computing, the European Commission Communication on Cloud Computing released on September 27, 2012 identifies cutting through the jungle of standards as a one of the key actions to foster mass adoption of cloud computing as it could help cloud users enjoy interoperability, data portability, reversibility, data protection and data security.[187]

Standards play a very important rule in cloud computing for a variety of reasons. Each category of cloud standards has a different contribution:

Standards for interoperability and data and application portability can guarantee cloud computing market competition and openness, cooperation, interaction and exchange of information. Customers are not locked-in to cloud providers; on the contrary, they are able to transfer data or applications between cloud providers. Interoperability standards are important for cloud providers so that multiple clouds can work together and operate together to offer better and various services, to deal

---

[184] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.17-18
See also: Hon, W. Kuan, and Christopher Millard. "Data Export in Cloud Computing-How Can Personal Data Be Transferred Outside the EEA." The Cloud of Unknowing, Part 4 (2012), p.29, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2034286

[185] European Data Protection Supervisor: "Opinion of 16 November 2012 on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf, p.18

[186] Ibid.

[187] http://europa.eu/rapid/press-release_IP-12-1025_en.htm and http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

with emergencies and to give their customers greater flexibility and choice in the types of service offerings.[188] Regarding Data Portability in Cloud Computing, the term implies the ability of cloud users to recover the data supplied to, or generated by, the cloud service and to relocate them between multiple cloud providers at low cost and with the minimum interruption possible.[189] The need for data portability standards is driven by a concern that there is a risk of customers becoming overly dependent on one cloud provider and being unable of changing between service providers, which could have a negative impact on competition in the cloud market.[190] Reversibility is also related to "lock-in" prevention by allowing users to withdraw data from the Cloud.[191]

Standards for cloud security and for data protection in the cloud can guarantee safe cloud computing usage for the cloud customers. Standards in these areas build trust in cloud computing. Demonstrating compliance with data protection laws has become an increasing concern for cloud providers and customers, especially in the context of trust building in their service and how personal data are dealt with.[192] In response to the increasing use of cloud, the ISO/IEC has published a new standard specifically for the use of public clouds as data processors.[193] The standard aims at creating a common framework of security controls that can be implemented by a public cloud service

---

[188] Gleeson, Niamh Christina, and Ian Walden. "'It's a Jungle Out There'?: Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law (May 23, 2014) (2014), p.2-3 Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2441182
See also European Telecommunications Standards Institute (ETSI),Cloud Standards Coordination Final Report (ETSI, November 2013), 7, available at: http://www.etsi.org/images/files/events/2013/2013_csc_delivery_Ws/csc-Final_report-013-csc_Final_report_v1_0_pdF_format-.pdF

[189] European Telecommunications Standards Institute (ETSI),Cloud Standards Coordination Final Report (ETSI, November 2013), 7, available at: http://www.etsi.org/images/files/events/2013/2013_csc_delivery_Ws/csc-Final_report-013-csc_Final_report_v1_0_pdF_format-.pdF

[190] Gleeson, Niamh Christina, and Ian Walden. "'It's a Jungle Out There'?: Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law (May 23, 2014) (2014), p.2,4 Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2441182
See also See Walden, I. and Laíse Da Correggio Luciano "Facilitating Competition in the Clouds", in Ch.Millard (ed), *Cloud Computing Law,* (OUP, 2013), p.327-328.

[191] Gleeson, Niamh Christina, and Ian Walden. "'It's a Jungle Out There'?: Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law (May 23, 2014) (2014), p.4 Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2441182
See also: Industry Recommendations to Vice President Neelie Kroes on the Orientation of a European Cloud Computing Strategy, November 2011. Available at: http://ec.europa.eu/information_society/activities/cloudcomputing/docs/industryrecommendationsccstrategy-nov2011.pdf

[192] Gleeson, Niamh Christina, and Ian Walden. "'It's a Jungle Out There'?: Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law (May 23, 2014) (2014), p.4 Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2441182

[193] ISO/IEC DIS 27018, ‗Code of practice for PII protection in public cloud acting as PII processors', see http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498 . ISO/IEC 27018 First edition 2014-08-01, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

provider that is processing personal data on behalf of another party. Organisations can use the standard to select applicable controls when implementing a cloud computing information security management system or guidance. The standard does not specify what controls are applicable to what organisation and a risk assessment is required in order to identify it. However, the main contribution of this standard is the ability that offers to cloud providers to verify compliance with data protection rules. A self-audit by a provider can be accepted as proof of compliance with technical and organisational measures required, for example, under Article 17 Directive 95/46/EC.[194] The standard addresses, in general, the key obligations in data protection and privacy laws but cannot address special and specific issues. Therefore, compliance with legal obligations is still in place for cloud providers and cloud clients. Furthermore, the standard does not address sector-specific rules or concerns. It is the first global standard on this topic and provides a useful reference for customers and suppliers alike.[195]

As far as cloud security standards are concerned, security is considered to be one of the main challenges in building trust and confidence in cloud computing services. ENISA in particular has identified many challenges and risks related to cloud security.[196] Cloud security is a broad term and includes more than personal data protection (data breaches, cyber-attacks) and rather means network and information security in general. Relevant risks and concerns include infrastructure resilience, authentication, certification of processes and protection against illegal activities in the cloud environment including malicious system or data interference to the cloud users or service providers.[197] An ISO standard on security for cloud computing services was published in 2015.[198]

---

[194] Gleeson, Niamh Christina, and Ian Walden. "'It's a Jungle Out There'?: Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law (May 23, 2014) (2014), p.4 Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2441182
See also: de Hert, Paul, Vagelis Papakonstantinou, and Irene Kamara. "The cloud computing standard ISO/IEC 27018 through the lens of the EU legislation on data protection." Computer Law & Security Review (2015)

[195] Ibid

[196] ENISA "Benefits, risk and recommendations for cloud security" November 2009, at: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computingrisk-assessment

[197] Gleeson, Niamh Christina, and Ian Walden. "'It's a Jungle Out There'?: Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law (May 23, 2014) (2014), p.4 Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2441182

[198] ISO/IEC CD 27017 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud computing services, available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43757

Finally, standards concerning cloud metrics and service levels enable customers to evaluate and compare cloud providers, leading to more trust in cloud computing and more competition.[199]

Due to their technical character, Cloud standards will be analysed in a more detailed way in the upcoming deliverables, as they are more related to their context.

8. General Conclusions

In this deliverable we have presented a comprehensive analysis of the EU Data Protection legal framework in connection with the complicated environment Cloud Computing. This analysis has produced several duties and responsibilities for the cloud players in order to maintain data protection at high level without prejudice to the services delivered.

A first step that should be taken from businesses who wish to use cloud computing services is a comprehensive and thorough risk analysis. The purpose of this risk analysis is to highlight and address the risks related to the processing of personal data in the cloud. Special attention should be paid to assessing the legal risks regarding data processing principles, the kind of data processed, technical and organizational measures ensuring security and international transfers. The conclusions are presented below as the most basic recommendations for data protection compliance by cloud clients and cloud providers based on the analysis of the relevant legal framework.

Cloud Client-Provider relationship

We focused on this relationship as a data controller-processor relationship. Exceptional circumstances may occur, where the cloud provider may act as a controller as well. In this case, the cloud provider has full (joint) responsibility for the data processing and must comply with all relevant legal obligations derived from Directives 95/46/EC and 2002/58/EC (if applicable).

Cloud Client's responsibility

As the data controller, the Cloud Client is responsible to comply with data protection legislation and is subject to all legal obligations stemming from Directives 95/46/EC and 2002/58/EC. Furthermore, the cloud client is responsible for selecting a Cloud Provider that guarantees compliance with EU data protection legislation.

Subcontractors

Contracts between the Cloud Provider and Cloud Clients should include provisions for subcontractors, specifying that sub-processors may only be delegated on the basis of

[199] Gleeson, Niamh Christina, and Ian Walden. "'It's a Jungle Out There'?: Cloud Computing, Standards and the Law." Cloud Computing, Standards and the Law (May 23, 2014) (2014), p.2 Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2441182

the controller's consent with regards to the processor's obligation to inform the controller of any intended changes. The controller should be able to object at any time to such changes or to terminate the contract. Furthermore, the cloud provider should sign a contract with each subcontractor, clearly reflecting the provisions of his contract with the cloud client. The cloud client should also have contractual recourse possibilities in case of contractual breaches by the cloud provider's sub-contractors.

Compliance with fundamental data protection principles

- ***Transparency:*** cloud providers should inform cloud clients about all data protection relevant aspects of their services during contract negotiations (e.g. subcontractors involved, locations in which data may be stored or processed by the cloud provider and/or its subcontractors, technical and organisational measures implemented by the provider. Accordingly, the client should inform data subjects about these aspects.
- ***Purpose specification and limitation:*** the cloud client should act in compliance with this principle and ensure that the data is not processed for further purposes, other than the original, by the cloud provider or any subcontractors. Contractual commitments can also be agreed upon, including technical and organisational safeguards.
- ***Data erasure/Retention of data:*** the cloud client must ensure 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 they were collected and processed. Contracts should include provisions on secure erasure mechanisms (destruction, demagnetisation, overwriting).
- ***Accountability:*** the cloud client and the cloud provider must be able to ensure and demonstrate, through the adoption and implementation of appropriate data protection policies and technical and organizational measures that their processing activities comply with the requirements of the EU Data Protection Law.

Technical and Organisational measures

- Technical and organizational measures should be guaranteed and included in the contract between the cloud client and the cloud provider, and also be reflected in the provider and sub-contractors relationship. They should be stipulated in written or another equivalent form.
- Technical measures must ensure availability of the data (timely and reliable access to personal data) and integrity of the data (the quality of the data to keep their authenticity and not been maliciously or accidentally altered during processing, storage or transmission).
- Confidentiality is very important. Only authorized persons should have access to data. Confidentiality clauses should be included in the contracts between the cloud provider and its employees.

- Isolation is a protective goal, which is meant to address the risk that data is used beyond its initial original purpose and to maintain confidentiality and integrity.
- The data subjects have the rights of access, rectification, erasure, blocking and objection. The cloud client must verify that the cloud provider does not impose technical and organisational obstacles to the exercise of these requirements, even in cases when data is further processed by subcontractors. The exercise of the data subject rights should be facilitated by the cloud provider.
- Interoperability and data portability are facilitated by the use of standard data formats and service interfaces by the cloud providers. If a cloud client decides to move to another cloud provider, any lack of interoperability may result in the impossibility or at least difficulties to transfer the client's (personal) data to the new cloud provider ("vendor lock-in").
- Accountability is also applicable in the context of technical and organizational measures. It expresses the ability of the cloud parties to demonstrate that they took appropriate steps to ensure the implementation of data protection principles. Cloud providers, especially, should provide documentary evidence of appropriate and effective measures.

Cross-border data transfers

The cloud client should verify that the cloud provider can guarantee the lawfulness of international 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 special arrangements (e.g. the former Safe Harbor – now Privacy Shield), standard contractual clauses (SCC) or binding corporate rules (BCR).

Cloud Standards

The adoption of privacy-oriented standards and certifications is of utmost importance for the establishment of trust between cloud providers, controllers and data subjects. These standards and certifications should address not only technical measures but also processes within cloud providers' organization/business that guarantee a high level of data protection.